Linear feedback shift registers and the minimal realization problem

Itziar BaragañaDepartamento de Ciencia de la Computación e I.A.,
Facultad de Informática, Universidad del País Vasco, UPV/EHU [*]

Alicia RocaDepartamento de Matemática Aplicada, IMM
Universitat Politècnica València
46021 Valencia, Spain [†]

Abstract

The Berlekamp-Massey algorithm solves the problem of finding the shortest linear feedback shift register which generates a given finite sequence of scalars. This problem is reinterpreted from the point of view of the realization theory and several extensions to sequences of matrices are analyzed. We give a generalization of the result on which the Berlekamp-Massey algorithm is based in terms of the partial Brunovsky indices of a sequence of matrices and propose an algorithm to obtain them for sequences of vectors. The results we obtain hold for arbitrary fields.

Keywords: Linear feedback shift registers, partial realizations, matrix generators,Brunovsky indices.

MSC 93B15, 93C05

1 Introduction

Given a finite sequence of numbers $\mathcal{Y}^N = (y_0, y_1, \ldots, y_{N-1})$, $y_i \in \mathbb{F}$, a classical problem consists in finding the shortest linear feedback shift register (LFSR) which generates it. The Berlekamp-Massey algorithm ([7, 18]) provides an efficient solution to this problem. This algorithm and its extensions to sequences of vectors or of matrices have been widely analyzed in the literature, and solutions have been provided from different approaches, with different achievements. We summarize below some of the most important results in the area.

[*] itziar.baragana@ehu.eus

[†] aroca@mat.upv.es

A LFSR is characterized by a length L and a polynomial $C(D) = 1 + c_1D + c_2D^2 + \cdots + c_LD^L$, $c_i \in \mathbb{F}$, satisfying

$$y_j = -\sum_{i=1}^{L} c_i y_{j-i}, \quad L \leq j \leq N-1.$$

For sequences of matrices $\mathcal{Y}^N = (Y_0, Y_1, \ldots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$, the problem can be interpreted in the following ways:

Problem 1: Find a minimal length linear generator of the sequence, i.e. a polynomial of minimal length L, $C(D) = 1 + c_1D + c_2D^2 + \cdots + c_LD^L$, such that

$$Y_j = -\sum_{i=1}^{L} c_i Y_{j-i}, \quad L \leq j \leq N-1.$$

Problem 2:

2a Find a minimal length right matrix generator of the sequence, i.e. a matrix polynomial of minimal length L, $C_R(D) = I_m + R_1D + \cdots + R_LD^L \in \mathbb{F}[D]^{m\times m}$ such that

$$Y_j = Y_{j-1}R_1 + \cdots + Y_{j-L}R_L, \quad L \leq j \leq N-1.$$

2b Find a minimal length left matrix generator of the sequence.
A left matrix generator of $\mathcal{Y}^N$ is a right matrix generator of $(Y_0^T, \ldots, Y_{N-1}^T)$.

Problem 3: Find a minimal partial realization of the sequence, i.e. a matrix triple $(A, B, C) \in \mathbb{F}^{d\times d} \times \mathbb{F}^{d\times m} \times \mathbb{F}^{p\times d}$ of least possible order d such that

$$Y_j = CA^jB, \qquad 0 \leq j \leq N-1.$$

If $m = 1$ ($p = 1$), Problems 1 and 2a (2b) coincide. Moreover, solving Problem 2a (2b) is equivalent to finding a minimal realization in reduced controllability (observability) form of the sequence (hence Problem 3 will be solved).

The Berlekamp-Massey algorithm is an iterative procedure, which nests the shortest LFSR generating the sequence $\mathcal{Y}^{N-1} = (Y_0, Y_1, \ldots, Y_{N-2})$ into a new one generating the sequence $\mathcal{Y}^N = (Y_0, Y_1, \ldots, Y_{N-1})$, updating the polynomial of the register if necessary and, eventually, its length. The updating of the length is based on Theorem 2.1 (see Section 2) proved in [18]. Additionally, in [18] all of the minimal length LFSRs generating the sequence $\mathcal{Y}^N$ are provided, and uniqueness is characterized.

A proof of Massey's conjecture of the extension of Berlekamp-Massey algorithm to the multisequence case (a multisequence can be considered as a sequences of vectors) was given in [11]. The result is very close to the scheme of the original algorithm by Massey ([18]).

