On the Uniqueness of Simultaneous Rational Function Reconstruction
Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore

To cite this version:

HAL Id: lirmm-02486922
https://hal-lirmm.ccsd.cnrs.fr/lirmm-02486922
Submitted on 21 Feb 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.
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 functions. This allows to reduce the number of evaluation points needed to guarantee the existence of a solution, but we may lose its uniqueness. In this work, we prove that uniqueness is guaranteed for a generic instance.

1 INTRODUCTION
The Vector rational function reconstruction (VRFR) is the problem of finding all rational functions \( v_i/d_i = (v_{i1}/d_{i1}, \ldots, v_{in}/d_{in}) \) which satisfy some degree constraints, given a certain number of their evaluations \( (v_i/d_i)(a_j) = \omega_j \). We consider a generalized version of this problem, where we suppose to know the images modulo different polynomials \( a_1, \ldots, a_n \), i.e. \( u_i = v_i/d \mod a_i \) for \( 1 \leq i \leq n \). The Simultaneous Rational Function Reconstruction (SRFR) problem is a particular case of the vector rational function reconstruction where the rational functions \( v_i/d_i = (v_{i1}/d_{i1}, \ldots, v_{in}/d_{in}) \) share the same denominator (see Section 2.1). We can apply the SRFR in different problems: from the decoding of classic and interleaved Reed-Solomon codes to the polynomial linear system solving. As in the classic rational function reconstruction we focus on the homogeneous linear system related to our equations in its weaker form, i.e. \( v - du \equiv 0 \mod a \). If the number of equations is equal to the number of unknowns minus one then there always exists a non-trivial solution. From now on, we will assume to be in this case. Note that the common denominator constraint of SRFR implies less unknowns than general VRFR, so less equations. This has a direct impact on the complexity of its applications. However, the uniqueness in not anymore guaranteed as shown in Counterexample 2.2. Having a unique solution is fundamental for decoding algorithms or Evaluation-Interpolation methods (like for instance in linear system solving). This paper focuses on the conditions that guarantee the uniqueness of solutions of the SRFR.

Previous works show that in the application of SRFR for polynomial linear system solving, the uniqueness is ensured under some specific degree conditions [OS07]. We have reasons to believe that we can generalize this result: we conjecture that for almost all \((v, d)\) the SRFR problem admits a unique solution (see Conjecture 2.5).

We can learn more about the conditions of uniqueness from the results coming from error correcting codes. Interleaved Reed Solomon Codes (IRS) can be seen as the evaluation of a vector of polynomials \( v \). The problem of decoding IRS codes consists in the reconstruction of the vector of polynomials \( v \) by its evaluations, some possibly erroneous. A classic approach to decode IRS codes is the application of the SRFR for instances \( u = v + e \) where \( e \) are the errors. Results from coding theory show that for all \( v \) and almost all errors \( e \), we get the uniqueness of SRFR for the corresponding instance \( u \) (provided that there are not too many errors) [BKY03, BMS04, SSB09]. There is a natural generalization of SRFR when errors occur (SRFRwE, see Section 2.2), which can be seen as fractional generalization of IRS [GLZ19, GLZ20]. We conjecture that we can decode almost all codeword \((u, d)\) and almost all errors \( e \) of this fractional code (Conjecture 2.9). In this paper we present a result which is a step towards this conjecture. We prove that uniqueness is guaranteed for a generic instance \( u \) of SRFR, (Theorem 5.2). Our result is valid not only given evaluations, but also in the general context of any moduli \( a \).

Our approach to prove Theorem 5.2 is to study the degrees of a relation module. Solutions of SRFR are related to generators of a row reduced basis of this \( \mathbb{F}[x] \)-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 the SRFR solution.

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 module of a polynomial matrix and specific matrix dimensions [JV05]. Both cases does not consider any shift. The generic degrees also appear in dimensions of blocks in a shifted Hessenberg form. However, the link with the degree of a module is unclear and no shift is discussed (shifted Hessenberg is not related to our shift) [PS07]. We prove our result for any shift and any matrix dimension by adapting some of their techniques, and by proving that they apply to the specific relation modules related to SRFR.

In Section 2 we introduce the motivations of our work, started 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 the SRFR and we finally prove the Theorem 5.2 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 \( K \) be a field, \( a, u \in K[x] \) with \( \deg(u) < \deg(a) \). The **Rational Function Reconstruction** (shortly RFR) is the problem of reconstructing a rational function \( v/d \in K(x) \) such that

\[
gcd(d, a) = 1, \quad v \equiv d\mod a, \quad \deg(v) < N, \quad \deg(d) < D. \tag{1}
\]

We focus on the weaker equation:

\[
v \equiv du \mod a, \quad \deg(v) < N, \quad \deg(d) < D. \tag{2}
\]

The RFR problem generalizes many problems including the Padé approximation if \( a = s^f \) and the Cauchy interpolation if \( a = \prod_{i=1}^{f}(x-a_i) \), where the \( a_i \) are pairwise distinct elements of the field \( K \). The homogeneous linear system related to the Equation (2) has degree \( n \) equations and \( N + D \) unknowns. If \( \deg(a) = N + D - 1 \), the dimension of the solution space of Eq. (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, \((\nu_{\min},d_{\min})\) (see e.g. [GG13, Theorem 5.16]). On the other hand, Equation (1) does not always have a solution, but when a solution exists, it is unique. Indeed, it is \( \nu_{\min}/d_{\min} \) and we can reconstruct it by the **Extended Euclidean Algorithm** (EEA). Throughout this paper, we will focus on Equation (2).

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

**Definition 2.1.** \((\text{SRFR})\) Given \( u = (u_1, \ldots, u_n) \in K[x]^n \) where \( \deg(u_i) < f_i \) and degree bounds \( 0 < N_i < f_i \) and \( 0 < D < \max_{1 \leq i \leq n} f_i \), we want to reconstruct the tuple \((v, d) = (v_1, \ldots, v_n, d)\) such that

\[
v_i \equiv d_iu_i \mod a_i, v_i \equiv N_i, d_i \equiv D_i. \tag{3}
\]

We denote \( S_u \) the set of solutions.

