On the Uniqueness of Simultaneous Rational Function Reconstruction

Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore
guerrini,lebreton,zappatore@lirmm.fr
LIRMM, Université de Montpellier, CNRS
Montpellier, France

ABSTRACT

This paper focuses on the problem of reconstructing a vector of rational functions given some evaluations, or more generally given their remainders modulo different polynomials. The special case of rational functions sharing the same denominator, *a.k.a.* Simultaneous Rational Function Reconstruction (SRFR), has many applications from linear system solving to coding theory, provided that SRFR has a unique solution. The number of unknowns in SRFR is smaller than for a general vector of rational function. This allows one to reduce the number of evaluation points needed to guarantee the existence of a solution, possibly losing its uniqueness. In this work, we prove that uniqueness is guaranteed for a generic instance.

CCS CONCEPTS

• **Mathematics of computing** → **Coding theory**; • **Computing methodologies** → **Algebraic algorithms**; *Linear algebra algorithms.*

ACM Reference Format:
Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore. 2020. On the Uniqueness of Simultaneous Rational Function Reconstruction. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20), July 20–23, 2020, Kalamata, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3373207.3404051

1 INTRODUCTION

Vector Rational Function Reconstruction (VRFR) is the problem of reconstructing a vector $\boldsymbol{v}/\boldsymbol{d} = (v_1/d_1, \ldots, v_n/d_n)$ of rational functions given their remainders $u_i = v_i/d_i \bmod a_i$ and bounds on their degrees. VRFR generalizes *interpolation* problems by taking $a_1 = \cdots = a_n = \prod(x - \alpha_j)$ for some distinct α_j because the modular equations become then equations on evaluations $u_i(\alpha_j) = (v_i/d_i)(\alpha_j)$. *Simultaneous Rational Function Reconstruction* (SRFR) is the particular case of VRFR where all the rational functions share the same denominator (see Section 2.1). The common denominator constraint of SRFR reduces the number of unknowns w.r.t. VRFR, lowering the number of equations (or the number of evaluations in the interpolation case) required to ensure existence of a non-trivial solution. This consideration has interesting consequences for several applications: SRFR appears in polynomial linear system solving via evaluation-interpolation which may be done with less evaluation points. Also, SRFR is related to the decoding of interleaved Reed-Solomon codes and previous consideration can improve the error correction capability of this code (see Section 2.2). However, having a unique solution is fundamental for these applications and there are SRFR instances where the number of equations required to ensure existence does not lead to a unique solution (see Example 2.2). This work studies SRFR instances leading to uniqueness.

A uniqueness result for instances of SRFR coming from polynomial linear system solving can be found in [OS07]. However, this result requires the solution to have a specific degree. We have reasons to believe that we can generalize this result: we conjecture that for almost all $(\boldsymbol{v}, d)$ the SRFR problem admits a unique solution (see Conjecture 2.5).

We can learn more about conditions of uniqueness by looking at results coming from error correcting codes. Interleaved Reed Solomon codes (IRS) can be seen as the evaluation of a vector of polynomials $\boldsymbol{v}$. The problem of decoding IRS codes consists in the reconstruction of the vector of polynomials $\boldsymbol{v}$ given its evaluations, some possibly erroneous. A classic approach to decode IRS codes is the application of SRFR (in its interpolation version) for instances $\boldsymbol{u} = \boldsymbol{v} + \boldsymbol{e}$ where $\boldsymbol{e}$ are the errors. Results from coding theory show that for all $\boldsymbol{v}$ and almost all errors $\boldsymbol{e}$, we get the uniqueness of SRFR for the corresponding instance $\boldsymbol{u}$ (provided that there are not too many errors) [BKY03, BMS04, SSB09]. There is a natural extension of SRFR when errors occur (SRFRwE, see Section 2.2), which can be related to a fractional generalization of IRS [GLZ19, GLZ20]. We conjecture that we can decode almost all codeword $\boldsymbol{v}/d$ and almost all errors $\boldsymbol{e}$ of this fractional code (Conjecture 2.9).

In this paper we present a result which is a step towards Conjectures 2.5 and 2.9. We prove that uniqueness is guaranteed for a generic instance $\boldsymbol{u}$ of SRFR (Theorem 2.4). Our result is valid not only given evaluations, but also in the general context of any moduli a. Our approach to prove Theorem 2.4 is to study the degrees of a relation module. Solutions of SRFR are related to generators of a particular basis of this $\mathbb{K}[x]$-module which have a negative shifted-row degree. Shifts are necessary to integrate degree constraints. We show that for generic instances, there is only one generator with negative row degree, hence uniqueness of SRFR solutions.

Previous works studied generic degrees of different but related modules: *e.g.* for the module of generating polynomials of a scalar matrix sequence [Vil97], for the kernel of a polynomial matrix of specific dimensions [JV05]. Both cases do not consider any shift. The generic degrees also appear as dimensions of blocks of a shifted Hessenberg form [PS07]. However, the link with the degrees of a

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

ACM ISBN 978-1-4503-7100-1/20/07…$15.00
https://doi.org/10.1145/3373207.3404051

module is unclear and no shift is discussed (shifted Hessenberg is not related to our shift). We prove our result for any shift and any matrix dimension by adapting some of their techniques to the specific relation module related to SRFR.

In Section 2 we introduce the motivations of our work, starting from the classic SRFR to the extended version with errors. We also show their respective applications in polynomial linear system solving and in error correcting algorithms. In Section 3, we define the algebraic tools that we will use to prove our technical results of the Section 4. In Section 5 we explain how these results are linked to the uniqueness of the solution of SRFR and we finally prove Theorem 2.4 about the generic uniqueness.

2 MOTIVATIONS

2.1 Rational Function Reconstruction

In this section we recall standard definitions and we state our problem, starting from rational function reconstruction and its application to linear algebra. Let $\mathbb{K}$ be a field, $a, u \in \mathbb{K}[x]$ with $\deg(u) < \deg(a)$. The *Rational Function Reconstruction* (RFR) is the problem of reconstructing rational functions $v/d \in \mathbb{K}(x)$ verifying

$$\gcd(d, a) = 1, \frac{v}{d} = u \bmod a, \deg(v) < N, \deg(d) < D. \quad (1)$$

Since the *gcd* equation is not linear, it is customary to focus on the weaker homogeneous linear equation in the polynomial pair (v, d)

$$v = du \bmod a, \deg(v) < N, \deg(d) < D. \quad (2)$$

RFR generalizes many problems including the *Padé approximation* if $a = x^f$ and the *Cauchy interpolation* if $a = \prod_{i=1}^{f}(x - \alpha_i)$, where the α_i are pairwise distinct elements of the field $\mathbb{K}$. The homogeneous linear system related to (2) has $\deg(a)$ equations and $N + D$ unknowns. If $\deg(a) = N + D - 1$, the dimension of the solution space of (2) is at least 1 and it always admits a non-trivial solution. Moreover, such a solution is unique in the sense that all solutions are polynomial multiples of a unique one, $(v_{\min}, d_{\min})$ (see *e.g.* [GG13, Theorem 5.16]). On the other hand, (1) does not always have a solution, but when a solution exists, it is unique and must be $v_{\min}/d_{\min}$, which can be computed using the *Extended Euclidean Algorithm*. Throughout this paper, we will focus on (2).

RFR can be naturally extended to the vector case as follows. Let $a_1, \ldots, a_n \in \mathbb{K}[x]$ with degrees $f_i = \deg(a_i)$ and $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{K}[x]^n$ where $\deg(u_i) < f_i$. Given $0 < N_i, D_i \leq f_i$, the *Vector Rational Function Reconstruction* (VRFR) is the problem of reconstructing (v_i, d_i) for $1 \leq i \leq n$ such that $v_i = d_i u_i \bmod a_i, \deg(v_i) < N_i, \deg(d_i) < D_i$. We can apply RFR componentwise and so, if $f_i = N_i + D_i - 1$, we can uniquely reconstruct the solution.

SRFR is then the problem of reconstructing a vector of rational functions with the same denominator.

Definition 2.1 (SRFR). Given $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{K}[x]^n$ where $\deg(u_i) < f_i$, and degree bounds $0 < N_i < f_i$ and $0 < D < \min f_i$, we want to reconstruct the tuple $(\boldsymbol{v}, d) = (v_1, \ldots, v_n, d)$ such that

$$v_i = du_i \bmod a_i, \deg(v_i) < N_i, \deg(d) < D. \quad (3)$$

We denote $\mathcal{S}_{\boldsymbol{u}}$ the set of solutions.

Since solutions of SRFR are solutions of VRFR, SRFR has a unique solution (if it exists) whenever $f_i = N_i + D - 1$ for all i. On the other hand, if the number of equations of (3) is equal to the number of unknowns minus one, that is if

$$\sum_{i=1}^{n} f_i = \sum_{i=1}^{n} N_i + D - 1 \quad (4)$$

then (3) always admits a non-trivial solution. This number of equations is always smaller than before, possibly up to a factor 2. However, the uniqueness is not anymore guaranteed.

Example 2.2. Let $\mathbb{K} = \mathbb{F}_{11}$, $n = 2$, $N_1 = N_2 = 4$, $D = 5$ and $a_1 = a_2 = \prod_{i=1}^{6}(x - 2^i) = x^6 + 6x^5 + 5x^4 + 7x^3 + 2x^2 + 8x + 2$. Let $\boldsymbol{u} = \left(5x^5 + 5x^3 + x^2 + 4x + 4, 8x^5 + 9x^4 + 8x^3 + 8x^2 + 4x + 6\right)$. Then SRFR has two $\mathbb{K}[x]$-linearly independent solutions $(\boldsymbol{v}, d)$: $\left(8x^3 + 5x^2 + x + 6, 7x^3 + 9x^2 + 8x + 9, 7x^3 + 7x^2 + 8x + 9\right)$ and $\left(2x^3 + 2x^2 + 8x, 10x^2 + 10x + 10, 6x^4 + 7x^3 + 8x^2 + 5x + 5\right)$.

Uniqueness is a central property for the applications of SRFR: unique decoding algorithms are essential in error correcting codes, and it is also a widespread condition to use evaluation interpolation techniques in computer algebra. The number of equations which guarantees uniqueness of SRFR has also repercussion on the complexity. Indeed, the complexity of decoding algorithms or evaluation interpolation techniques depends on this number of equations. Since SRFR decreases this number up to a factor 2, this implies a constant factor speedup for applications, like in [OS07].