Other achievements in the multisequence case can be found in [20, 21, 12]. An improvement of these results is given in [1] and [2] for multisequences of the same length and of arbitrary lengths, respectively. In these papers the linear recurrence relations satisfied by the given sequences are described by the annihilator ideal of the sequences. The problem of finding the linear recurrence of minimal order for the multisequence turns then into the problem of finding a minimal Gröbner basis of the ideal. Essentially, in all these papers the problem solved is Problem 1 for $m = 1$ ($p = 1$).

Following a different approach, some results in the realization theory of linear systems led to reinterpretations of Berlekamp-Massey algorithm. In an early strategy, minimal state-space realizations of sequences were obtained from the Hankel matrix associated to the sequence ([14, 19, 13, 8, 15]). In general, minimal realizations of successively longer parts of the sequence were found, and intermediate results were nested to obtain a partial realization of a longer piece of the sequence. The updating step has been carried out, in turn, using different tools. Several authors ([10, 3]) obtained partial realizations of sequences taking advantage of matrix fraction descriptions of systems. In [3], once a partial realization is obtained, its Kronecker indices are involved in order to construct the transfer matrix of the updating step. Another approach, within the theory of linear systems, was based on the modeling of behaviors ([4, 17]).

Finally, minimal matrix generators of sequences of matrices are obtained in [22]. See also [16] for a summary of previous results.

We revisit here Problems 2 and 3 for sequences of matrices. Our approach remains within the framework of the realization theory, involving Hankel matrices and Kronecker indices of linear systems. Interesting to our work is the paper by Bosgra ([8]) who introduced the partial Kronecker indices of a sequence. They are defined in terms of ranks of Hankel matrices associated to the sequence, and it was proved in [8] that they coincide with the Kronecker indices of all minimal partial realizations of the sequence, therefore, avoiding the need of obtaining a minimal realization to compute them.

The minimal order d of a partial realization of a sequence of matrices is the sum of its partial Kronecker column (row) indices. We will see that the minimal length β (α) of a right (left) matrix generator is the largest partial Kronecker column (row) index. It results that a minimal realization is unique, modulo similarity, if and only if $\alpha + \beta \leq N$. In the scalar case, $d = \alpha = \beta$ and they coincide with the length of all the shortest LFSRs which generate the sequence. Therefore, the uniqueness condition reduces to $2d \leq N$, which is Massey's characterization of uniqueness.

In this paper we relate the partial Kronecker indices of a sequence with those of a subsequence. It allows us to generalize Theorem 2.1 (see Theorem 5.5), showing that in the matrix case the role of the minimal length of a register is split into α and β.

For the case $m = 1$ ($p = 1$), we provide a method for obtaining α and β and the partial Kronecker indices of a sequence, which allows us to find minimal realizations in reduced controllability and observability forms. From them, we also obtain minimal length right and left matrix generators of the sequence. Hence, Problems 1, 2a (2b) are solved. Concerning Problem 3, we obtain solutions in controllability and observability forms for both cases $m = 1$ and $p = 1$.

The paper is structured as follows: In Section 2 we introduce some notation, definitions and previous results. In Section 3 we review some known results about partial realizations and introduce the partial Brunovsky indices of a sequence of matrices. In Section 4 we characterize the minimal length of a matrix generator of a given sequence of matrices, and provide a method to obtain it. In Section 5 we generalize the main result of [18]. From it, we propose in Section 6 an algorithm to compute the Brunovsky indices of a sequence of vectors. In turn, from them we are able to obtain minimal realizations in controllability and observability forms, and minimum length matrix generators. The latter are shown in an example.

2 Preliminaries

Let $\mathbb{F}$ be a field. $\mathbb{F}^{n\times m}$ denotes the set of $n \times m$ matrices over $\mathbb{F}$ and $\mathbb{F}[D]^{n\times m}$ the set of polynomial matrices of size $n \times m$ with indeterminate D.

A linear feedback shift register (LFSR) of length L is a structure formed by L cells of memory $\{S_0, S_1, \dots, S_{L-1}\}$ able to store information, and provided with a clock. The initial content of the cells is denoted by $(y_0, y_1, \dots, y_{L-1})$, $y_i \in \mathbb{F}$. At each clock control the information is shifted one step sideways producing an output term, and leaving an empty cell, which is filled in with the result of a linear feedback function according to an expression of the form

$$y_j = -\sum_{i=1}^{L} c_i y_{j-i}, \quad j = L, L+1, \dots \tag{1}$$

where $y_i, c_i \in \mathbb{F}$ for $i = 0, 1, \dots$. The polynomial in the indeterminate D, $C(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_L D^L$ (D means "delay"), is associated to the LFSR and is called the connection polynomial. The LFSR is determined by the length L and the connection polynomial $C(D)$.