The SRFR is then the problem of reconstructing a vector of rational functions with the same denominator. Therefore, if \( f_i = N_i + D_i - 1 \) for \( 1 \leq i \leq n \), we can uniquely reconstruct the solution. In this case, the common denominator property allows to reduce the number of unknowns, with an impact on the degree of the \( a_i \)'s. In detail, the number of equations of (3) is \( \sum_{i=1}^{n} f_i \), while the number of the unknowns, i.e. the coefficients of \( v \) and \( d \), is \( \sum_{i=1}^{n} N_i + D_i \). If

\[
\sum_{i=1}^{n} f_i = \sum_{i=1}^{n} N_i + D_i - 1 \tag{4}
\]

then Equation (3) always admits a non-trivial solution. However, the uniqueness is not anymore guaranteed.

**Counterexample 2.2.** Let \( K = \mathbb{F}_{11}, n = 2, N_1 = N_2 = 2, D = 3 \) and \( a_1 = a_2 = \prod_{i=1}^{2}(x-i^2) = x^3 + 8x^2 + x + 2 \). Let \( u = v/d \) with \( u = (2x + 6, 8x + 2) \) and \( d = 2x^2 + 2x + 2 \) invertible modulo \( a_i \). Then the SRFR with instance \( u \) has two \( K[x] \)-linearly independent solutions \((d, v) = (4x^2 + 9x + 10, 0) \) and \((d', v') = (8x + 3, 9x + 5, 3x+9) \).

Uniqueness is a central property for the applications of SRFR: unique decoding algorithms are essential in error correcting codes, and it is also a necessary condition to use evaluation interpolation techniques in computer algebra. The study of the bound on the number of equations which guarantees the 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. So decreasing this number has a direct impact on the complexity.

We denote by \( s \) the rank of the \( K[x] \)-module spanned by the solutions \( S_u \). Therefore, 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 \( S_u \) satisfies \( s \leq k \).

Note that if \( k = 1 \), the solution is always unique (\( s = 1 \)). This matches the uniqueness condition on the \( \deg(a) \) of VRFR. On the other hand, if \( k = n \) and \( \deg(a) \geq N + (D - 1)/n \) then \( s \leq n \) which is always true. Hence in this case the theorem does not provide any new information about the solution space. This theorem represents a connection between the classic bound on the \( \deg(a) = N + D - 1 \) which guarantees the uniqueness and the \textit{ideal} one, i.e. \( \deg(a) = N + (D - 1)/n \) (see Equation (4)), which exploits the common denominator property. They also proposed an algorithm that computes a complete basis of the solution space using \( \mathcal{O}(nk^{\omega-1}B(\deg(a))) \) operations in \( \mathbb{F} \) where \( 2 \leq \omega \leq 3 \) is the exponent of the matrix multiplication and \( B(t) := M(t)\log t \) where \( M \) is the classical polynomial multiplication arithmetic complexity (see [GG13] for instance). In [RS16] the complexity was improved. In particular, they introduced an algorithm that computes the solution space (in the general case of different moduli, i.e. \( a_1, \ldots, a_n \)) with complexity \( \mathcal{O}(n^{\omega-1}B(f)(\log f / n^2)) \) where \( f = \max_{1 \leq i \leq n} \deg(a_i) \).

We now came back to general case of the SRFR. The main result of this work is to prove that when the degree constraints guarantee the existence of the solution, then for almost all \( u \) we also get the uniqueness (see Theorem 5.2).

**Theorem 2.4.** If Equation (4) is satisfied, then for almost all instances \( u \) the SRFR admits a unique solution, i.e. it has rank \( s = 1 \).

We will both use the expressions "almost all" or "generic", meaning that there exists a polynomial \( R \) such that a certain property is true for all instances that do not cancel \( R \). In our case, we state that there exists a polynomial \( R \) such that the SRFR admits a unique solution for all instances \( u \) such that \( R(u) \neq 0 \).

The SRFR problem has a natural application in a linear algebra context.

**Application to polynomial linear system solving.** Suppose that we want to compute the solution of a full rank polynomial linear system, \( y(x) = A^{-1}b \in K(x) \) where \( A \in K[x]^{n \times n} \) and \( b \in K[x]^{n \times 1} \).
from its image modulo a polynomial $a(x)$. We will refer to this problem as \textit{polynomial linear system solving} (shortly PLS). We remark that, by the Cramer’s rule, $y$ is vector of rational functions with the same denominator: PLS is then a special case of SRFR. In [OS07], the authors proved that the solution space is uniquely generated $(s = 1)$ when $\deg(a) \geq N + (D - 1)/n$ in the special case of $D = N = n \deg(A)$ and $\deg(A) = \deg(b)$. 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.

\textbf{Conjecture 2.5.} If Equation (4) is satisfied then for almost all $(\mathbf{u}, d)$ with $\gcd(d, a_1) = 1$, the SRFR with $u = \frac{\mathbf{u}}{d}$ as input admits a unique solution.

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

\subsection{Reconstruction with Errors}

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

\textbf{Definition 2.6.} (SRFR with Errors) Fix $0 < N, D, \varepsilon < f \leq q$. An instance of the SRFR with errors (SRFRwE) is a matrix $\mathbf{A} \in \mathbb{K}^{n \times f}$ whose columns are $\alpha_j = \mathbf{u}(\alpha_j)/d(\alpha_j) + e_j$ for some reduced $\mathbf{u}/d \in \mathbb{K}(x)^{n \times 1}$ and some error matrix $\mathbf{e}$. The reduced vector must satisfy $\deg(\mathbf{u}) < N$, $\deg(d) < D$ and $d(\alpha_i) \neq 0$. The error matrix must have its error support $E := \{1 \leq j \leq f \mid e_j \neq 0\}$ which satisfies $|E| \leq \varepsilon$.