We denote by s the rank of the $\mathbb{K}[x]$-module spanned by the solutions $\mathcal{S}_{\boldsymbol{u}}$. All solutions can be written as a linear combination $\sum_{i=1}^{s} c_i p_i$ of s polynomials p_i with polynomial coefficients c_i. The case $s = 1$ corresponds to what we call uniqueness of the solution. In [OS07], the authors studied the particular case where $a_1 = \ldots = a_n = a$ and $N_1 = \ldots = N_n = N$. They proved the following,

Theorem 2.3 ([OS07, Theorem 4.2]). *Let k be minimal such that $\deg(a) \geq N + (D-1)/k$, then the rank s of the solution space $\mathcal{S}_{\boldsymbol{u}}$ satisfies $s \leq k$.*

Note that if $k = 1$, the solution is always unique ($s = 1$). This matches the uniqueness condition on $\deg(a)$ of VRFR. On the other hand, if $k = n$ and $\deg(a) \geq N + (D-1)/n$ then $s \leq n$, which does not provide any new information about the solution space. Theorem 2.3 represents a connection between the classic bound $\deg(a) \geq N + D - 1$ which guarantees the uniqueness and the *ideal* one $\deg(a) \geq N + (D-1)/n$ (see (4)), which exploits the common denominator property.

Our main contribution is the following

Theorem 2.4. *If $\sum_{i=1}^{n} f_i = \sum_{i=1}^{n} N_i + D - 1$ then for almost all instances $\boldsymbol{u}$, SRFR admits a unique solution,* i.e. *it has rank $s = 1$.*

Moreover, if $\mathbb{K}$ is a finite field of cardinality q, the proportion of instances leading to non-uniqueness is $\leq (D-1)/q$.

Note that when $D = 1$, rational functions become polynomials and $N_i = f_i$ so that SRFR has always a unique solution $(\boldsymbol{v}, d) = (\boldsymbol{u}, 1)$. Theorem 2.4 will be proved in Section 5. We say that a certain property $\mathcal{P}$ is verified by a generic instance $\boldsymbol{u}$ (or interchangeably for almost all instances $\boldsymbol{u}$) if and only if there exists a nonzero polynomial C such that C does not vanish on $\boldsymbol{u}$ implies that $\mathcal{P}$ is true. In our case, the property is the uniqueness of SRFR and the indeterminates of C are the polynomial coefficients $u_{j,k}$ of the components $u_j = \sum_{k=0}^{f_j - 1} u_{j,k} x^k$ of $\boldsymbol{u}$.

In terms of complexity, [OS07] computes a complete basis of the solution space using $O(nk^{\omega-1}B(\deg(a)))$ operations in $\mathbb{K}$ where $2 \le \omega \le 3$ is the exponent of the matrix multiplication and $B(t) := M(t)\log t$ where M is the classic polynomial multiplication arithmetic complexity (see [GG13] for instance). In [RNS16] the complexity was improved: they compute the solution space (in the general case of different moduli a_i) in complexity $O(n^{\omega-1}B(f)\log(f/n)^2)$ where $f = \max_i \deg(a_i)$.

Application to polynomial linear system solving. SRFR has a natural application in linear algebra. Suppose that we want to compute the solution $\boldsymbol{y} = A^{-1}\boldsymbol{b} \in \mathbb{K}(x)$ of a full rank polynomial linear system $A \in \mathbb{K}[x]^{n\times n}$, $\boldsymbol{b} \in \mathbb{K}[x]^{n\times 1}$, from its image modulo a polynomial a. We will refer to this problem as *Polynomial Linear System solving* (PLS). We remark that, by Cramer's rule, $\boldsymbol{y}$ is vector of rational functions with the same denominator: PLS is then a special case of SRFR. In [OS07, Theorem 5.1], the authors proved that the solution space is uniquely generated ($s = 1$) when $\deg(a) \ge N + (D-1)/n$ in the special case of $D = N = n\deg(A)+1$ and $\deg(A) = \deg(b)$. For this purpose, they exploited another bound on the degree of a based on [Cab71].

In view of Theorem 2.4 and as our experiments suggest, we could hope for the following,

Conjecture 2.5. *If* (4) *is satisfied then for almost all* $(\boldsymbol{v}, d)$ *with* $\gcd(d, a_i) = 1$, *SRFR with* $\boldsymbol{u} = \frac{\boldsymbol{v}}{d}$ *as input admits a unique solution.*

Since we have proved the uniqueness for generic instances $\boldsymbol{u}$, it would be sufficient to show the existence of an instance $\boldsymbol{u}$ of the form $\boldsymbol{v}/d$ for any N_i, D, a_i to prove the conjecture.

2.2 Reconstruction with Errors

In this section we introduce the problem of the Simultaneous Rational Function with Errors, *i.e.* SRFR in a scenario where errors may occur in some evaluations [BK14, KPSW17, GLZ19, Per14, GLZ20]. Throughout this section we suppose that $\mathbb{K}$ is a finite field of cardinality q, we fix $\boldsymbol{\alpha} = \{\alpha_1, \dots, \alpha_f\}$ pairwise distinct evaluation points in $\mathbb{K}$ and we consider the polynomial $a = \prod_{i=1}^{f}(x - \alpha_i)$.

Definition 2.6 (SRFR with Errors). Fix $0 < N, D, \varepsilon < f \le q$. An instance of SRFR with errors (SRFRwE) is a matrix $\boldsymbol{\omega} \in \mathbb{K}^{n\times f}$ whose columns are $\boldsymbol{\omega}_j = \boldsymbol{v}(\alpha_j)/d(\alpha_j) + \boldsymbol{e}_j$ for some reduced $\boldsymbol{v}/d \in \mathbb{K}(x)^{n\times 1}$ and some error matrix $\boldsymbol{e}$. The reduced vector must satisfy $\deg(\boldsymbol{v}) < N$, $\deg(d) < D$ and $d(\alpha_i) \ne 0$. The error matrix must have its *error support* $E := \{1 \le j \le f \mid \boldsymbol{e}_j \ne \boldsymbol{0}\}$ which satisfies $|E| \le \varepsilon$. Then SRFRwE is the problem of finding a solution $(\boldsymbol{v}, d)$ given an instance $\boldsymbol{\omega}$.

SRFRwE as Reed-Solomon decoding. Observe that if $n = 1$ and $D = 1$, $\boldsymbol{v}/d$ becomes a polynomial. Then SRFRwE is the problem of recovering a polynomial v given evaluations, some of which possibly erroneous; that is decoding an instance of a *Reed-Solomon code*. Its vector generalization, that is $n > 1$ and $D = 1$, coincides with the decoding of an *homogeneous Interleaved Reed-Solomon (IRS) code*. Indeed, an IRS codeword can be seen as the evaluation of a vector of polynomials $\boldsymbol{v}$ on $\boldsymbol{\alpha}$. Thus decoding IRS codes is the problem of recovering $\boldsymbol{v}$ from $\boldsymbol{\omega}_j = \boldsymbol{v}(\alpha_j) + \boldsymbol{e}_j$.

Let us now detail how we can solve SRFRwE using SRFR. We use the same technique of decoding RS and IRS codes [BW86, BKY03, PRN17]. We introduce the *Error Locator Polynomial* $\Lambda = \prod_{j\in E}(x - \alpha_j)$. Its roots are the erroneous evaluations so $\deg(\Lambda) = |E| \le \varepsilon$. We consider the *Lagrangian polynomials* $u_i \in \mathbb{K}[x]$ such that $u_i(\alpha_j) = \omega_{ij}$ for any $1 \le i \le n$. The classic approach is to remark that $(\boldsymbol{\varphi}, \psi) = (\Lambda\boldsymbol{v}, \Lambda d)$ is a solution of $\boldsymbol{\varphi} = \psi\boldsymbol{u} \bmod \prod_{i=1}^{f}(x - \alpha_i)$ such that $\deg(\boldsymbol{\varphi}) < N + \varepsilon$ and $\deg(\psi) < D + \varepsilon$. In this way we reduce SRFRwE to SRFR. If the unique $(\boldsymbol{\varphi}, \psi)$ satisfying latter conditions is $(\Lambda\boldsymbol{v}, \Lambda d)$, then we can reconstruct $(\boldsymbol{v}, d)$ and solve SRFRwE. Uniqueness can be obtained by taking VRFR constraints $f = (N + \varepsilon) + (D + \varepsilon) - 1 = N + D + 2\varepsilon - 1$ [BK14, KPSW17].

It is possible to reduce the number of evaluations w.r.t. the maximal number of errors ε in the setting of IRS decoding ($D = 1$).

Theorem 2.7 ([BKY03, BMS04, SSB09]). *Fix* $0 < N, \varepsilon < f \le q$ *and* E *such that* $|E| \le \varepsilon$. *If* $f = N + \varepsilon + \varepsilon/n$, *then for all* $(\boldsymbol{v}, 1)$ *and almost all error matrices* $\boldsymbol{e}$ *of support* E, *SRFRwE admits a unique solution on the instance* $\boldsymbol{\omega}$ *where* $\boldsymbol{\omega}_j = \boldsymbol{v}(\alpha_j)/d(\alpha_j) + \boldsymbol{e}_j$.

We proved a similar result in the rational function case,

Theorem 2.8 ([GLZ19, GLZ20]). *Fix* $0 < N, D, \varepsilon < f \le q$ *and* E *such that* $|E| \le \varepsilon$. *If* $f = N + D - 1 + \varepsilon + \varepsilon/n$, *then for all* $(\boldsymbol{v}, d)$ *and almost all error matrices* $\boldsymbol{e}$ *of support* E, *SRFRwE admits a unique solution on the instance* $\boldsymbol{\omega}$ *where* $\boldsymbol{\omega}_j = \boldsymbol{v}(\alpha_j)/d(\alpha_j) + \boldsymbol{e}_j$.

Since the problem of SRFRwE reduces to SRFR, there always exists a non-trivial $(\boldsymbol{\varphi}, \psi)$ whenever $f = N + \varepsilon + (D + \varepsilon - 1)/n$. Our ideal result would be to prove a uniqueness result also in this case. Our experiments suggest the following,

Conjecture 2.9. *Fix* $0 < N, D, \varepsilon < f \le q$ *and* E *such that* $|E| \le \varepsilon$. *If* $f = N + \varepsilon + (D + \varepsilon - 1)/n$, *then for almost all* $(\boldsymbol{v}, d)$ *and almost all error matrices* $\boldsymbol{e}$ *of support* E, *SRFRwE admits a unique solution on the instance* $\boldsymbol{\omega}$ *where* $\boldsymbol{\omega}_j = \boldsymbol{v}(\alpha_j)/d(\alpha_j) + \boldsymbol{e}_j$.