The Berlekamp-Massey algorithm ([18]) solves the following problem: Given a sequence of numbers $\mathcal{Y}^N = (y_0, y_1, \dots, y_{N-1})$, find a LFSR of minimal length which generates $\mathcal{Y}^N$. It is an iterative adaptive procedure which is based on the result of the next theorem, where given $\mathcal{Y} = (y_0, y_1, \dots)$, L_i denotes the length of the shortest register generating $\mathcal{Y}^i = (y_0, y_1, \dots, y_{i-1})$, for $i \geq 1$.

Theorem 2.1 [18, Theorem 2]

1. *If some LFSR of length L_N generates the sequences $\mathcal{Y}^N = (y_0, y_1, \ldots, y_{N-1})$ and $\mathcal{Y}^{N+1} = (y_0, y_1, \ldots, y_{N-1}, y_N)$, then $L_{N+1} = L_N$.*

2. *If some LFSR of length L_N generates the sequence $\mathcal{Y}^N = (y_0, y_1, \ldots, y_{N-1})$ but not the sequence $\mathcal{Y}^{N+1} = (y_0, y_1, \ldots, y_{N-1}, y_N)$, then*

$$L_{N+1} = \max\{L_N, N+1-L_N\}.$$

Additionally, in [18] all of the minimal length LFSRs generating the sequence $\mathcal{Y}^N$ are provided. It is proven that the solution is unique if and only if $2L_N \leq N$.

A LFSR can be considered as a linear generator or as a right (left) matrix generator. On the other hand, these problems are closely related to the minimal partial realization problem. Then, natural generalizations of the problem solved by the Berlekamp-Massey algorithm are Problems 1, 2 and 3 stated in the Introduction section.

In [8, Theorem 2.1] it is shown that the order d_N of the minimal partial realizations of a sequence $\mathcal{Y}^N = (Y_0, Y_1, \ldots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$, is equal to the sum of the partial Kronecker row indices and to the sum of the partial Kronecker column indices of $\mathcal{Y}^N$. In addition, if α_N and β_N are the biggest partial Kronecker row and column indices of $\mathcal{Y}^N$, respectively, then a minimal partial realization is unique modulo similarity if and only if $\alpha_N + \beta_N \leq N$.

In this paper, following [5, 6], we work with the conjugate partitions of the partial Kronecker row (column) indices and we call them *partial Brunovsky row (column) indices* of $\mathcal{Y}^N$. We will introduce them in Section 3, together with some known results about partial realizations. We will show that when $m = 1$ ($p = 1$) the problem of finding a right (left) matrix generator of $\mathcal{Y}^N$ is equivalent to that of finding a partial realization of $\mathcal{Y}^N$, and that the order d_N of all minimal partial realizations is $d_N = \beta_N$ ($d_N = \alpha_N$). Moreover, if $m = p = 1$, then both problems are equivalent to that of finding a LFSR which generates $\mathcal{Y}^N$. In this case, $d_N = \alpha_N = \beta_N$ (with the notation of Theorem 2.1, $d_N = L_N$).

For the general case, we will prove that the minimal length of the right (left) matrix generators of a given sequence of matrices is β_N (α_N) (Proposition 4.4) and we will give a method to obtain such a generator of minimal length (Corollary 4.6). Afterwards, we will analyze the relation between β_{N+1}, α_{N+1} and β_N, α_N. In particular, Theorem 5.5 generalizes Theorem 2.1, and from it we will obtain an algorithm to compute the partial Brunovsky indices of a sequence of vectors.

3 Partial realizations

In this section we will review some known results about partial realizations, and will relate the problem of finding a LFSR which generates a sequence of numbers to the problem of finding a partial realization of the sequence.

Let $(A, B, C) \in \mathbb{F}^{\delta\times\delta}\times\mathbb{F}^{\delta\times m}\times\mathbb{F}^{p\times\delta}$ be a partial realization of $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$, of order δ. If $(\overline{A}, \overline{B}, \overline{C})$ is similar to (A, B, C), i. e. $\overline{A} = T^{-1}AT$, $\overline{B} = T^{-1}B$, $\overline{C} = CT$ for some invertible matrix T, then $(\overline{A}, \overline{B}, \overline{C})$ is also a partial realization of $\mathcal{Y}^N$.