The solution of the SRFRwE instance is $\mathbf{u} = (\mathbf{u}, d)$.

\textbf{SRFRwE as Reed-Solomon code decoding.} We observe that if $n = 1$ and $D = 1$, $\mathbf{u}/d$ is a polynomial. Then the SRFRwE is the problem of recovering a polynomial $\mathbf{v}$ given evaluations, some of which possibly erroneous. So in this case, SRFRwE is the problem of decoding an instance of a Reed-Solomon code.

Its vector generalization, that is $n > 1$ and $D = 1$, coincides with the decoding of an \textit{homogeneous Interleaved Reed-Solomon (IRS) code}. Indeed, an IRS codeword can be seen as the evaluation of a vector of polynomials $\mathbf{v}$ on $\alpha$. Thus decoding IRS codes is the problem of recovering $\mathbf{v}$ from $\omega_j = \mathbf{v}(\alpha_j) + e_j$.

Let us now detail how we can solve SRFRwE using SRFR. We use the same technique of decoding RS and IRS codes [BW86, BKY03, PR17]. We introduce the \textit{Error Locator Polynomial} $A = \prod_{j \in E}(x - \alpha_j)$. Its roots are the erroneous evaluations so $\deg(A) = |E| \leq \varepsilon$. We consider the \textit{Lagrangian polynomials} $u_i \in \mathbb{K}[x]$ such that $u_i(\alpha_j) = \omega_j$ for any $1 \leq i \leq n$. The classic approach is to remark that $(\varphi, \psi) = (A(x)\mathbf{v}(x), A(x)d(x))$ is a solution of

\[ \varphi = \psi u \mod \prod_{i=1}^{f}(x - \alpha_i). \quad (5) \]

In order to reconstruct $(\mathbf{u}, d)$ it suffices to study the set of $(\varphi, \psi)$ which verify Equation (5) and such that $\deg(\varphi) < N+\varepsilon$ and $\deg(\psi) < D + \varepsilon$. In this way we reduce SRFRwE to SRFR (see Eq. 3). Hence, if $f = (N + \varepsilon) + (D + \varepsilon - 1) = N + D + 2\varepsilon - 1$ we can uniquely reconstruct every component of the vector (cf. [BK14, KPSW17]).

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

\textbf{Theorem 2.7} ([BK03, BMS04, SSB09]). Fix $0 < N, \varepsilon < f \leq q$ and $E$ such that $|E| \leq \varepsilon$. If $f = N - 1 + \varepsilon + \varepsilon/n$, then for all $(\mathbf{u}, d)$ and almost all error matrices $e$ of support $E$, the SRFRwE admits a unique solution on the instance $\omega$ where $\alpha_j = (\mathbf{v}(\alpha_j))/d(\alpha_j) + e_j$.

We prove a similar result in the rational function case.

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

Since the problem of SRFRwE reduces to a simultaneous rational function reconstruction, the Equation (5) always admits a non-trivial solution 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.

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

Note that Conjecture 2.5 is for almost all fractions $(\mathbf{u}, d)$ whereas Theorems 2.7 and 2.8 are for all fractions. This difference is due to Counterexample 2.2, which states that we can not have uniqueness for all $(\mathbf{u}, d)$ when $f = N + (D - 1)/n$. This latter number of evaluations matches the one of Conjecture 2.5 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 2.5: Since uniqueness of the SRFR is true generic instance $\omega_j$, it remains to prove the existence of an instance of the form $\mathbf{v}(\alpha_j)/d(\alpha_j) + e_j$ for any $E$ such that $|E| \leq \varepsilon$ to prove the conjecture.

The SRFRwE was first introduced by [BK14] in a special case of its application, \textit{i.e.} the Polynomial Linear System Solving with Errors, that we will introduce in the following paragraph.

\textbf{Polynomial linear system solving with errors.} We now suppose that we want to compute the unique solution of a PLS $y(x) = \mathbf{v}(x)/d(x) = A^{-1}\mathbf{b} \in \mathbb{K}[x]^{n \times n}$ in a scenario where some errors occur [BK14, KPSW17, GLZ19]. In detail, we fix $f$ distinct evaluation points $\alpha = \{\alpha_1, \ldots, \alpha_f\}$ such that $d(\alpha_i) \neq 0$. In our model, we suppose that there is a black box which for any evaluation point $\alpha_i$, gives a solution of the evaluated systems of linear equations, \textit{i.e.} $y_i = A(\alpha_i)^{-1}\mathbf{b}(\alpha_i)$. However, this black box could do some errors in the computations. In particular, an evaluation $\alpha_i$ is \textit{erroneous} if $y_i \neq \mathbf{v}(\alpha_i)/d(\alpha_i)$ and we denote by $E := \{i \mid y_i \neq \mathbf{v}(\alpha_i)/d(\alpha_i)\}$ the set of erroneous positions. We refer to the problem of reconstructing the solution of a PLS in this model of errors as \textbf{Polynomial Linear System Solving with Errors} (shortly PLSwE). We observe that if $i \in E$, then there exists a nonzero $e_i \in \mathbb{K}[x]^{n \times n}$ such that $y_i = \mathbf{v}(\alpha_i)/d(\alpha_i) + e_i$. Hence, this problem is a special case
of SRF rwE. 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. Furthermore, in [KPSW17] authors introduced another bound which guaranties the uniqueness based on the bounds on the degree of the polynomial matrix $A$ and the vector $b$.

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 the definitions and lemmas of this section, and for historical references.

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

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

Definition 3.1 (Shifted row degree). Let $r_\tau = \deg(p_\tau) + s_\tau$ for $1 \leq \tau \leq \rho$. The row degree of $p$ is $\text{rdeg}(p) = \max_{1 \leq \tau \leq \rho} r_\tau$.

We also denote $p = (r_1, s_1, \ldots, r_\rho, s_\rho)$ a vector of polynomials where $r_\tau = \deg(p_\tau) + s_\tau$.