Note that Conjecture 2.9 is for almost all fractions $(\boldsymbol{v}, d)$ whereas Theorems 2.7 and 2.8 are for all fractions. This difference is due to Example 2.2, which shows that we can not have uniqueness for all instances $\boldsymbol{u}$ of the form $\boldsymbol{u} = \boldsymbol{v}/d$ when $f = N + (D-1)/n$. This latter number of evaluations matches the one of Conjecture 2.9 in the situation without errors $\varepsilon = 0$. Remark that this obstruction does not affect Theorems 2.7 and 2.8 because their number of evaluations f becomes $N + D - 1$ when $\varepsilon = 0$.

Our result Theorem 2.4 is a first step towards Conjecture 2.9: Since uniqueness of SRFR is true for generic instance $\boldsymbol{\omega}$, it remains to prove the existence of an instance of the form $\boldsymbol{\omega}_j = \boldsymbol{v}(\alpha_j)/d(\alpha_j) + \boldsymbol{e}_j$ for any N, D, ε, E to prove the conjecture.

Polynomial linear system solving with errors. SRFRwE was first introduced by [BK14] as a special case of Polynomial Linear System Solving with Errors (PLSwE), that we now introduce. Suppose that we want to compute the unique solution $\boldsymbol{y} = \boldsymbol{v}/d = A^{-1}\boldsymbol{b} \in \mathbb{K}[x]^{n\times n}$ of a PLS in a scenario where some errors occur [BK14, KPSW17, GLZ19]. Suppose a black box gives us solutions $\boldsymbol{y}_i = A(\alpha_i)^{-1}\boldsymbol{b}(\alpha_i)$ of evaluated systems, where α_i are f distinct evaluations points such that $d(\alpha_i) \ne 0$. This black box could make some errors in the computations; an evaluation α_j is *erroneous* if $\boldsymbol{y}_j \ne \boldsymbol{v}(\alpha_j)/d(\alpha_j)$ and we denote by $E := \{j \mid \boldsymbol{y}_j \ne \boldsymbol{v}(\alpha_j)/d(\alpha_j)\}$ the set of erroneous positions. We observe that if $j \in E$, then there exists a nonzero $\boldsymbol{e}_j \in \mathbb{K}^{n\times f}$ such that $\boldsymbol{y}_j = \boldsymbol{v}(\alpha_j)/d(\alpha_j) + \boldsymbol{e}_j$.

Hence, this problem is a special case of SRFRwE. Here we want to reconstruct a vector of rational functions which is a solution of a polynomial linear system. Therefore, all the results about uniqueness of the previous sections hold. Finally, we mention that there exists another bound on f which guarantees the uniqueness in the context of PLSwE; this bound depends on the degree of the polynomial matrix A and the vector $\boldsymbol{b}$ [KPSW17].

3 PRELIMINARIES

In this section we will give some definitions and set out the notation that we will use throughout this paper. We refer to [Nei16] for proofs of lemmas, examples and historical references.

3.1 Row degrees of a $\mathbb{K}[x]$-module

Let $\mathbb{K}$ be a field and $\mathbb{K}[x]$ its ring of polynomials. We start by defining the row degree of a vector, then of a matrix. Let $\boldsymbol{p} = (p_1, \ldots, p_v) \in \mathbb{K}[x]^v = \mathbb{K}[x]^{1\times v}$ and $\boldsymbol{s} = (s_1, \ldots, s_v) \in \mathbb{Z}^v$ a shift.

Definition 3.1 (Shifted row degree). Let $r_i = \deg(p_i) + s_i$ for $1 \le i \le v$. The $\boldsymbol{s}$*-row degree* of $\boldsymbol{p}$ is $\mathrm{rdeg}_{\boldsymbol{s}}(\boldsymbol{p}) = \max r_i$. We also denote $\boldsymbol{p} = ([r_1]_{s_1}, \ldots, [r_v]_{s_v})$ a vector of polynomials with these degrees.

We can extend this definition to polynomial matrices. In fact, let $P \in \mathbb{K}[x]^{\rho\times v}$ be a polynomial matrix, with $\rho \le v$. Let $P_{i,*}$ be the i-th row of P for $1 \le i \le \rho$. We can define the $\boldsymbol{s}$*-row degrees* of the matrix P as $\mathrm{rdeg}_{\boldsymbol{s}}(P) := (r_1, \ldots, r_\rho)$ where $r_i := \mathrm{rdeg}_{\boldsymbol{s}}(P_{i,*})$.

Let $\mathcal{N}$ be a $\mathbb{K}[x]$-submodule of $\mathbb{K}[x]^v = \mathbb{K}[x]^{1\times v}$. Since $\mathbb{K}[x]$ is a principal ideal domain, $\mathcal{N}$ is *free* of *rank* $\rho := \mathrm{rank}(\mathcal{N})$ less than v [DF03, Section 12.1, Theorem 4]. Hence, we can consider a *basis* $P \in \mathbb{K}[x]^{\rho\times v}$, *i.e.* a full rank polynomial matrix, such that $\mathcal{N} = \mathbb{K}[x]^{1\times\rho}P = \{\boldsymbol{\lambda}P \mid \boldsymbol{\lambda} \in \mathbb{K}[x]^{1\times\rho}\}$.

Our goal is to define a notion of row degrees of $\mathcal{N}$ in order to study later the $\mathbb{K}$-vector space $\mathcal{N}_{<r} := \left\{\boldsymbol{p} \in \mathcal{N} \;\middle|\; \mathrm{rdeg}_{\boldsymbol{s}}(\boldsymbol{p}) < r\right\}$ for some $r \in \mathbb{Z}$. Different bases P of $\mathcal{N}$ have different $\boldsymbol{s}$-row degrees so we need more definitions. We start with row reduced bases.

Let $\boldsymbol{t} = (t_1, \ldots, t_v) \in \mathbb{Z}^v$. We denote by $X^{\boldsymbol{t}}$ the diagonal matrix whose entries are $x^{t_1}, \ldots, x^{t_v}$. The $\boldsymbol{s}$*-leading matrix* $LM_{\boldsymbol{s}}(P)$ of P is a matrix in $\mathbb{K}^{\rho\times v}$, whose entries are the coefficient of degree zero of $X^{-\mathrm{rdeg}_{\boldsymbol{s}}(P)}PX^{\boldsymbol{s}}$. A basis $P \in \mathbb{K}[x]^{\rho\times v}$ of $\mathcal{N}$ is $\boldsymbol{s}$*-row reduced* (shortly $\boldsymbol{s}$-reduced) if $LM_{\boldsymbol{s}}(P)$ has full rank. This definition is equivalent to [Nei16, Definition 1.10], which implies that all $\boldsymbol{s}$-reduced basis of $\mathcal{N}$ have the same row degrees, up to permutation. We now focus on the following crucial property.

Lemma 3.2 (Predictable degree property). *P is $\boldsymbol{s}$-reduced if and only if for all $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_\rho) \in \mathbb{K}[x]^{1\times\rho}$,*

$$rdeg_{\boldsymbol{s}}(\boldsymbol{\lambda}P) = \max_{1\le i\le\rho}(\deg(\lambda_i) + rdeg_{\boldsymbol{s}}(P_{i,*})) = rdeg_{rdeg_{\boldsymbol{s}}(P)}(\boldsymbol{\lambda}).$$

The proof of this classic proposition can be found for instance in [Nei16, Theorem 1.11]. This latter proposition is useful because it implies that $\dim_{\mathbb{K}} \mathcal{N}_{<r} = \sum_{\{i \mid r_i < r\}}(r - r_i)$ where $(r_1, \ldots, r_\rho)$ are the $\boldsymbol{s}$-row degrees of any $\boldsymbol{s}$-reduced basis of $\mathcal{N}$.

Since we will need to define the $\boldsymbol{s}$-row degrees of $\mathcal{N}$ uniquely, not just up to permutation, we need to introduce ordered weak Popov form, which relies on the notion of pivot. The $\boldsymbol{s}$*-pivot index* of $\boldsymbol{p} \in \mathbb{K}[x]^{1\times v}$ is $\max\{j \mid \mathrm{rdeg}_{\boldsymbol{s}}(\boldsymbol{p}) = \deg(p_j) + s_j\}$. Moreover the corresponding p_j is the $\boldsymbol{s}$*-pivot entry* and $\deg(p_j)$ is the $\boldsymbol{s}$*-pivot degree* of $\boldsymbol{p}$. We naturally extend the notion of pivot to polynomial matrices. A basis P of $\mathcal{N}$ is in $\boldsymbol{s}$*-weak Popov form* if the $\boldsymbol{s}$-pivot indices of its rows are pairwise distinct. On the other hand, it is in $\boldsymbol{s}$*-ordered weak Popov form* if the sequence of the $\boldsymbol{s}$-pivot indices of its rows is strictly increasing. A basis in $\boldsymbol{s}$-weak Popov form is $\boldsymbol{s}$-reduced. Indeed, $LM_{\boldsymbol{s}}(P)$ becomes, up to row permutation, a lower triangular matrix with non-zero entries on the diagonal. Hence it is full-rank.

Assume from now on that $\mathcal{N}$ is a submodule of $\mathbb{K}[x]^v$ of rank v and that P is a basis of $\mathcal{N}$ in $\boldsymbol{s}$-ordered weak Popov form. Then its pivot indices must be $\{1, \ldots, v\}$. Weak Popov bases have a strong degree minimality property, stated in the following lemma.

Lemma 3.3 ([Nei16, Lemma 1.17]). *Let $\boldsymbol{s} \in \mathbb{Z}^v$, P be a basis of $\mathcal{N}$ in $\boldsymbol{s}$-weak Popov form with $\boldsymbol{s}$-pivot degrees $(d_1, \ldots, d_v)$. Let $\boldsymbol{p} \in \mathcal{N}$ whose pivot index is $1 \le i \le v$. Then the $\boldsymbol{s}$-pivot degree of $\boldsymbol{p}$ is $\ge d_i$ or equivalently $rdeg_{\boldsymbol{s}}(\boldsymbol{p}) \ge rdeg_{\boldsymbol{s}}(P_{i,*})$.*

As it turns out, ordered weak Popov bases are reduced bases for which the $\boldsymbol{s}$-row degrees is unique. The following lemma is a consequence of Lemma 3.3.

Lemma 3.4 ([Nei16, Lemma 1.25]). *Let $\boldsymbol{s} \in \mathbb{Z}^v$ and assume $\mathcal{N}$ is a submodule of $\mathbb{K}[x]^v$ of rank v. Let P and Q be two bases of $\mathcal{N}$ in $\boldsymbol{s}$-ordered weak Popov form. Then P and Q have the same $\boldsymbol{s}$-row degrees and $\boldsymbol{s}$-pivot degrees.*

3.2 Link between pivot and leading term

In this section, we will focus on the relation between pivots of weak Popov bases and leading terms w.r.t. a specific monomial order, as in Gröbner basis theory (see for instance [CLO98]).