Given a triple $(A, B, C) \in \mathbb{F}^{\delta\times n} \times \mathbb{F}^{\delta\times m} \times \mathbb{F}^{p\times\delta}$, the *Brunovsky indices of controllability* of (A, B, C) are defined as follows ([9]):

$$r_i = \operatorname{rank}\mathcal{C}_i(A, B) - \operatorname{rank}\mathcal{C}_{i-1}(A, B), \quad 1 \le i \le \delta,$$

where

$$\mathcal{C}_i(A, B) = \begin{bmatrix} B & AB & \dots & A^{i-1}B \end{bmatrix}, \quad 1 \le i \le \delta,$$

and we take $\operatorname{rank}\mathcal{C}_0(A, B) := 0$.

Analogously, the *Brunovsky indices of observability* of (A, B, C) are

$$s_i = \operatorname{rank}\mathcal{O}_i(C, A) - \operatorname{rank}\mathcal{O}_{i-1}(C, A), \quad 1 \le i \le \delta,$$

where

$$\mathcal{O}_i(C, A) = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{i-1} \end{bmatrix}, \quad 1 \le i \le \delta,$$

and we take $\operatorname{rank}\mathcal{O}_0(C, A) := 0$.

Notice that $r_1 \ge \cdots \ge r_\delta \ge 0$ and $s_1 \ge \cdots \ge s_\delta \ge 0$. We take $r_i = 0$ and $s_i = 0$ for $i > \delta$.

The pair (A, B) is *controllable* if $\operatorname{rank}\mathcal{C}_\delta(A, B) = \delta$ (equivalently, if $\sum_{i=1}^{\delta} r_i = \delta$) and the pair (C, A) is *observable* if $\operatorname{rank}\mathcal{O}_\delta(C, A) = \delta$ (equivalently, if $\sum_{i=1}^{\delta} s_i = \delta$).

If (A, B, C) is a minimal partial realization of $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$, then (A, B) is controllable and (C, A) is observable.

On the other hand, two sequences of nonnegative integers can also be associated to $\mathcal{Y}^N$. We define:

$$r'_i = \operatorname{rank} H_{N+1-i,i}(\mathcal{Y}^N) - \operatorname{rank} H_{N+1-i,i-1}(\mathcal{Y}^N), \quad 1 \le i \le N,$$

$$s'_i = \operatorname{rank} H_{i,N+1-i}(\mathcal{Y}^N) - \operatorname{rank} H_{i-1,N+1-i}(\mathcal{Y}^N), \quad 1 \le i \le N,$$

where $H_{i,j}(\mathcal{Y}^N)$ is the Hankel matrix

$$H_{i,j}(\mathcal{Y}^N) = \begin{bmatrix} Y_0 & Y_1 & \dots & Y_{j-2} & Y_{j-1} \\ Y_1 & Y_2 & \dots & Y_{j-1} & Y_j \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ Y_{i-2} & Y_{i-1} & \dots & Y_{i+j-2} & Y_{i+j-1} \\ Y_{i-1} & Y_i & \dots & Y_{i+j-3} & Y_{i+j-2} \end{bmatrix}, \ 1 \leq i \leq N;\ 1 \leq j \leq N+1-i,$$

and we take $\operatorname{rank} H_{0,N}(\mathcal{Y}^N) = \operatorname{rank} H_{N,0}(\mathcal{Y}) = 0$. It is clear that $r'_i \geq r'_{i+1} \geq 0$ and $s'_i \geq s'_{i+1} \geq 0$, $1 \leq i \leq N-1$.

The sequences of integers $r'_1 \geq \cdots \geq r'_N$ and $s'_1 \geq \cdots \geq s'_N$ are called *the partial Brunovsky column and row indices* of $\mathcal{Y}^N$, respectively ([5] and [6]). They are in fact the conjugate partitions of the *the partial Kronecker column and row indices* of $\mathcal{Y}^N$ introduced by Bosgra in [8], respectively.

The following proposition can be derived from definitions.