We can extend this definition to polynomial matrices. In fact, let $P \in \mathbb{K}[x]^{p \times v}$ be a polynomial matrix, with $r \leq v$. Let $P_{ij}$ be the $j$-th row of $P$ for $1 \leq j \leq \rho$. We can define the row degrees of the matrix $P$ as $\text{rdeg}_P = (r_1, \ldots, r_\rho)$ where $r_\tau = \deg(P_{\tau,j})$.

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

Our goal is to define a notion of row degrees of $N$ in order to study later the $\mathbb{K}$-vector space $N_{\text{cr}} = \{p \in N \mid \text{rdeg}_p < r\}$ for some $r \in \mathbb{N}$. Different bases $P$ of $N$ have different row degrees so we need more definitions. We start with row reduced bases.

Let $t = (t_1, \ldots, t_\rho) \in \mathbb{Z}^\rho$. We denote by $X^t$ a diagonal matrix whose entries are $x^{t_1}, \ldots, x^{t_\rho}$.

Definition 3.2 (Shifted Leading Matrix). The s-leading matrix of $P$ is a matrix in $\mathbb{K}[x]^{p \times v}$, whose entries are the coefficient of degree zero of $X^dP \mathbb{K}$.

Definition 3.3. (Row reduced basis) A basis $P \in \mathbb{K}[x]^{p \times v}$ of $N$ is row reduced (shortly s-reduced) if its leading matrix $LM_\rho(P)$ has full rank.

This definition is equivalent to [Nei16, Definition 1.10], which implies that all s-reduced bases of $N$ have the same row degree, up to permutation. We now focus on the following crucial property.

Proposition 3.4. (Predictable degree property) $P$ is s-reduced if and only if for all $\lambda = (\lambda_1, \ldots, \lambda_\rho) \in \mathbb{K}[x]^{1 \times \rho}$, $\text{rdeg}_\rho(\lambda P) = \max_{\nu \leq \rho} (\deg(\lambda_\nu) + \text{rdeg}(P_{\nu, \nu})) = \text{rdeg}(\lambda)$

where $d = \text{rdeg}(P)$.

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 $\text{dim}_{\mathbb{K}} N_{\text{cr}} = \sum (i | (r_\tau < r_\nu) \implies (r_\tau - r_\nu) = \text{the s-row degree of any s-reduced basis of } N$.

Since we will need to define the s-row degrees of $N$ uniquely, not just up to permutation, we need to introduce ordered weak Popov form, which relies on the notion of pivot.

Definition 3.5 (Pivot). Let $p \in \mathbb{K}[x]^{1 \times v}$. The s-pivot index of $p$ is $\max\{j \mid \text{rdeg}_p = \deg(p_j) + s_j\}$. Moreover the corresponding $p_j$ is the s-pivot entry and $\text{deg}(p_j)$ is the s-pivot degree of $p$.

We can naturally extend the notion of pivot to polynomial matrices.

Definition 3.6. ((Ordered) weak Popov form) The basis $P$ of $N$ in s-weak Popov form if the s-pivot indices of its rows are pairwise distinct. On the other hand, it is in s-ordered weak Popov form if the sequence of the s-pivot indices of its rows is strictly increasing.

A basis in s-weak Popov form is s-reduced. Indeed, $LM_\rho(P)$ 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 $N$ is a submodule of $\mathbb{K}[x]^v$ of rank $v$ and that $P$ is a basis of $N$ in 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 3.8 (Nei16, Lemma 1.25). Let $s \in \mathbb{Z}^\rho$ and assume $N$ is a submodule of $\mathbb{K}[x]^v$ of rank $v$. Let $P$ and $Q$ be two bases of $N$ in s-ordered weak Popov form. Then $P$ and $Q$ have the same s-row degrees and s-pivot vectors.

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 $\mathbb{K}[x] := \mathbb{K}[x_1, \ldots, x_n]$ be the ring of multivariate polynomials. Recall that a monomial in $\mathbb{K}[x]$ is a product of powers of the indeterminates $x^i := \prod x_i^{i_j}$ for some $i := (i_1, \ldots, i_n) \in \mathbb{N}^n$. On the other hand, a monomial in $\mathbb{K}[x]^n$ is $x^{e_1} e_1$, where $e_1, \ldots, e_n$ is the canonical basis of the $\mathbb{K}[x]$-module $\mathbb{K}[x]^n$.

A monomial order on $\mathbb{K}[x]^n$ is a total order $\prec$ on the monomials of $\mathbb{K}[x]^n$ such that, for any monomials $\phi e_1, \psi e_j \in \mathbb{K}[x]^n$ and any monomial $\tau \neq \phi \in \mathbb{K}[x]$, $\phi e_1 \prec \tau e_1 \iff \phi e_1 \prec \tau e_j$.

Given a monomial order $\prec$ on $\mathbb{K}[x]^n$ and $f \in \mathbb{K}[x]^n$, the $\prec$-initial term $\text{in}_\prec(f)$ 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 must be the natural degree order $x^a < x^b \iff a < b$. 

Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore
We call \( \varphi_i \prec_{s-TOP} \psi_j \) for any pairs of monomials \( \varphi_i \) and \( \psi_j \) and \( i < j \) the s-TOP ordering on \( \mathbb{K}[x] \), which induces a monomial order on \( \mathbb{K}[x] \) called s-TOP (Term Over Position):

\[
\varphi e_i \prec_{s-TOP} \psi e_j \iff (\varphi y_i \prec \psi y_j) \text{ or } (\varphi y_i = \psi y_j \text{ and } i < j)
\]

for any pairs of monomials \( \varphi e_i \) and \( \psi e_j \) in \( \mathbb{K}[x] \).