Let $\mathbb{K}[\boldsymbol{x}] := \mathbb{K}[x_1, \ldots, x_n]$ be the ring of multivariate polynomials. Recall that a *monomial in* $\mathbb{K}[\boldsymbol{x}]$ is a product of powers of the indeterminates $\boldsymbol{x}^{\boldsymbol{i}} := x_1^{i_1}\cdots x_n^{i_n}$ for some $\boldsymbol{i} := (i_1, \ldots, i_n) \in \mathbb{N}^n$. On the other hand, a *monomial in* $\mathbb{K}[\boldsymbol{x}]^n$ is $\boldsymbol{x}^{\boldsymbol{i}}\boldsymbol{\varepsilon}_j$, where $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_n$ is the canonical basis of the $\mathbb{K}[\boldsymbol{x}]$-module $\mathbb{K}[\boldsymbol{x}]^n$.

A *monomial order* on $\mathbb{K}[\boldsymbol{x}]^n$ is a *total order* $\prec$ on the monomials of $\mathbb{K}[\boldsymbol{x}]^n$ such that, for any monomials $\varphi\boldsymbol{\varepsilon}_i, \psi\boldsymbol{\varepsilon}_j \in \mathbb{K}[\boldsymbol{x}]^n$ and any monomial $\tau \ne 1$, $\tau \in \mathbb{K}[\boldsymbol{x}]$, $\varphi\boldsymbol{\varepsilon}_i \prec \psi\boldsymbol{\varepsilon}_j \implies \varphi\boldsymbol{\varepsilon}_i \prec \tau\varphi\boldsymbol{\varepsilon}_i \prec \tau\psi\boldsymbol{\varepsilon}_j$. Given a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{x}]^n$ and $f \in \mathbb{K}[\boldsymbol{x}]^n$, the $\prec$*-initial term* $in_{\prec}(f)$ of f is the term of f whose monomial is the greatest with respect to the order $\prec$. We remark that in the case of $\mathbb{K}[x]$, the only monomial order is the natural degree order $x^a \prec x^b \Leftrightarrow a < b$.

We now define the *shifted* $\boldsymbol{s}$*-TOP order* (Term Over Position) on $\mathbb{K}[\boldsymbol{x}]^n$ related to a monomial order $\prec$ on $\mathbb{K}[\boldsymbol{x}]$ and a choice of *shifting monomials* $\gamma_1, \ldots, \gamma_n$ in $\mathbb{K}[\boldsymbol{x}]$:

$$\varphi\boldsymbol{\varepsilon}_i \prec_{\boldsymbol{s}-TOP} \psi\boldsymbol{\varepsilon}_j \iff (\varphi\gamma_i \prec \psi\gamma_j) \text{ or } (\varphi\gamma_i = \psi\gamma_j \text{ and } i < j)$$

for any pairs of monomials $\varphi\boldsymbol{\varepsilon}_i$ and $\psi\boldsymbol{\varepsilon}_j$ of $\mathbb{K}[\boldsymbol{x}]^n$. In the univariate case $\mathbb{K}[x]^n$, the only monomial order $\prec$ on $\mathbb{K}[x]$ is the *natural* one and the shifting monomials are $\gamma_i = x^{s_i}$ for $\boldsymbol{s} = (s_1, \ldots, s_n) \in \mathbb{N}^n$, so that the $\boldsymbol{s}$-TOP order on $\mathbb{K}[x]^n$ is

$$x^a\boldsymbol{\varepsilon}_i \prec_{\boldsymbol{s}\text{-TOP}} x^b\boldsymbol{\varepsilon}_j \iff (a + s_i, i) \prec_{lex} (b + s_j, j). \tag{5}$$

We can now state the link between this monomial order and the pivot's definition: let $\boldsymbol{p} \in \mathbb{K}[x]^{1\times n}$ and write $in_{\prec_{\boldsymbol{s}\text{-TOP}}}(\boldsymbol{p}) = \alpha x^d\boldsymbol{\varepsilon}_i$, then the $\boldsymbol{s}$-pivot index, entry, and degree are respectively i, p_i and d. This will be useful later on, in *e.g.* Proposition 4.3.

4 ROW DEGREE OF THE RELATION MODULE

Fix $m \geq n \geq 0$, and $M \in \mathbb{K}[x]^{m\times n}$. We consider a $\mathbb{K}[x]$-submodule $\mathcal{M}$ of $\mathbb{K}[x]^n$. We define the $\mathbb{K}[x]-$*module homomorphism*

$$\varphi_{\hat{M}} : \begin{array}{ccc} \mathbb{K}[x]^m & \longrightarrow & \mathbb{K}[x]^n/\mathcal{M} \\ \boldsymbol{p} & \longmapsto & \boldsymbol{p}M \end{array}.$$

Set $\mathcal{A}_{\mathcal{M},M} := \ker(\varphi_{\hat{M}})$ to get the injection

$$\varphi_M : \mathbb{K}[x]^m/\mathcal{A}_{\mathcal{M},M} \hookrightarrow \mathbb{K}[x]^n/\mathcal{M}.$$

We call $\mathcal{A}_{\mathcal{M},M}$ the *relation module* because $p \in \mathcal{A}_{\mathcal{M},M} \Leftrightarrow \varphi_M(\boldsymbol{p}) = \boldsymbol{p}M = 0 \bmod \mathcal{M}$, *i.e.* $\boldsymbol{p}$ is a relation between rows of M.

Let $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_m$ be the *canonical basis* of $\mathbb{K}[x]^m$, $\boldsymbol{\varepsilon}'_1, \ldots, \boldsymbol{\varepsilon}'_n$ the *canonical basis* of $\mathbb{K}[x]^n$ and $\boldsymbol{e}_i = \boldsymbol{\varepsilon}_i \bmod \mathbb{K}[x]^m/A_{\mathcal{M},M}$ for $1 \leq i \leq m$.

Remark 4.1. We observe that by the *Invariant Factor Form of modules over Principal Ideal Domains* (*cf.* [DF03, Theorem 4, Chapter 12]), $\mathcal{K} := \mathbb{K}[x]^n/\mathcal{M} \simeq \mathbb{K}[x]^n/\left\langle a_i\boldsymbol{\varepsilon}'_i\right\rangle_{1\leq i\leq n}$ for nonzero $a_i \in \mathbb{K}[x]$ such that $a_n|a_{n-1}|\ldots|a_1$. The polynomials a_i are the *invariants* of the module $\mathcal{M}$. We also denote $f_i := \deg(a_i)$ and we observe that $f_1 \geq f_2 \geq \ldots \geq f_n$.

From now on we will assume that $\mathcal{M} = \left\langle a_i\boldsymbol{\varepsilon}'_i\right\rangle_{1\leq i\leq n}$. It means that any $\boldsymbol{q} \in \mathcal{K}$ can be seen as $(q_1 \bmod a_1, \ldots, q_n \bmod a_n)$. Using the result of Lemma 3.4, we can define the row and pivot degrees of the relation module $\mathcal{A}_{\mathcal{M},M}$.

Definition 4.2 (Row and pivot degrees of the relation module). Let $\boldsymbol{s} \in \mathbb{Z}^m$ be a shift and P be any basis of $\mathcal{A}_{\mathcal{M},M}$ in ordered weak Popov form. The $\boldsymbol{s}$-row degrees of the relation module $\mathcal{A}_{\mathcal{M},M}$ are $\boldsymbol{\rho} := \mathrm{rdeg}_{\boldsymbol{s}}(P) = (\rho_1, \ldots, \rho_m)$ and the $\boldsymbol{s}$-pivot degrees are $\boldsymbol{\delta} := (\delta_1, \ldots, \delta_m)$ where $\delta_i = \rho_i - s_i$.

Throughout this paper we will also denote $\boldsymbol{\rho}_M$ and $\boldsymbol{\delta}_M$ when we want to stress out the matrix dependency.

4.1 Row degrees as row rank profile

In this section, we will see that the row degrees of the relation module can be deduced from the row rank profile of a matrix associated to $\varphi_{\hat{M}}$. We start by associating the pivot degree of $\boldsymbol{p} \in \mathcal{A}_{\mathcal{M},M}$ to linear dependency relation.

Proposition 4.3. *There exists $\boldsymbol{p} \in \mathcal{A}_{\mathcal{M},M}$ with $\boldsymbol{s}$-pivot index i and $\boldsymbol{s}$-pivot degree d if and only if $x^d\boldsymbol{e}_i \in B_M^{\prec x^d\boldsymbol{\varepsilon}_i}$ where $B_M^{\prec x^d\boldsymbol{\varepsilon}_i} := \langle x^n\boldsymbol{e}_j \mid x^n\boldsymbol{\varepsilon}_j \prec_{s-TOP} x^d\boldsymbol{\varepsilon}_i\rangle$.*

Proof. Fix $i, d \in \mathbb{N}$ and let $\boldsymbol{p} \in \mathbb{K}[x]^n$ with $\boldsymbol{s}$-pivot index i and $\boldsymbol{s}$-pivot degree d, so $r := \mathrm{rdeg}_{\boldsymbol{s}}(\boldsymbol{p}) = d + s_i$. Then $\boldsymbol{p} = ([\leq r]_{s_1}, \ldots, [\leq r]_{s_{i-1}}, [r]_{s_i}, [< r]_{s_{i+1}}, \ldots, [< r]_{s_m})$ (see Definition 3.1) and we can write $\boldsymbol{p} = cx^d\boldsymbol{\varepsilon}_i + \boldsymbol{p}'$ where $c \in \mathbb{K}^*$ and $\boldsymbol{p}' = ([\leq r]_{s_1}, \ldots, [\leq r]_{s_{i-1}}, [< r]_{s_i}, [< r]_{s_{i+1}}, \ldots, [< r]_{s_m})$. So $\boldsymbol{p} \in \mathcal{A}_{\mathcal{M},M}$ has s-pivot index i and degree $d \Leftrightarrow x^d\boldsymbol{\varepsilon}_i = -1/c\ \boldsymbol{p}' \bmod \mathcal{A}_{\mathcal{M},M} \Leftrightarrow$

$$x^d\boldsymbol{e}_i \in \left\langle x^n\boldsymbol{e}_j \;\middle|\; \begin{array}{ll} n + s_j \leq d + s_i, & \text{for } 1 \leq j \leq i-1 \\ n + s_j < d + s_i, & \text{for } i \leq j \leq m \end{array} \right\rangle = B_M^{\prec x^d\boldsymbol{\varepsilon}_i}. \quad \square$$