Proposition 3.1 *Let $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$ be a sequence of matrices, $Y_i \in \mathbb{F}^{p\times m}$, and let $(r'_1, \dots, r'_N)$ and $(s'_1, \dots, s'_N$ be its partial Brunovsky column and row indices, respectively. Then*

$$\operatorname{rank} H_{N+1-i,i}(\mathcal{Y}^N) = \sum_{j=1}^{i} r'_j - \sum_{j=N+2-i}^{N} s'_j = \sum_{j=1}^{N+1-i} s'_j - \sum_{j=i+1}^{N} r'_j, \quad 1 \leq i \leq N,$$

and

$$\operatorname{rank} H_{N-i,i}(\mathcal{Y}^N) = \sum_{j=1}^{i} r'_j - \sum_{j=N+1-i}^{N} s'_j = \sum_{j=1}^{N-i} s'_j - \sum_{j=i+1}^{N} r'_j, \quad 1 \leq i \leq N-1.$$

In the next theorem we see that the partial Brunovsky indices of a given sequence of matrices and the Brunovsky indices of its minimal realizations coincide.

Theorem 3.2 [8, Th. 2.2] *Given a finite sequence of matrices $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$, all the minimal partial realizations of $\mathcal{Y}^N$ have the same Brunovsky indices of controllability and of observability, and they are equal to the partial Brunovsky column and row indices of $\mathcal{Y}^N$, respectively.*

The following proposition shows that, when the number of positive partial indices of a sequence of matrices is less than or equal to the number of matrices in the sequence, then the minimal partial realizations of the sequence are unique modulo similarity.

Proposition 3.3 [8, Th. 2.1] *Let $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$ be a sequence of matrices and let $(r_1, \dots, r_N)$, $(s_1, \dots, s_N)$ be its partial Brunovsky column and row indices, respectively. Assume that*

$$\begin{array}{l} m \geq r_1 \geq \cdots \geq r_{\beta_N} > 0 = r_{\beta_N+1} = \cdots = r_N = 0, \\ p \geq s_1 \geq \cdots \geq s_{\alpha_N} > 0 = s_{\alpha_N+1} = \cdots = s_N = 0. \end{array} \qquad (2)$$

If $\alpha_N + \beta_N \leq N$, then all the minimal partial realizations of $\mathcal{Y}^N$ are similar.

From now on, if $(r_1, \ldots, r_N)$ and $(s_1, \ldots, s_N)$ are the partial Brunovsky column and row indices of $\mathcal{Y}^N$, respectively, we will assume that they satisfy (2).

Let $(A, B, C) \in \mathbb{F}^{d_N \times d_N} \times \mathbb{F}^{d_N \times m} \times \mathbb{F}^{p \times d_N}$ be a minimal partial realization of $\mathcal{Y}^N$. Notice that by Theorem 3.2, the integers $(r_1, \ldots, r_N)$ and $(s_1, \ldots, s_N)$ are the Brunovsky indices of controllability and of observability of (A, B, C), respectively. Moreover, as (A, B) is controllable and (C, A) is observable, we have that

$$\sum_{i=1}^{N} r_i = \sum_{i=1}^{N} s_i = d_N.$$

If in addition $m = 1$, then $r_1 = \cdots = r_{\beta_N} = 1$, $d_N = \beta_N$, and since (A, B) is controllable, (A, B, C) is similar to a unique triple of the form

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & c_{\beta_N} \\ 1 & 0 & 0 & \ldots & 0 & c_{\beta_N - 1} \\ 0 & 1 & 0 & \ldots & 0 & c_{\beta_N - 2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & c_1 \end{bmatrix}, \; B = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; C = \begin{bmatrix} Y_0 & Y_1 & \ldots & Y_{\beta_N - 2} & Y_{\beta_N - 1} \end{bmatrix}.$$

Then

$$CA^j B = \sum_{i=1}^{L} c_i Y_{j-i}, \quad L \leq j \leq N - 1. \tag{3}$$

We see that in this case, the problem of finding a minimal partial realization of $\mathcal{Y}^N$ is equivalent to that of finding a right matrix generator of $\mathcal{Y}^N$.

Analogously, if $p = 1$, then $s_1 = \cdots = s_{\alpha_N} = 1$, $d_N = \alpha_N$ and the problem of finding a minimal partial realization of $\mathcal{Y}^N$ is equivalent to that of finding a left matrix generator of $\mathcal{Y}^N$.

As a consequence, in the scalar case ($m = p = 1$), the problem of finding a LFSR of minimal length which generates a given sequence $\mathcal{Y}^N$ is equivalent to that of finding a minimal partial realization of $\mathcal{Y}^N$, and to that of finding a right a left matrix generator of $\mathcal{Y}^N$.