As for the univariate module \( \mathbb{K}[x]^n \), the only monomial order \( \prec \) on \( \mathbb{K}[x] \) is the natural one. The shifting monomials are \( x^d \), defined by the shift \( s = (s_1, \ldots, s_n) \in \mathbb{N}^n \), hence the s-TOP order on \( \mathbb{K}[x] \) is

\[
x^d e_i \prec_{s-TOP} x^b e_j \iff (a + s_i, i) \prec_{lex} (b + s_j, j)
\]

where \( \prec_{lex} \) is the lexicographic order on \( \mathbb{Z}^2 \).

We can now state the link between the monomial order and the pivot's definition: let \( p \in \mathbb{K}[x]^{1 \times n} \) and \( \pi_{\prec_{s-TOP}}(p) = ax^d e_i \) be the \( \prec_{s-TOP} \)-initial term of \( p \), then the 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 \( m \geq 0 \), and \( M \in \mathbb{K}[x]^{m \times n} \). We consider a \( \mathbb{K}[x] \)-submodule \( M \) of \( \mathbb{K}[x]^n \). We define the \( \mathbb{K}[x] \)-module homomorphism

\[
\varphi_M : \mathbb{K}[x]^m \rightarrow \mathbb{K}[x]^n / M
\]

\[
p \mapsto pM.
\]

Set \( A_{M,M} := \ker(\varphi_M) \) to get the injection

\[
\varphi_M : \mathbb{K}[x]^m / A_{M,M} \rightarrow \mathbb{K}[x]^n / M.
\]

We call \( A_{M,M} \) the relation module because \( p \in A_{M,M} \iff \varphi_M(p) = pM = 0 \mod M, i.e. p is a relation between rows of M.\)

Let \( e_1, \ldots, e_m \) be the canonical basis of \( \mathbb{K}[x]^m \), \( e'_1, \ldots, e'_n \) the canonical basis of \( \mathbb{K}[x]^n \) and \( e_i \equiv e_i \mod \mathbb{K}[x]^m / A_{M,M} \) 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]), \( K = \mathbb{K}[x]^m / A_{M,M} \cong \mathbb{K}[x]^n / (a_1(x)e'_1, \ldots, a_n(x)e'_n) \) for nonzero \( a_i(x) \in \mathbb{K}[x] \) such that \( a_0(x)|a_{n-1}(x) | \ldots | a_1(x) \). The polynomials \( a_i(x) \) are the invariants of the module \( M \). We denote \( \delta_i := \deg(a_i(x)) \) and we observe that \( \delta_1 \geq \delta_2 \geq \ldots \geq \delta_n \).

From now on we will assume that \( M = \left< a_1(x)e'_1, \ldots, a_n(x)e'_n \right>_{1 \leq 1 \leq n} \). It means that any \( q \in K \) can be seen as \( (q_1 \mod a_1, \ldots, q_n \mod a_n) \). Using the result of Lemma 3.8, we can define the row and pivot degrees of the relation module \( A_{M,M} \).

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

Throughout this paper we will also denote \( \rho_M \) and \( \delta_M \) when we want to stress out the matrix dependency.

4.1. Row degree 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 \( \hat{\phi}_M \). We start by associating the pivot degree of \( p \in A_{M,M} \) to linear dependency relation.

Proposition 4.3. There exists \( p \in A_{M,M} \) with s-pivot index \( i \) and s-pivot degree \( d \) if and only if \( x^d e_i \in B_{M} e_i \). Let \( B_{M} e_i := (x^d e_i | x^d e_i \prec_{s-TOP} x^d e_i) \).

Proof. Fix \( s, d \in \mathbb{N} \) and let \( p \in \mathbb{K}[x]^n \) with s-pivot index \( i \) and s-pivot degree \( d \), so \( r := \deg_x(p) = d + s \). Then \( p = (\lfloor r \rfloor_1, \ldots, \lfloor r \rfloor_{\lfloor r \rfloor_m}) \) (see Definition 3.1) and we can write \( p = c x^d e_i + p' \) where \( c \in \mathbb{K}^n \) and \( p' = (\lfloor r \rfloor_1, \ldots, \lfloor r \rfloor_{\lfloor r \rfloor_m}) \). So \( p \in A_{M,M} \) has s-pivot index \( i \) and degree \( d \) \( \iff \) \( x^d e_i = -1/c p' \mod A_{M,M} \iff \)

\[
x^d e_i \in \left( x^d e_i | n + s_j \leq d + s_i, \quad \text{for } 1 \leq j \leq i - 1 \right)
\]

\[
\text{and} \quad \left( x^d e_i | n + s_j \leq d + s_i, \quad \text{for } 1 \leq j \leq m \right) \Rightarrow B_{M} e_i \text{, } \Box
\]
We now introduce a particular family of monomials, that we will frequently use: we will denote \( F_d := \{ x^i e_j \}_{i \leq d, \, j \leq m} \) for any \( d = (d_1, \ldots, d_m) \in \mathbb{N}^m \).

This family allows us to finally relate the row rank profile of \( M_{\mathcal{L}} \) to the row degree of the relation module.

**Proposition 4.6.** The row rank profile of the ordered matrix \( M_{\mathcal{L}} \) is given by the pivot degrees \( \delta_M \) of the relation module \( \mathcal{A}_{\mathcal{M}, \mathcal{L}} \), i.e., \( RRP_M = \mathcal{F}_{\delta_M} \).

**Proof.** We fix the matrix \( M \) in order to simplify notations. We define \( \delta'_j = \min \{ \delta_i \mid x^i e_j \notin RRP \} \) and \( \delta' := (\delta'_1, \ldots, \delta'_m) \). By properties of row rank profile, we have that \( x^i e_j \in B \cdot x^j e_l \) (otherwise we could create a smaller family of linearly independent monomial with \( x^i e_j \)). Using Theorem 4.4, we deduce that \( \delta'_j \geq \delta_j \). Therefore \( \mathcal{F}_{\delta'} \subset \mathcal{F}_\delta \subset RRP \). Since the families of monomials \( \mathcal{F}_\delta \) and \( RRP \) have the same cardinality \( r = \text{rank}(M_{\mathcal{L}}) \), they are equal so \( \mathcal{F}_{\delta} = RRP \). \( \Box \)

### 4.2 Constraints on relation's row degree

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

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

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

The latter proposition 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 the proof later in Theorem 5.2. Note also that we complete the ’if’ part of the proof because it was not detailed in earlier references. For this matter, we introduce the following

**Lemma 4.8.** Let \( N \) be a \( \mathbb{K}[x] \)-submodule of \( \mathcal{K} \) of rank \( 1 \). Then the dimension of \( N \) as \( \mathbb{K} \)-vector space is at most \( f_1 + \ldots + f_l \).