Theorem 4.4. *Let $\boldsymbol{\delta}$ be the $\boldsymbol{s}$-pivot degrees of the relation module $\mathcal{A}_{\mathcal{M},M}$. Then $\delta_j = min\{d \mid x^d\boldsymbol{e}_j \in B_M^{\prec x^d\boldsymbol{\varepsilon}_j}\}$ for any $1 \leq j \leq m$.*

Proof. Fix $1 \leq j \leq m$. During this proof we denote $\overline{\delta}_j := min\{d \mid x^d\boldsymbol{e}_j \in B_M^{\prec x^d\boldsymbol{\varepsilon}_j}\}$. We want to prove that $\delta_j = \overline{\delta}_j$. Recall that by Proposition 4.3, $x^{\delta_j}\boldsymbol{e}_j \in B_M^{\prec x^{\delta_j}\boldsymbol{\varepsilon}_j}$. Hence, by the minimality of $\overline{\delta}_j$, $\delta_j \geq \overline{\delta}_j$. On the other hand, $x^{\overline{\delta}_j}\boldsymbol{e}_j \in B_M^{\prec x^{\overline{\delta}_j}\boldsymbol{\varepsilon}_j}$ so by Proposition 4.3 there exists $\boldsymbol{p} \in \mathcal{A}_{\mathcal{M},M}$ of $\boldsymbol{s}$-pivot index j and degree $\overline{\delta}_j$. Finally, by Lemma 3.3 we can conclude that $\overline{\delta}_j \geq \delta_j$. $\square$

We now define the *ordered matrix* O_M as the matrix of $\hat{\varphi}_M$ w.r.t. particular $\mathbb{K}$-vector space bases: the rows of O_M from top to bottom are the monomials of $\mathbb{K}[x]^m$ sorted increasingly for the $\prec_{s-TOP}$ order (see (5)). The columns of O_M are written *w.r.t.* the basis $\{x^i\boldsymbol{\varepsilon}'_j\}_{\substack{1\leq j\leq n \\ 0\leq i<f_j}}$ of $\mathbb{K}[x]^n/\mathcal{M}$. Therefore, O_M has finite rank $\mathrm{rank}(O_M) = \mathrm{rank}(\hat{\varphi}_M) = \mathrm{rank}(\varphi_M)$, infinite number of rows and $(\sum_{i=1}^n f_i) = \dim_{\mathbb{K}}(\mathbb{K}[x]^n/\mathcal{M})$ columns.

Monomial row rank profile. Our goal is to relate the row rank profile of O_M to the row degrees of the relation module. The classic definition of row rank profile of a rank r polynomial matrix is the lexicographically smallest sequence of r indices of linearly independent rows (*cf.* [DPS15] for instance). Since the rows of our ordered matrix O_M correspond to monomials, we will transpose the previous definition to monomials instead of indices.

Let Mon_r be the sets of r monomials of $\mathbb{K}[x]^m$. We define the lexicographical ordering on Mon_r by comparing lexicographically the sorted monomials for $\prec_{s-TOP}$. In detail, $\mathcal{F} \prec_{lex} \mathcal{F}'$ iff there exists $1 \leq t \leq r$ s.t. $x^{i_l}\boldsymbol{\varepsilon}_{j_l} = x^{u_l}\boldsymbol{\varepsilon}_{v_l}$ for $l < t$ and $x^{i_t}\boldsymbol{\varepsilon}_{j_t} \prec_{s-TOP} x^{u_t}\boldsymbol{\varepsilon}_{v_t}$ where $\mathcal{F} = \{x^{i_l}\boldsymbol{\varepsilon}_{j_l}\}_{1\leq l\leq r}$ and $\mathcal{F}' = \{x^{u_l}\boldsymbol{\varepsilon}_{v_l}\}_{1\leq l\leq r}$ and both $\{x^{i_l}\boldsymbol{\varepsilon}_{j_l}\}$ and $\{x^{u_l}\boldsymbol{\varepsilon}_{v_l}\}$ are increasing for the $\prec_{s-TOP}$ order.

We will use this lexicographic order on monomials to define the row rank profile of O_M. Let $r = \mathrm{rank}(O_M)$.

Definition 4.5 (Row rank profile). For any matrix $M \in \mathbb{K}[x]^{m\times n}$, we define the *row rank profile* of O_M (shortly RRP_M) as the family of monomials of $\mathbb{K}[x]^m$ defined by $RRP_M := min_{\prec_{lex}}\mathcal{P}_M$ where

$$\mathcal{P}_M := \left\{\mathcal{F} \in \mathsf{Mon}_r \;\middle|\; \{mM\}_{m\in\mathcal{F}} \text{ are linearly independent in } \mathcal{K}\right\}.$$

We now introduce a particular family of monomials, that we will frequently use: we will denote $\mathcal{F}_{\boldsymbol{d}} := \{x^i\boldsymbol{\varepsilon}_j\}_{\substack{i<d_j \\ 1\leq j\leq m}}$ for any $\boldsymbol{d} = (d_1, \ldots, d_m) \in \mathbb{N}^m$.

This family allows us to finally relate the row rank profile of O_M to the row degrees of the relation module.

Proposition 4.6. *The row rank profile of the ordered matrix O_M is given by the pivot degrees $\boldsymbol{\delta}_M$ of the relation module $\mathcal{A}_{\mathcal{M},M}$,* i.e. *$RRP_M = \mathcal{F}_{\boldsymbol{\delta}_M}$.*

Proof. We fix the matrix M in order to simplify notations. We define $\delta'_j = min\left\{\delta \mid x^\delta\boldsymbol{\varepsilon}_j \notin RRP\right\}$ and $\boldsymbol{\delta}' = (\delta'_1, \ldots, \delta'_m)$. By properties of row rank profile, we have that $x^{\delta_j}\boldsymbol{e}_j \in B^{\prec x^{\delta_j}\boldsymbol{\varepsilon}_j}$ (otherwise we could create a smaller family of linearly independent monomial with $x^{\delta_j}\boldsymbol{e}_j$). Using Theorem 4.4, we deduce that $\delta'_j \geq \delta_j$. Therefore $\mathcal{F}_{\boldsymbol{\delta}} \subset \mathcal{F}_{\boldsymbol{\delta}'} \subset RRP$. Since the families of monomials $\mathcal{F}_{\boldsymbol{\delta}}$ and RRP have the same cardinality $r = \mathrm{rank}(O_M)$, they are equal so $\mathcal{F}_{\boldsymbol{\delta}} = RRP$. $\square$

4.2 Constraints on relation's row degrees

We will now focus on integer tuples $\boldsymbol{\delta}_M$ which can be achieved. For this matter, in the light of Proposition 4.6, we need to understand which families $\mathcal{F}_{\boldsymbol{d}}$ of monomials can be linearly independent in the ordered matrix, *i.e.* belong to $\mathcal{P}_M$ (see Definition 4.5).

Recall that $\mathcal{K} = \mathbb{K}[x]^n/\mathcal{M} = \mathbb{K}[x]^n/\langle a_i\boldsymbol{\varepsilon}'_i\rangle_{1\le i\le n}$ and $f_i = \deg(a_i)$ are non-increasing as in Remark 4.1. Recall also from Definition 4.5 that $\mathcal{P}_M$ is the set of families $\mathcal{F}$ of r monomials in $\mathbb{K}[x]^m$ such that $\{mM\}_{m\in\mathcal{F}}$ are linearly independent in $\mathbb{K}[x]^n/\mathcal{M}$.

Theorem 4.7. *Let $\boldsymbol{d} \in \mathbb{N}^m$ be non-increasing. We can extend $\boldsymbol{f} \in \mathbb{N}^m$ by $f_{n+1} = \ldots = f_m = 0$. Then $\exists M \in \mathbb{K}[x]^{m\times n}$ such that $\mathcal{F}_{\boldsymbol{d}} \in \mathcal{P}_M$ if and only if $\sum_{i=1}^{l} d_i \le \sum_{i=1}^{l} f_i$ for all $1 \le l \le m$.*

The non-increasing property of $\boldsymbol{d}$ can be lifted: let $\boldsymbol{d}$ be non-increasing and $\boldsymbol{d}'$ be any permutation of $\boldsymbol{d}$. Then $\exists M \in \mathbb{K}[x]^{m\times n}$ such that $\mathcal{F}_{\boldsymbol{d}} \in \mathcal{P}_M$ if and only if $\exists M' \in \mathbb{K}[x]^{m\times n}$ such that $\mathcal{F}_{\boldsymbol{d}'} \in \mathcal{P}_{M'}$. Indeed, permuting $\boldsymbol{d}$ amounts to permuting the components of $\boldsymbol{p}$, *i.e.* permuting the rows of M. This does not affect the existence property.

Theorem 4.7 is an adaptation of [Vil97, Proposition 6.1] and its derivation [PS07, Theorem 3]. Even if the statements of these two papers are in a different but related context, their proof can be applied almost straightforwardly. We will still provide the main steps of the proof, for the sake of clarity and also because we will have to adapt it later in the proof of Theorem 2.4. Note also that we complete the 'if' part of the proof because it was not detailed in earlier references. For this purpose, we introduce the following

Lemma 4.8. *Let $\mathcal{N}$ be a $\mathbb{K}[x]$-submodule of $\mathcal{K}$ of rank l. Then the dimension of $\mathcal{N}$ as $\mathbb{K}$-vector space is at most $f_1 + \cdots + f_l$.*

Proof. First, remark that if $\boldsymbol{q} \in \mathcal{N}$ has its first non-zero element at index p then $a_p\boldsymbol{q} = 0$. Now since $\mathcal{N}$ has rank l, we can consider the matrix B whose rows are the l elements of a basis of $\mathcal{N}$. We operate on the rows of B to obtain the *Hermite normal form* B' of B. The rows $(\boldsymbol{b}'_i)_{1\le i\le l}$ of B' have first non-zero elements at distinct indices $k_1, \ldots, k_l$. Therefore $a_{k_j}\boldsymbol{b}'_j = 0$ and $\{x^i\boldsymbol{b}'_j\}_{\substack{0\le i<f_{k_j}\\ 1\le j\le l}}$ is a generating set of $\mathcal{N}$ and so $\dim_{\mathbb{K}} \mathcal{N} \le f_{k_1} + \cdots + f_{k_l} \le f_1 + \cdots + f_l$ since (f_i) are non increasing and (k_j) pairwise distinct. □

Corollary 4.9. *Let $r \ge 0$, $\boldsymbol{d} \in \mathbb{N}^l$ and $v_1, \ldots, v_l \in \mathcal{K}$ such that $\{x^j\boldsymbol{v}_i\}_{\substack{0\le j<d_i\\ 1\le i\le l}}$ are linearly independent then $\sum_{i=1}^{l} d_i \le \sum_{i=1}^{l} f_i$.*

Proof. We consider $\mathcal{N}$ the $\mathbb{K}[x]$-module spanned by $\{v_1, \ldots, v_l\}$, and we observe that $d_1 + \cdots + d_l \le \dim \mathcal{N} \le f_1 + \cdots + f_l$ by Lemma 4.8. □

Proof of Theorem 4.7. We observe that if $m > n$, we can write $\mathcal{K} = \mathbb{K}[x]^n/\langle a_i\boldsymbol{\varepsilon}'_i\rangle_{1\le i\le n} = \mathbb{K}[x]^m/\langle a_i\boldsymbol{\varepsilon}_i\rangle_{1\le i\le m}$ where $a_j = 1$ for $n+1 \le j \le m$. Hence, we can suppose *w.l.o.g.* that $m = n$.