For the general case, we will show how to obtain a partial realization of $\mathcal{Y}^N$. Although developed in another context, the result was presented in [5, Section 6] (see also [6, Section 5]), and it can be adapted to our situation. From the realization of $\mathcal{Y}^N$, we will see in the next section how to obtain a right matrix generator of the sequence. We summarize here the method.

We will use the following notation: If a and b are positive integers $0 < a \leq b$, the set of families of ordered indices of length a chosen from 1 to b is denoted by $Q_{a,b} := \{(i_1, \ldots, i_a) \; : \; 1 \leq i_1 < \cdots < i_a \leq b\}$. If $I = (i_1, \ldots, i_a) \in Q_{a,b}$ and p is an integer number, $p + I = (p + i_1, \ldots, p + i_a)$. For $A \in \mathbb{F}^{p \times m}$, $I \in Q_{s,p}$ and

$J \in Q_{r,m}$, $A(I,J)$ will denote the $s \times r$ submatrix of A formed by the rows in I and the columns in J. Similarly, $A(I,:) \in \mathbb{F}^{s\times m}$ and $A(:,J) \in \mathbb{F}^{p\times r}$ are the submatrices of A formed by the rows in I and the columns in J, respectively.

In the rest of this section, and to simplify notation, we will denote the Hankel matrices $H_{ij}(\mathcal{Y}^N)$ as H_{ij}.

From the definition of the partial Brunovsky row indices, we can select sets of indices (not necessarily unique) $I_i \in Q_{s_i,p}$, $0 \leq i \leq \alpha_N$ ($s_0 = p$), corresponding to rows of the matrix $H_{i,N-i+1}$, satisfying

$$I_{i+1} \subseteq I_i, \quad 0 \leq i \leq \alpha_N - 1,$$

and

$$\operatorname{rank} H_{i,N+1-i} = \operatorname{rank} H_{i,N+1-i}(\underline{I}_i,:), \quad 1 \leq i \leq \alpha_N,$$

where $\underline{I}_i := I_1 \cup (p + I_2) \cup \cdots \cup (i-1)p + I_i$, $1 \leq i \leq \alpha_N$.

Hence, if $I_i^c = I_{i-1} \backslash I_i$, the rows corresponding to the positions in I_i^c are linearly dependent from the rows corresponding to the positions in $\underline{I}_i$. Then there exist matrices

$$\begin{bmatrix} A_{i1} & \dots & A_{ii} \end{bmatrix} \in \mathbb{F}^{(s_{i-1}-s_i)\times(s_1+\cdots+s_i)}, \quad 1 \leq i \leq \alpha_N,$$

and a matrix $\begin{bmatrix} A_{\alpha_N+1,1} & \dots & A_{\alpha_N+1,\alpha_N} \end{bmatrix} \in \mathbb{F}^{s_{\alpha_N}\times d}$ such that

$$\begin{aligned} &\begin{bmatrix} Y_{i-1} \dots Y_{N-1} \end{bmatrix}(I_i^c,:) = \begin{bmatrix} A_{i1} \dots A_{ii} \end{bmatrix} H_{i,N-i+1}(\underline{I}_i,:), \quad 1 \leq i \leq \alpha_N, \\ &\begin{bmatrix} Y_{\alpha_N} \dots Y_{N-1} \end{bmatrix}(I_{\alpha_N},:) = \begin{bmatrix} A_{\alpha_N+1,1} \dots A_{\alpha_N+1,\alpha_N} \end{bmatrix} H_{\alpha_N,N-\alpha_N}(\underline{I}_{\alpha_N},:). \end{aligned} \tag{4}$$

(If $\alpha_N = N$, then $\begin{bmatrix} A_{\alpha_N+1,1} & \dots & A_{\alpha_N+1,\alpha_N} \end{bmatrix}$ is any matrix in $\mathbb{F}^{s_{\alpha_N}\times d}$).