**Proof.** First, remark that if \( q \in N \) has its first non-zero element at index \( p \) then \( \partial_p(x)q = 0 \). Now since \( N \) has rank \( 1 \), we can consider the matrix \( B \) whose rows are the \( l \) elements of a basis of \( N \). We operate on the rows of \( B \) to obtain the Hermite normal form \( B' \) of \( B \).

The rows \( (b'_i)_{1 \leq i \leq l} \) of \( B' \) have first non-zero elements at distinct indices \( k_1, \ldots, k_l \). Therefore \( a_{k_i}(x)b'_i = 0 \) and \( (x^i b'_i)_{1 \leq i \leq l} \) is a generating set of \( N \) and so \( \dim \mathbb{K}[x]N \leq f_{k_1} + \ldots + f_{k_l} \leq f_1 + \ldots + f_l \) since \( (f_i) \) are non increasing and \( (k_j) \) pairwise distinct. \( \Box \)

**Corollary 4.9.** Let \( r \geq 0 \), \( d \in \mathbb{N}^m \) and \( v_1, \ldots, v_l \in \mathcal{K} \) such that \( \{ x^i v_j \}_{0 \leq i < d_j} \) are linearly independent then \( \sum_{i=1}^l d_i \leq \sum_{i=1}^l f_i \).

**Proof.** We consider \( N \) the \( \mathbb{K}[x] \)-module spanned by \( \{ v_1, \ldots, v_l \} \), and we observe that \( d_1 + \ldots + d_l \leq \dim \mathbb{K}[x]N \leq f_1 + \ldots + f_l \) by Lemma 4.8. \( \Box \)

**Proof of Theorem 4.7.** We observe that if \( m > n \), we can write \( \mathcal{K} = \{ x^n/(a_j(x)e_{i_j}) \}_{1 \leq i_j \leq n} = \{ x^m/(a_j(x)e_{i_j}) \}_{1 \leq i_j \leq m} \) where \( a_j(x) = 1 \) for \( n+1 \leq j \leq m \). Hence we can suppose \( \text{w.l.o.g. that } m = n \).

By the hypotheses, there exists a matrix \( M \in \mathbb{K}[x]^{|m| \times |m|} \) such that \( \{ x^j e_j \}_{1 \leq i \leq d_j} \) are linearly independent in \( \mathcal{K} \) where \( e_j \) is \( e_j \cdot M \). Hence, for all \( 1 \leq i \leq m \), \( v_1, \ldots, v_l \) satisfy the conditions of the Corollary 4.9 and so \( \sum_{i=1}^l d_i \leq \sum_{i=1}^l f_i \).

So we can conclude that \( \{ x^j v_j \}_{1 \leq j \leq m} \) are linearly independent in \( \mathcal{K} \). We now consider the matrix \( K := [K_1 | \ldots | K_m] \) where each \( K_j \in \mathbb{K}[x]^{|m| \times f_j} \) is in the Kronecker form, that is \( K_j = K(\{ u_j \}, \{ v_j \}) := [u_j x^{k_j} \ldots x^{k_m} u_j] \) by considering \( u_j \) as a column vector. Note that \( K \) is full column rank by construction. Our goal is to find vectors \( v_1, \ldots, v_m \) such that \( K(v_1, d_1) | \ldots | K(v_m, d_m) \) is full column rank (see \( K \) later).

For this matter, we first need to consider the matrix \( K_1 \) made of columns of \( K \) so that it remains full column rank. It is defined as \( K_1 := [K_1 | \ldots | K_m] \) where for \( 1 \leq j \leq m \), \( K_j \in \mathbb{K}[x]^{|m| \times f_j} \) are defined iteratively by \( K_j := [K(\{ u_j \}, \min(f_j, d_j)) | \ldots | K(x^{k_j} u_j, t_1)] \).

We want to transform \( K_j \) into a Kronecker matrix \( \tilde{K}_j \), working by block by block. First we extend \( [K(\{ u_j \}, \min(f_j, d_j))] \) to the right to \( K(\{ u_j \}, d_j) \). Then we extend all blocks \( \ldots | K(x^{k_j} u_j, t_1) | \ldots | 0 \) to the right and the left to \( K(x^{k_j} u_j, d_j) \) such \( s_j \) equals \( s_j \) minus the number of columns of the last extension. In this way, the extension matches the original matrix on its non-zero columns. Now we can define \( \tilde{K} := [K_1 | \ldots | K_m] \), where \( \tilde{K}_j := K(v_j, d_j) \) with \( v_j := \{ u_j \} | \ldots | x^{k_j} u_j \).

A crucial point of the proof is to show that \( s_j \geq 0 \). But since \( d_j \) are not increasing, \( j_i \) are increasing and \( k_j < j_i \) we get \( s_j \geq d_j \geq s_{j_i} \geq d_{j_i} \). As the number of columns of the last extension is at most \( d_{j_i} \), we can conclude \( s_{j_i} \geq 0 \).

In [Vil97] and [PS07] it is proved that there exist an upper triangular matrices \( T \) such that \( \tilde{K} = \mathcal{RT} \). So we can conclude that \( \tilde{K} \), which is in the desired block Kronecker form, is full column rank as \( \tilde{K} \), which concludes the proof. \( \Box \)
4.3 Generic row degree of relation module

We now will show that this pivot degree constraint $d_{2r}$ is attainable by $\delta_{M}$ for matrices $M$ such that $\text{rank}(M_{0}M_{0}) = \text{rank}(q_{M}) = \text{dim}_{\mathbb{K}} \mathbb{K}[x]^{m \times n}$ in which case $q_{M}$ 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 $\delta_{M}$ of the relation module $A_{M,M}$ satisfy $\delta_{M} = d_{2r}$ where $\Sigma = \sum_{i=1}^{n} f_{i}$.