$\Rightarrow$) By the hypotheses, there exists a matrix $M \in \mathbb{K}[x]^{m\times n}$ such that $\{x^i\boldsymbol{\varepsilon}_jM\}_{x^i\boldsymbol{\varepsilon}_j\in\mathcal{F}_{\boldsymbol{d}}} = \{x^i\boldsymbol{v}_j\}_{0<i<d_j}$ are linearly independent in $\mathcal{K}$ where $\boldsymbol{v}_j := \boldsymbol{\varepsilon}_jM$. Hence, for all $1 \le l \le m$, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ satisfy the conditions of the Corollary 4.9 and so $\sum_{i=1}^{l} d_i \le \sum_{i=1}^{l} f_i$.

$\Leftarrow$) Set $\boldsymbol{u}_i = \boldsymbol{\varepsilon}_i$ for $1 \le i \le m$ so that $\{x^i\boldsymbol{u}_j\}_{\substack{i<f_j\\ 1\le j\le m}}$ are linearly independent in $\mathcal{M}$. We now consider the matrix $K := [K_1|\ldots|K_m]$ where $K_j \in \mathbb{K}[x]^{m\times f_j}$ is in *Krylov* form, that is $K_j = K(\boldsymbol{u}_j, f_j) := [\boldsymbol{u}_j|x\boldsymbol{u}_j|\ldots|x^{f_j-1}\boldsymbol{u}_j]$ by considering $\boldsymbol{u}_j$ as a column vector. Note that K is full column rank by construction. Our goal is to find vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ such that $[K(\boldsymbol{v}_1, d_1)|\ldots|K(\boldsymbol{v}_m, d_m)]$ is full column rank (see $\widetilde{K}$ later).

For this purpose, we first need to consider the matrix $\overline{K}$ made of columns of K so that it remains full column rank. It is defined as $\overline{K} := [\overline{K}_1|\ldots|\overline{K}_m]$ where for $1 \le j \le m$, $\overline{K}_j \in \mathbb{K}[x]^{m\times d_j}$ are defined iteratively by

$$\overline{K}_j := [K(\boldsymbol{u}_j, \min(f_j, d_j))|K(x^{s_1}\boldsymbol{u}_{j_1}, t_1)|\ldots|K(x^{s_k}\boldsymbol{u}_{j_k}, t_k)]$$

and $K(x^{s_l}\boldsymbol{u}_{j_l}, t_l)$ derives from previously unused columns in K, which we add from left to right, *i.e.* (j_l) are increasing. Since $\sum_{i=1}^{j} d_i \le \sum_{i=1}^{j} f_i$, we will only pick from previous blocks, *i.e.* $j_k < j$. Since we must have depleted a block K_{i_l} before going to another one, we can observe that $s_l + t_l = f_l$ for $l < k$. The last block K_{i_k} is the only one that may not be exhausted, *i.e.* $s_k + t_k \le f_k$. Conversely, $s_l = d_l$ for $l > 1$ because no columns have been picked yet from the blocks j_l, except maybe the first block j_1 where $s_1 \ge d_1$.

We want to transform $\overline{K}_j$ into a Krylov matrix $\widetilde{K}_j$, working block by block. First we extend $[K(\boldsymbol{u}_j, \min(f_j, d_j))|0|\ldots|0]$ to the right to $K(\boldsymbol{u}_j, d_j)$. Then we extend all blocks $[0|\ldots|0|K(x^{s_l}\boldsymbol{u}_{j_l}, t_l)|0|\ldots|0]$ to the left and the right to $K(x^{s'_l}\boldsymbol{u}_{j_l}, d_l)$ where s'_l equals s_l minus the number of columns of the left extension. In this way, the extension matches the original matrix on its non-zero columns. Now we can define $\widetilde{K} := [\widetilde{K}_1|\ldots|\widetilde{K}_m]$, where $\widetilde{K}_j := K(\boldsymbol{v}_j, d_j)$ with $\boldsymbol{v}_j := \boldsymbol{u}_j + \sum_{l=1}^{k} x^{s'_l}\boldsymbol{u}_{j_l}$.

A crucial point of the proof is to show that $s'_k \ge 0$. But since d_i are-non increasing, j_l are increasing and $j_k < j$, we get $s_l \ge d_{j_l} \ge d_{j_k} \ge d_j$. As the number of columns of the left extension is at most d_j, we can conclude $s'_k \ge 0$.

In [Vil97] and [PS07] it is proved that there exist an upper triangular matrices T such that $\widetilde{K} = \overline{K}T$. So we can conclude that $\widetilde{K}$, which is in the desired block Krylov form, is full column rank as is $\overline{K}$, which concludes the proof. □

Example 4.10. We illustrate the construction of the proof of Theorem 4.7 with example. Let $m = 4$, $n = 3$, $\boldsymbol{f} = (8, 4, 4)$ extended to $f_4 = 0$ and $\boldsymbol{d} = (5, 5, 3, 3)$. Remark that $\sum_{i=1}^{l} d_i \le \sum_{i=1}^{l} f_i$ for all $1 \le l \le m$. Then $\overline{K}_1 = K(\boldsymbol{u}_1, d_1)$, $\overline{K}_2 = [K(\boldsymbol{u}_2, f_2)|K(x^{d_1}\boldsymbol{u}_1, d_2 - f_2)]$ picks its missing column from the first unused column of K_1, $\overline{K}_3 = K(\boldsymbol{u}_3, d_3)$, and $\overline{K}_4 = [K(\boldsymbol{u}_4, f_4) = \varnothing|K(x^{d_1+1}\boldsymbol{u}_1, f_1 - (d_1 + 1)|K(x^{d_3}\boldsymbol{u}_3, f_3 - d_3)]$ picks its 3 missing columns first from the 2 unused of K_1, then from the remaining one of K_3. Then the construction extends $\overline{K}$ to $\widetilde{K} = K(\boldsymbol{v}_i, d_i)$ where $\boldsymbol{v}_1 = \boldsymbol{u}_1 = [1, 0, 0]$, $\boldsymbol{v}_2 = \boldsymbol{u}_2 + x^{d_2-(d_1-1)}\boldsymbol{u}_1 = [x, 1, 0]$, $\boldsymbol{v}_3 = \boldsymbol{u}_3 = [0, 0, 1]$ and $\boldsymbol{v}_4 = x^{d_1+1}\boldsymbol{u}_1 + x^{d_3-(f_1-(d_1+1))}\boldsymbol{u}_3 = [x^6, 0, x]$. Finally the matrix M of the statement of Theorem 4.7 has its j-th row $M_{j,*}$ equal to $\boldsymbol{v}_j$. ◇

We now have all the cards in our hand to state the principal constraint on the pivot degrees $\boldsymbol{\delta}_M$ of the relation module $\mathcal{A}_{\mathcal{M},M}$ when M varies in the set of matrices $\mathbb{K}[x]^{m\times n}$ such that $\operatorname{rank}(O_M) = \operatorname{rank}(\varphi_M)$ is fixed. We will denote by $\mathbf{d}_r$ the pivot degrees corresponding to the constraint.

Theorem 4.11. *Recall that $\boldsymbol{f} = (f_1, \ldots, f_m)$ are the degrees of the invariants of $\mathcal{M}$ where $f_i = 0$ for $n+1 \le i \le m$, and let $r = \operatorname{rank}(O_M)$.*

Then $\mathcal{F}_{\boldsymbol{\delta}_M} \geq_{lex} \mathcal{F}_{\mathbf{d}_r}$ *where*

$$\mathcal{F}_{\mathbf{d}_r} = min_{<_{lex}} \left\{ \mathcal{F}_{\boldsymbol{d}} \in \mathsf{Mon}_r \;\middle|\; \forall 1 \leq l \leq m,\ \sum_{i=1}^{l} d_i \leq \sum_{i=1}^{l} f_i \right\} \quad (6)$$

Proof. We know from Proposition 4.6 that $RRP_M = \mathcal{F}_{\boldsymbol{\delta}_M}$ so $\{x^i \boldsymbol{\varepsilon}_j M\}_{\substack{i<\delta_{j,M} \\ 1\leq j\leq m}}$ are linearly independent and $\sum_{i=1}^{m} \delta_{i,M} = r$. Using Theorem 4.7, we get that $\sum_{i=1}^{l} \delta_{i,M} \leq \sum_{i=1}^{l} f_i$ for all $1 \leq l \leq m$. This means that $\mathcal{F}_{\boldsymbol{\delta}_M}$ belongs to the set whose minimum is $\mathcal{F}_{\mathbf{d}_r}$, which implies our result. □

We observe that $r = \mathrm{rank}(O_M)$ must satisfy $0 \leq r \leq \Sigma := \sum_{i=1}^{m} f_i = \dim_{\mathbb{K}} \mathbb{K}[x]^n/\mathcal{M}$ and that $r = \Sigma$ is reachable since $m \geq n$. Note also that $\mathbf{d}_r$ is well-defined in Theorem 4.11 as long as $0 \leq r \leq \Sigma := \sum_{i=1}^{m} f_i$ because it is related to the minimum of a non-empty set.

4.3 Generic row degrees of relation module

We will now show that this pivot degrees constraint $\mathbf{d}_\Sigma$ is attainable by $\boldsymbol{\delta}_M$ for matrices M such that $\mathrm{rank}(O_M) = \mathrm{rank}(\varphi_M) = \dim_{\mathbb{K}} \mathbb{K}[x]^n/\mathcal{M}$ in which case φ_M becomes a bijection. More specifically, we will show that this is the case for almost all matrices $M \in \mathbb{K}[x]^{m\times n}$.