Then, defining for $1 \leq i \leq \alpha_N$

$$\begin{bmatrix} C_{i1} & \dots & C_{ii} \end{bmatrix}(I_i,:) = \begin{bmatrix} 0 & \dots & I_{s_i} \end{bmatrix}, \quad \begin{bmatrix} C_{i1} & \dots & C_{ii} \end{bmatrix}(I_i^c,:) = \begin{bmatrix} A_{i1} & \dots & A_{ii} \end{bmatrix},$$

a minimal partial realization of $\mathcal{Y}^N$ is given by

$$A_o = \begin{bmatrix} C_{21} & C_{22} & 0 & \dots & 0 & 0 \\ C_{31} & C_{32} & C_{33} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ C_{\alpha_N 1} & C_{\alpha_N 2} & C_{\alpha_N 3} & \dots & C_{\alpha_N,\alpha_N-1} & C_{\alpha_N \alpha_N} \\ A_{\alpha_N+1,1} & A_{\alpha_N+1,2} & A_{\alpha_N+1,3} & \dots & A_{\alpha_N+1,\alpha_N-1} & A_{\alpha_N+1,\alpha_N} \end{bmatrix},$$

$$B_o = \begin{bmatrix} Y_0(I_1,:) \\ Y_1(I_2,:) \\ \vdots \\ Y_{\alpha_N-1}(I_{\alpha_N},:) \end{bmatrix}, \quad C_o = \begin{bmatrix} C_{11} & 0 & \dots & 0 \end{bmatrix}.$$

It is said that (A_o, B_o, C_o) is in *observability reduced form.*

Remark 3.4 *For $1 \leq i \leq \alpha_N + 1$, the number de equations in (4) is $\# I_i^c = s_{i-1} - s_i$. Then, the solution depends on*

$$(s_{i-1} - s_i)(\sum_{j=1}^{i} s_j - \operatorname{rank} H_{i,N+1-i}).$$

free parameters. By Proposition 3.1,

$$\sum_{j=1}^{i} s_j - \operatorname{rank} H_{i,N+1-i} = \sum_{j=N+2-i}^{N} r_j.$$

Therefore, the total number of free parameters in an observability reduced form is

$$n_o(\mathcal{Y}^N) = \sum_{i=1}^{\alpha_N+1} (s_{i-1}-s_i) \sum_{j=N+2-i}^{N} r_j = (s_1-s_2)r_N+(s_2-s_3)(r_{N-1}+r_N)+\cdots+s_{\alpha_N}(r_1+\cdots+r_N)$$

$$= \sum_{i=1}^{\alpha_N} s_i r_{N+1-i} = \sum_{i=N+1-\beta_N}^{\alpha_N} s_i r_{N+1-i}.$$

Analogously, we can obtain a partial realization in *controllability reduced form*, and the number total of free parameters in this case is

$$n_c(\mathcal{Y}^N) = \sum_{j=1}^{\beta_N+1} (r_{i-1} - r_i) \sum_{j=N+2-i}^{n} s_j = \sum_{i=N+1-\alpha_N}^{\beta_N} r_i s_{N+1-i} = n_o(\mathcal{Y}^N).$$

We observe that the number of free parameters in the reduced forms is the same. Moreover, if $\alpha_N + \beta_N \leq N$, then $n_o(\mathcal{Y}^N) = n_c(\mathcal{Y}^N) = 0$, which means that once the sets of indices I_i, J_i are fixed, the reduced forms are unique.

Example 3.5 *Let $p = 4$, $m = 2$, $\mathcal{Y}^5 = (Y_0, Y_1, Y_2, Y_3, Y_4)$ with $\alpha_5 = 3$, $\beta_5 = 4$, Assume that*

$$(s_1, s_2, s_3) = (3, 1, 1), \quad (r_1, r_2, r_3, r_4) = (2, 1, 1, 1),$$

and $I_1 = \{1, 2, 4\}, I_2 = I_3 = \{2\}$, i.e. (notice that $p + I_2 = \{6\}$, $2p + I_3 = \{10\}$)

$\operatorname{rank} H_{1,5}(\mathcal{Y}^5) = \operatorname{rank} H_{1,5}(\mathcal{Y}^5)(\{1, 2, 4\}, :) = s_1 = 3,$
$\operatorname{rank} H_{2,4}(\mathcal{Y}^5) = \operatorname{rank} H_{2,4}(\mathcal{Y}^5)(\{1, 2, 4, 6\}, :) = s_1 + s_2 - r_5 = 4,$
$\operatorname{rank} H_{3,3}(\mathcal{Y}^5) = \operatorname{rank} H_{3,3}(\mathcal{Y}^5)(\{1, 2, 4, 6, 10\}, :) = s_1 + s_2 + s_3 - r_5 - r_4 = 4,$
$\operatorname{rank} H_{4,2}(\mathcal{Y}^5) = \operatorname{rank} H_{4,2}(\mathcal{Y}^5)(:, \{1, 2, 4, 6, 10\}, :) = s_1 + s_2 + s_3 + s_4 - r_5 - r_4 - r_3 = 3,$