PROOF. Since $\sum_{i=1}^{n} d_{2r,i} \leq \sum_{i=1}^{n} f_{i}$ for all $1 \leq i \leq m$, we deduce from Theorem 4.7 that there exists $M \in \mathbb{K}[x]^{m \times n}$ such that $(mM)_{m} \in \mathcal{F}_{d_{2r}}$ and is non-zero for this matrix $M$. We now consider this $\Sigma$-minors as a polynomial $A$ in the coefficients of $M$. This polynomial is then nonzero since it admits a nonzero evaluation.

Now for any matrix $M = (m_{ij})$ such that $\text{rank}(m_{ij}) \neq 0$, the vectors $(m_{ij})_{m \times \mathcal{F}_{d_{2r}}}$ must be linearly independent, so $\text{rank}(M_{0}M_{0}) = \Sigma$. We have $\text{RRP}_{M} \leq_{\text{lex}} \mathcal{F}_{d_{2r}}$ because $\mathcal{F}_{d_{2r}} \in \mathcal{P}_{M}$ (see Definition 4.5).

Theorem 4.11 gives the other inequality, so $\mathcal{F}_{d_{2r}} = \text{RRP}_{M} = \mathcal{F}_{\delta_{M}}$ and $\delta_{M} = d_{2r}$. □

4.3.1 Special cases. In this section, we will see that our definition of the generic pivot degree $d_{2r}$ in Eq. (7) has a simplified expression in a wide range of settings. Set the notation $\bar{\Sigma} = \max \{ \Sigma \}$. We will see that under some assumptions the expected row degree $p_{2r} := d_{2r} + s$ has a nice form. Define $p$ and $u$ to be the quotient and remainder of the Euclidean division $\sum_{i=1}^{m} f_{i} + s = p \cdot m + u$. The expected nice form of the row degrees will be

$$p := (p + 1, \ldots, p + 1, p, \ldots, p) \quad (8)$$

This nice form of row degree will appear the following conditions on $f$ and $s$:

$$p \geq \bar{\Sigma}$$

$$\forall 1 \leq l \leq m - 1, \sum_{i=1}^{l} p_{i} \leq \sum_{i=1}^{l} (f_{i} + s_{i}) \quad (10)$$

THEOREM 4.13. Let $p$ as in Equation (8), ant let $f$ be non-increasing such that Equations (9) and (10) hold. Then $p_{2r} = p$.

This nice form of row degree was already observed in particular cases 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 $s$), and in [JV05, after Eq. (2)] for kernel bases were $m = 2n$ with no shifts.

PROOF. Denote again $\Sigma = \sum_{i=1}^{n} f_{i}$. Let $\mathcal{F}$ be the first $\Sigma$ monomials of $\mathbb{K}[x]^{m}$ for the $\Sigma_{-\text{top}}$ ordering. Let $p = (p + 1, \ldots, p + 1, p, \ldots, p)$ be the candidate row degrees as in the theorem statement and $d = p - s$ be the corresponding pivot degrees. Note that Equation (9) implies that $p \geq \bar{\Sigma}$ so $d \in \mathbb{N}^{m}$.

First we show that Equation (9) implies $\mathcal{F} = \mathcal{F}_{d}$. For the first part, in order to prove $\mathcal{F} = \mathcal{F}_{d}$, we need to show that $d_{i} \in \mathbb{N} \setminus \{ x^{k} \varepsilon_{i} \notin \mathcal{F} \}$. 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 $s$-row degree $r$ ordered increasingly for $\Sigma_{-\text{top}}$ are $[x^{k} \varepsilon_{i}]$ for increasing $1 \leq i \leq m$ such that $\sigma_{i} \leq r$. There are $m$ such monomials when $r \geq \bar{\Sigma}$. The monomials of $s$-row degree less than $\bar{\Sigma}$ are $[x^{k} \varepsilon_{i}]$ with $x^{k} \varepsilon_{i} \notin \mathcal{F}$. From this, we can deduce that the row degree of the $n$-th smallest monomial is $[(n - 1 - \sum_{i=1}^{n} (\sigma_{i} - s_{i})) / m]$. Provided that $n \geq \sum_{i=1}^{n} (\sigma_{i} - s_{i}) + 1$. We can now remark that the $(\Sigma + 1)$-th smallest monomial has a row degree $p$. More precisely, the $(\Sigma + 1)$-th smallest monomial is the $(\Sigma + 1)$-th monomial of row degree $s$, so $\mathcal{F}$ is equal to all monomials of row degree less than $p$ and the first $u$ monomials of row degree $p$. This proves $d_{i} \in \mathbb{N} \setminus \{ x^{k} \varepsilon_{i} \notin \mathcal{F} \}$ and $\mathcal{F} = \mathcal{F}_{d}$.

Second we deduce from Equation (10) that for all $1 \leq i \leq m$, $\sum_{i=1}^{l} d_{i} = \sum_{i=1}^{l} (f_{i} + s_{i}) \leq \sum_{i=1}^{l} f_{i}$, so $\mathcal{F}_{d} \leq_{\text{lex}} \mathcal{F}_{d}$ by Theorem 4.11 and finally $\mathcal{F}_{d} = \mathcal{F}_{d}$ because $\mathcal{F}$ is the smallest set of $\Sigma$ monomials. □
Example 4.14. Here we provide 3 examples of generic row pivot $d_2$ and row degree $p_2$: Corollary 4.12 applies only to the first situation because the second and third situations are made so that Eq. (9) and respectively Eq. (10) are not satisfied. Let $m = n = 3$ and $s = (0, 2, 4)$ so that $3 = 4$ and $\sum (s - s_j) = 6$.