Corollary 4.12. *For a generic matrix* $M \in \mathbb{K}[x]^{m\times n}$*, the pivot degrees* $\boldsymbol{\delta}_M$ *of the relation module* $A_{\mathcal{M},M}$ *satisfy* $\boldsymbol{\delta}_M = \mathbf{d}_\Sigma$ *where* $\Sigma = \sum_{i=1}^{n} f_i$.

Proof. Our goal is to prove that there exists a non-zero polynomial C in the coefficients $m_{i,j,k}$ of the polynomial entries $m_{i,j}$ of M such that $C(m_{i,j,k}) \neq 0$ implies that $\boldsymbol{\delta}_M = \mathbf{d}_\Sigma$.

Since $\sum_{i=1}^{l} \mathrm{d}_{\Sigma,i} \leq \sum_{i=1}^{l} f_i$ for all $1 \leq l \leq m$, we deduce from Theorem 4.7 that there exists $M \in \mathbb{K}[x]^{m\times n}$ such that $\{mM\}_{m\in\mathcal{F}_{\mathbf{d}_\Sigma}}$ are linearly independent. So the Σ-minor of the ordered matrix O_M of M corresponding to those lines is non-zero. We now consider this Σ-minor as a function C in the coefficients $m_{i,j,k}$ of the polynomial entries $m_{i,j}$ of M. Note that $C \in \mathbb{K}[m_{i,j,k}]$ since the entries of O_M are linear combinations of $m_{i,j,k}$. Indeed, we can write $m_{i,j} = \sum_{k=0}^{f_j-1} m_{i,j,k} x^k$ because $m_{i,j}$ is only considered modulo a_j, and the coefficient of O_M w.r.t. line $x^u\boldsymbol{\varepsilon}_i$ and column $x^v\boldsymbol{\varepsilon}'_j$ is $\sum_{k=0}^{f_j-1} m_{i,j,k} c_{j,k,u,v}$ where $c_{j,k,u,v} \in \mathbb{K}$ is the coefficient of $(x^{k+u} \bmod a_j)$ in x^v. We have seen that C admits a nonzero evaluation so is a non-zero polynomial.

Now for any matrix M such that $C(m_{i,j,k}) \neq 0$, the vectors $\{mM\}_{m\in\mathcal{F}_{\mathbf{d}_\Sigma}}$ must be linearly independent, so $\mathrm{rank}(O_M) = \Sigma$. We have $RRP_M \leq_{lex} \mathcal{F}_{\mathbf{d}_\Sigma}$ because $\mathcal{F}_{\mathbf{d}_\Sigma} \in \mathcal{P}_M$ (see Definition 4.5). Theorem 4.11 gives the other inequality, so $\mathcal{F}_{\mathbf{d}_\Sigma} = RRP_M = \mathcal{F}_{\boldsymbol{\delta}_M}$ and $\boldsymbol{\delta}_M = \mathbf{d}_\Sigma$. □

4.3.1 Special cases. In this section, we will see that our definition of the generic pivot degrees $\mathbf{d}_\Sigma$ in (6) has a simplified expression in a wide range of settings. Set the notation $\bar{s} = \max(\boldsymbol{s})$. We will see that under some assumptions the expected row degrees $\mathbf{p}_\Sigma := \mathbf{d}_\Sigma + \boldsymbol{s}$ has a nice form. Define p and u be the quotient and remainder of the Euclidean division $\sum_{i=1}^{m}(f_i + s_i) = p \cdot m + u$. The expected nice form of the row degrees will be

$$\boldsymbol{p} := (\underbrace{p+1, \ldots, p+1}_{u \text{ times}}, \underbrace{p, \ldots, p}_{m-u \text{ times}}). \quad (7)$$

This nice form will appear if the following conditions on $\boldsymbol{f}$ and $\boldsymbol{s}$ hold:

$$p \geq \bar{s} \quad (8)$$

$$\forall 1 \leq l \leq m-1,\ \sum_{i=1}^{l} p_i \leq \sum_{i=1}^{l} (f_i + s_i) \quad (9)$$

Theorem 4.13. *Let* $\boldsymbol{p}$ *as in* (7)*, and let* $\boldsymbol{f}$ *be non-increasing such that* (8) *and* (9) *hold. Then* $\mathbf{p}_\Sigma = \boldsymbol{p}$.

This nice form of row degree was already observed in different but related settings. To the best of our knowledge, it can be found in [Vil97, Proposition 6.1] for row degrees of minimal generating matrix polynomial but with no shift, in [PS07, Corollary 1] for dimensions of blocks in a shifted Hessenberg form but the link to row degree is unclear and no shift is discussed (shifted Hessenberg is not related to our shift $\boldsymbol{s}$), and in [JV05, after (2)] for kernel basis were $m = 2n$ with no shifts.

Proof. Denote again $\Sigma = \sum_{i=1}^{n} f_i$. Let $\overline{\mathcal{F}}$ be the first Σ monomials of $\mathbb{K}[x]^m$ for the $\prec_{\boldsymbol{s}-TOP}$ ordering. Let $\boldsymbol{p} = (p+1, \ldots, p+1, p, \ldots, p)$ be the candidate row degrees as in the theorem statement and $\boldsymbol{d} = \boldsymbol{p} - \boldsymbol{s}$ be the corresponding pivot degrees. Note that (8) implies that $p \geq \bar{s}$ so $\boldsymbol{d} \in \mathbb{N}^m$.

First we show that (8) implies $\overline{\mathcal{F}} = \mathcal{F}_{\boldsymbol{d}}$. For the first part, in order to prove $\overline{\mathcal{F}} = \mathcal{F}_{\boldsymbol{d}}$, we need to show that $d_i = \min\{d \in \mathbb{N} \mid x^d\boldsymbol{\varepsilon}_i \notin \overline{\mathcal{F}}\}$. We already know that $d_i \in \mathbb{N}$. We will need to study the row degrees of the first monomials to conclude. The monomials of $\mathbb{K}[x]^m$ of $\boldsymbol{s}$-row degree r ordered increasingly for $\prec_{\boldsymbol{s}-TOP}$ are $[x^{r-s_i}\boldsymbol{\varepsilon}_i]$ for increasing $1 \leq i \leq m$ such that $s_i \leq r$. There are m such monomials when $r \geq \bar{s}$. The monomials of $\boldsymbol{s}$-row degree less than $\bar{s}$ are $\{x^i\boldsymbol{\varepsilon}_j\}_{i+s_j<\bar{s}}$ and their number is $\sum_{i=1}^{m}(\bar{s} - s_i)$. From this we can deduce that the row degree of the n-th smallest monomial is $\left\lfloor (n - 1 - \sum_{i=1}^{m}(\bar{s} - s_i))/m \right\rfloor + \bar{s} = \left\lfloor (n - 1 + \sum_{i=1}^{m} s_i)/m \right\rfloor$ provided that $n \geq \sum_{i=1}^{m}(\bar{s} - s_i) + 1$. We can now remark that the $(\Sigma+1)$-th smallest monomial has $\boldsymbol{s}$-row degree p. More precisely, the $(\Sigma+1)$-th smallest monomial is the $(u+1)$-th monomial of row-degree r, so $\overline{\mathcal{F}}$ is equal to all monomials of row degree less than p and the first u monomials of row degree p. This proves $d_i = \min\{d \in \mathbb{N} \mid x^d\boldsymbol{\varepsilon}_i \notin \overline{\mathcal{F}}\}$ and $\overline{\mathcal{F}} = \mathcal{F}_{\boldsymbol{d}}$.

Second we deduce from (9) that for all $1 \leq l \leq m$, $\sum_{i=1}^{l} d_i = \sum_{i=1}^{l}(p_i - s_i) \leq \sum_{i=1}^{l} f_i$, so $\mathcal{F}_{\mathbf{d}_r} \leq_{lex} \mathcal{F}_{\boldsymbol{d}}$ by Theorem 4.11 and finally $\mathcal{F}_{\mathbf{d}_r} = \mathcal{F}_{\boldsymbol{d}}$ because $\overline{\mathcal{F}}$ is the smallest set of Σ monomials. □

Example 4.14. Here we provide 3 examples of generic pivot degrees $\mathbf{d}_\Sigma$ and row degrees $\mathbf{p}_\Sigma$: Corollary 4.12 applies only to the first situation because the second and third situations are constructed so that (8) and respectively (9) are not satisfied. Let $m = n = 3$ and $\boldsymbol{s} = (0, 2, 4)$ so that $\bar{s} = 4$ and $\sum(\bar{s} - s_i) = 6$.

In the first situation $\boldsymbol{f} = (6, 1, 0)$, so $\sum(f_i + s_i) = 4m + 1$ and using Corollary 4.12 we get $\mathbf{p}_\Sigma = (5, 4, 4)$ from (7) and $\mathbf{d}_\Sigma = (5, 2, 0)$. In the second situation, $\boldsymbol{f} = (3, 0, 0)$ and (8) is not satisfied. We use Theorem 4.13 to get $\mathbf{d}_\Sigma = (3, 0, 0)$ from (6) and $\mathbf{p}_\Sigma = (3, 2, 4)$. Finally in the third situation, $\boldsymbol{f} = (3, 3, 1)$ and (9) is not satisfied. We

use Theorem 4.13 to get $\mathbf{d}_\Sigma = (3,3,1)$ from (6) and $\mathbf{p}_\Sigma = (3,5,5)$. Let $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ be the respective families of monomial of the three situations. We picture these families in the following table, where *Mon* are the first monomials for $\prec_{s-TOP}$

Mon	$\boldsymbol{\varepsilon}_1$	$x\boldsymbol{\varepsilon}_1$	$x^2\boldsymbol{\varepsilon}_1$	$\boldsymbol{\varepsilon}_2$	$x^3\boldsymbol{\varepsilon}_1$	$x\boldsymbol{\varepsilon}_2$	$x^4\boldsymbol{\varepsilon}_1$	$x^2\boldsymbol{\varepsilon}_2$	$\boldsymbol{\varepsilon}_3$
$\text{rdeg}_{\boldsymbol{s}}$	0	1	2		3		4		
$\mathcal{F}_1$	•	•	•	•	•	•	•		
$\mathcal{F}_2$	•	•	•						
$\mathcal{F}_3$	•	•	•	•		•		•	•

5 UNIQUENESS RESULTS ON SRFR

Let's recall SRFR defined in Section 2.1: let $a_1, \ldots, a_n \in \mathbb{K}[x]$ with degrees $f_i := \deg(a_i)$ and $\boldsymbol{u} := (u_1, \ldots, u_n) \in \mathbb{K}[x]^n$ such that $\deg(u_i) < f_i$ and $0 < N_i \leq f_i$ for $1 \leq i \leq n$, $0 < D \leq \min_{1\leq i\leq n}\{f_i\}$. We want to reconstruct $(\boldsymbol{v}, d) = (v_1, \ldots, v_n, d) \in \mathbb{K}[x]^{1\times(n+1)}$ such that $v_i = du_i \bmod a_i, \deg(v_i) < N_i, \deg(d) < D$. We consider $\mathcal{M} = \langle a_i\boldsymbol{\varepsilon}_i'\rangle$ and we denote by $S_{\boldsymbol{u}}$ the set of tuples which verify (3).