In the first situation $f = (6, 1, 0)$, so $\sum (f_j + s_j) = 4 \ast m + 1$ and using Corollary 4.12 we get $p_2 = (5, 4, 4)$ from Eq. (8) and $d_2 = (5, 2, 0)$. In the second situation, $f = (3, 0, 0)$ and Eq. (9) is not satisfied. We use Theorem 4.13 to get $d_3 = (3, 0, 0)$ from Eq. (7) and $p_3 = (3, 2, 4)$. Finally in the third situation, $f = (3, 3, 1)$ and Eq. (10) is not satisfied. We use Theorem 4.13 to get $d_4 = (3, 3, 1)$ from Eq. (7) and $p_4 = (3, 3, 5)$. Let $F_1, F_2, F_3$ be the respective families of monomials of the three situations. We picture these monomials in the following table, where $Mon$ are the first monomials for $\langle s-TOP$.

<table>
<thead>
<tr>
<th>$Mon$</th>
<th>$e_i$</th>
<th>$Xe_1$</th>
<th>$X^2e_1$</th>
<th>$Xe_2$</th>
<th>$X^2e_2$</th>
<th>$Xe_3$</th>
<th>$X^2e_3$</th>
<th>$e_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_1$</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>$F_2$</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>$F_3$</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

5 UNIQUENESS RESULTS ON SRFR

Recall the SRFR, defined in Section 2.1. In particular, $a_1, \ldots, a_n \in \mathbb{E}[x]$ with degrees $f_i := \deg(a_i)$ and $u := (a_1, \ldots, a_n) \in \mathbb{E}[x]^n$ such that $\deg(a_i) < f_i$ and $0 < N_1 \leq f_i$ for $1 \leq i \leq n$. If $D > \min_{i \leq j \leq n} \{ f_i \}$, we want to reconstruct $(u, d) = (v_1, \ldots, v_n, d) \in \mathbb{E}[x]^{n+1}$ such that $v_i \equiv d u_i \mod a_i, \deg(v_i) < N_i, \deg(d) < D$.

We consider $M = \langle a_i(x) \rangle$ and denote by $S_n$ the set of tuples which verify Eq. (3).

Lemma 5.1. For the shift $s = (-N_1, \ldots, -N_n, -D) \in \mathbb{Z}^{n+1}$, we have $(v, d) \in S_n \Leftrightarrow (v, d) \in A_M R_u$ with $\deg_d ((v, d)) < 0$, where

$$R_u := \left[ \begin{array}{c} i_d \\ u \end{array} \right] \in \mathbb{E}[x]^{(n+1) \times n}$$

Proof. Observe that $(v, d) \in S_n$ if and only if it satisfies the equation $v - du \equiv (v, d) R_u \mod M$, that is $(v, d) \in A_M R_u$.

So in order to study the solutions of the SRFR we introduce the $s$-row degrees $P_u := \rho_{R_u}$ and the $s$-pivot indices $\delta_u := \delta_{R_u}$ of $A_{R_u} M$ (see Definition 4.2). As remarked just after the predictable degree property (Proposition 3.4),

$$\dim_S R_u = \dim_S (A_{R_u} M < 0) = - \sum_{\rho_{u_i} = 0} \rho_{u_i}.$$  

We can now show our main theorem about uniqueness in SRFR for generic instances $u$.

Theorem 5.2. Assume $\sum_{i=1}^{n} f_i = \sum_{i=1}^{n} N_i + D - 1$. Then for generic $u = (u_1, \ldots, u_n) \in \mathbb{E}[x]^n$, the solution space $S_n$ has dimension $1$ as $\mathbb{E}$-vector space.

Proof. By the previous considerations (see Eq. (12)) it is sufficient to prove that for generic $u \in \mathbb{E}[x]^{n+1}$, $P_u = (0, \ldots, 0, -1)$.

First, we need to show that the generic $s$-row degree $p_{S_u}$ is the expected nice form $p = (0, \ldots, 0, -1)$ and $n = m = m - 1$

because $\sum (f_j + s_i) = -1 - m + (m - 1)$, see Eq. (8). It remains to check that we verify the hypotheses of Theorem 4.13. By Equation (9), $\sum_{i=1}^{n} P_i = 0$. By Equation (10), $\sum_{i=1}^{n} p_i \geq \sum_{i=1}^{l} (f_i + s_i)$ for all $0 \leq l \leq m - 1$ since $f_i + s_i \geq 0, 0$ for all $i$.

It remains to show that there exists a matrix of the form $R_u$ which satisfies the genericity condition of Corollary 4.12. Hence, the genericity condition is a non-zero polynomial when evaluated on matrices $R_u$ and finally we have our result for generic $u$.

In order to do so, we show that the construction of the proof of the Theorem 4.7 provides a matrix of the form $R_u$ in our case. In our case $(d_1, \ldots, d_{n+1}) = (N_1, \ldots, N_n, D - 1)$ and $m = n + 1$, where $f_{n+1} = 0$. In particular, by SRFR assumptions, for any $1 \leq i \leq n$, $d_i = f_i$ and so the matrices $\overline{R}_i = [K(u_i, d_i)]$ are already in the Krylov form. On the other hand, the last matrix is in the form $\overline{R}_{n+1} = [K(x^d u_i, f_i)]_{1 \leq j \leq n}$ where $d_i + f_i = f_i$. Then $\overline{R}_{n+1} = [K(\sum_{j=1}^{n} x^{d_i} u_j, d_j)]$ and we need to prove that $s'_i \geq 0$ differently because we don’t have the assumption about the non-increasing $d$. Recall that $s'_i$ is $s_i$ 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 $t_1$ of the current block. So $s'_i \geq d_i - (d_{n+1} - 1) = d_i - (d_n + 1 - (f_i - d_i)) = f_i - d_{n+1} \geq 0$ because $d_{n+1} = D - 1 \leq D = \min(f_i)$ and so the construction works.

REFERENCES