Lemma 5.1. *For the shift $\boldsymbol{s} = (-N_1, \ldots, -N_n, -D) \in \mathbb{Z}^{n+1}$, we have $(\boldsymbol{v}, d) \in S_{\boldsymbol{u}} \Leftrightarrow (\boldsymbol{v}, d) \in \mathcal{A}_{\mathcal{M},R_{\boldsymbol{u}}}$ with $rdeg_{\boldsymbol{s}}((\boldsymbol{v}, d)) < 0$, where*

$$R_{\boldsymbol{u}} := \begin{bmatrix} \mathrm{Id}_n \\ -\boldsymbol{u} \end{bmatrix} \in \mathbb{K}[x]^{(n+1)\times n} \tag{10}$$

Proof. Observe that $(\boldsymbol{v}, d) \in S_{\boldsymbol{u}}$ if and only if it satisfies the equation $\boldsymbol{v} - d\boldsymbol{u} = (\boldsymbol{v}, d)R_{\boldsymbol{u}} = 0 \bmod \mathcal{M}$, that is $(\boldsymbol{v}, d) \in \mathcal{A}_{\mathcal{M},R_{\boldsymbol{u}}}$, and if it satisfies the degree conditions equivalent to $\text{rdeg}_{\boldsymbol{s}}((\boldsymbol{v}, d)) = \max\{\deg(v_1) - N_1, \ldots, \deg(v_n) - N_n, \deg(d) - D\} < 0$ (see Def. 3.1). □

So in order to study the solutions of SRFR we introduce the $\boldsymbol{s}$-row degrees $\boldsymbol{\rho}_{\boldsymbol{u}} := \boldsymbol{\rho}_{R_{\boldsymbol{u}}}$ and the $\boldsymbol{s}$-pivot indices $\boldsymbol{\delta}_{\boldsymbol{u}} := \boldsymbol{\delta}_{R_{\boldsymbol{u}}}$ of $A_{\mathcal{M},R_{\boldsymbol{u}}}$ (see Definition 4.2). As remarked just after the *predictable degree property* (Lemma 3.2),

$$\dim_{\mathbb{K}} S_{\boldsymbol{u}} = \dim_{\mathbb{K}}(A_{\mathcal{M},R_{\boldsymbol{u}}})_{<0} = -\sum_{\rho_{\boldsymbol{u},i}<0} \rho_{\boldsymbol{u},i}. \tag{11}$$

We can now prove our main Theorem 2.4 about uniqueness in SRFR. Recall the theorem's statement: assuming $\sum_{i=1}^n f_i = \sum_{i=1}^n N_i + D - 1$ then the solution space $S_{\boldsymbol{u}}$ has dimension 1 as $\mathbb{K}$-vector space for generic $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{K}[x]^{1\times n}$.

Proof of Theorem 2.4. By the previous considerations (see (11)) it is sufficient to prove that for generic $\boldsymbol{u} \in \mathbb{K}[x]^{n+1}$, $\boldsymbol{\rho}_{\boldsymbol{u}} = (0, \ldots, 0, -1)$.

First, we need to show that the generic $\boldsymbol{s}$-row degrees $\mathbf{p}_\Sigma$ have the expected nice form $\boldsymbol{p} = (0, \ldots, 0, -1)$ ($p = -1$ and $u = n = m - 1$ because $\sum(f_j + s_j) = -1 \cdot m + (m-1)$, see (7)). It remains to check that we verify the hypotheses of Theorem 4.13. By (8), $\bar{s} \leq -1 = p$. By (9), $\sum_{i=1}^l p_i \leq 0 \leq \sum_{i=1}^l (f_i + s_i)$ for all $0 \leq l \leq m-1$ since $f_i + s_i \geq 0 \geq p_i$ for all i.

We now show that there exists $\boldsymbol{u}$ such that $R_{\boldsymbol{u}}$ satisfies the genericity condition C of Corollary 4.12. This will prove that our new genericity condition $C'(u_{j,k})$ is not the zero polynomial, where C' is $C(m_{i,j,k})$ evaluated on matrices $R_{\boldsymbol{u}}$, and $u_{j,k}$ are the polynomial coefficients of u_j. Let's show that the construction of the proof of Theorem 4.7 provides a matrix of the form $R_{\boldsymbol{u}}$ in our case $(d_1, \ldots, d_{n+1}) = (N_1, \ldots, N_n, D-1)$ and $m = n+1$. In particular, by SRFR assumptions, for any $1 \leq i \leq n$, $d_i \leq f_i$ and so the matrices $\overline{K}_i = [K(\boldsymbol{u}_i, d_i)]$ are already in Krylov form. On the other hand, the last matrix is in the form $\overline{K}_{n+1} = [K(x^{d_j}\boldsymbol{u}_j, t_j)]_{1\leq j\leq n}$ where $d_j + t_j = f_j$ (here $f_{n+1} = 0$). Then $\widetilde{K}_{n+1} = [K(\sum_{j=1}^n x^{s'_j}\boldsymbol{u}_j, d_j)]$ and we need to prove that $s'_j \geq 0$ differently because we don't have the assumption about the non-increasing $\boldsymbol{d}$. Recall that s'_j is s_j minus the number of columns added to extend the matrix to the left. This number of columns is at most d_{n+1} minus the size t_l of the current block. So $s'_l \geq d_l - (d_{n+1} - t_l) = d_l - (d_{n+1} - (f_l - d_l)) = f_l - d_{n+1} \geq 0$ because $d_{n+1} = D - 1 \leq D \leq \min(f_i)$ and so the construction works.

When $\mathbb{K}$ is a finite field of cardinality q, we want to bound the number of $\boldsymbol{u}$ such that $C'(u_{j,k}) = 0$. Recall that $u_j = \sum_{k=0}^{f_j-1} u_{j,k}x^k$ and that $C' \in \mathbb{K}[u_{j,k}]$ is a constructed as a Σ-minor of the ordered matrix $O_{R_{\boldsymbol{u}}}$ where $\Sigma = \sum_{i=1}^n f_i$. The coefficients of $O_{R_{\boldsymbol{u}}}$ are in $\mathbb{K}$, except for the $D-1$ lines corresponding to $(x^u\boldsymbol{\varepsilon}_{n+1})_{0\leq u<D-1}$ which are linear combinations of $u_{j,k}$ as mentioned in the proof of Corollary 4.12. Therefore the total degree of C' is $\leq D-1$ and we can conclude using Schwartz-Zippel Lemma that the proportion of instances leading to non-uniqueness among all possible instances is $\leq (D-1)/q$. □

REFERENCES

[BK14] B. Boyer and E. Kaltofen. Numerical linear system solving with parametric entries by error correction. In *Proceedings of SNC'14*, 2014.

[BKY03] D. Bleichenbacher, A. Kiayias, and M. Yung. Decoding of interleaved reed solomon codes over noisy data. In *Proceedings of ICALP'03*, 2003.

[BMS04] A. Brown, L. Minder, and A. Shokrollahi. Probabilistic decoding of interleaved RS-codes on the q-ary symmetric channel. In *Proceedings of ISIT'04*, 2004.

[BW86] E. Berlekamp and L. Welch. Error correction of algebraic block codes., 1986. US Patent 4,633,470.

[Cab71] S. Cabay. Exact solution of linear equations. In *Proceedings of SYMSAC'71*, 1971.

[CLO98] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, 1998.

[DF03] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Wiley, 3rd edition, 2003.

[DPS15] J.-G. Dumas, C. Pernet, and Z. Sultan. Computing the Rank Profile Matrix. In *Proceedings of ISSAC'15*, 2015.

[GG13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013.

[GLZ19] E. Guerrini, R. Lebreton, and I. Zappatore. Polynomial linear system solving with errors by simultaneous polynomial reconstruction of interleaved reed-solomon codes. In *Proceedings of ISIT'19*, 2019.

[GLZ20] E. Guerrini, R. Lebreton, and I. Zappatore. Enhancing simultaneous rational function recovery: adaptive error correction capability and new bounds for applications, 2020. Arxiv eprint 2003.01793.

[JV05] C.-P. Jeannerod and G. Villard. Essentially optimal computation of the inverse of generic polynomial matrices. *Journal of Complexity*, 21(1), 2005.

[KPSW17] E. L. Kaltofen, C. Pernet, A. Storjohann, and C. Waddell. Early termination in parametric linear system solving and rational function vector recovery with error correction. In *Proceedings of ISSAC'17*, 2017.

[Nei16] V. Neiger. *Bases of relations in one or several variables: fast algorithms and applications*. Phd thesis, ÉNS Lyon - University of Waterloo, 2016.

[OS07] Z. Olesh and A. Storjohann. The vector rational function reconstruction problem. In *Proceedings of the Waterloo Workshop*, 2007.

[Per14] C. Pernet. *High Performance and Reliable Algebraic Computing*. Habilitation à diriger des recherches, Université Joseph Fourier, Grenoble 1, 2014.

[PRN17] S. Puchinger and J. Rosenkilde né Nielsen. Decoding of interleaved reed-solomon codes using improved power decoding. In *Proceedings of ISIT'17*, 2017.

[PS07] C. Pernet and A. Storjohann. Faster Algorithms for the Characteristic Polynomial. In *Proceedings of ISSAC'07*, 2007.

[RNS16] J. Rosenkilde né Nielsen and A. Storjohann. Algorithms for simultaneous padé approximations. In *Proceedings of ISSAC'16*, 2016.

[SSB09] G. Schmidt, V. R. Sidorenko, and M. Bossert. Collaborative decoding of interleaved reed–solomon codes and concatenated code designs. *IEEE Transactions on Information Theory*, 55(7), 2009.

[Vil97] G. Villard. *A study of Coppersmith's block Wiedemann algorithm using matrix polynomials*. IMAG, 1997.