and there exist $a_{ij} \in \mathbb{F}$ such that ($I_1^c = \{1, 2, 3, 4\} \setminus \{1, 2, 4\} = \{3\}, I_2^c = I_1 \setminus I_2 = \{1, 4\}, I_3^c = I_2 \setminus I_3 = \emptyset$)

$$\begin{bmatrix} Y_0 & Y_1 & \dots & Y_4 \end{bmatrix} (3, :) = \begin{bmatrix} a_{31} & a_{32} & a_{33} \end{bmatrix} H_{1,5}(\mathcal{Y}^5)(\{1, 2, 4\}, :),$$

$$\begin{bmatrix} Y_1 & \dots & Y_4 \end{bmatrix} (\{1, 4\}, :) = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} H_{2,4}(\mathcal{Y}^5)(\{1, 2, 4, 6\}, :),$$

$$\begin{bmatrix} Y_3 & Y_4 \end{bmatrix} (\{2\}, :) = \begin{bmatrix} a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \end{bmatrix} H_{3,2}(\mathcal{Y}^5)(\{1, 2, 4, 6, 8\}, :)$$

Then a minimal partial realization of $\mathcal{Y}^5$ in observability reduced form is

$$A_o = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & 0 \\ 0 & 0 & 0 & 1 & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} & 0 \\ 0 & 0 & 0 & 0 & 1 \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \end{bmatrix}, \; B_o = \begin{bmatrix} Y_0(\{1,2,4\},:) \\ Y_1(\{2\},:) \\ Y_2(\{2\},:) \end{bmatrix}, \; C_o = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Similarly, if $J_1 = \{1,2\}$, $J_2 = J_3 = J_4 = \{1\}$, a minimal partial realization of $\mathcal{Y}^5$ in controllability reduced form is

$$A_c = \begin{bmatrix} 0 & b_{12} & 0 & 0 & b_{11} \\ 0 & b_{22} & 0 & 0 & b_{21} \\ 1 & b_{32} & 0 & 0 & b_{31} \\ 0 & 0 & 1 & 0 & b_{41} \\ 0 & 0 & 0 & 1 & b_{51} \end{bmatrix}, \; B_c = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \; C_c = \begin{bmatrix} Y_0 & Y_1(:,\{1\}) & Y_2(:,\{1\}) & Y_3(:,\{1\}) \end{bmatrix}.$$

□

4 Matrix generators

In this section we deal with the problem of finding a right matrix generator of $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$, $Y_i \in \mathbb{F}^{p\times m}$. Obviously, analogous results can be obtained for left matrix generators.

Recall that when $m = 1$, the problem is equivalent to that of finding a minimal partial realization of $\mathcal{Y}^N$.

For the general case, we observe first that the problem can also be stated in terms of partial realizations.

Proposition 4.1 *$C_R(D) = I_m + R_1 D + \cdots + R_\rho D^\rho \in \mathbb{F}[D]^{m\times m}$ is a right matrix generator of $\mathcal{Y}^N$ if and only if*

$$A_R = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & R_\rho \\ I_m & 0 & 0 & \dots & 0 & R_{\rho-1} \\ 0 & I_m & 0 & \dots & 0 & R_{\rho-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & I_m & R_1 \end{bmatrix}, \; B_R = \begin{bmatrix} I_m \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; C_R = \begin{bmatrix} Y_0 & Y_1 & \dots & Y_{\rho-1} \end{bmatrix}$$

is a partial realization of $\mathcal{Y}^N$.

Proof. Defining

$$Z_j := Y_j, \quad 0 \le j \le Y_{\rho-1},$$

$$Z_j := Z_{j-1}R_1 + \cdots + Z_{j-\rho}R_\rho, \quad N \le j \le N + \rho - 2,$$

we have

$$\begin{bmatrix} C_R \\ C_R A_R \\ \vdots \\ C_R A_R^{N-1} \end{bmatrix} = \begin{bmatrix} Z_0 & Z_1 & \dots & Z_{\rho-1} \\ Z_1 & Z_2 & \dots & Z_\rho \\ \vdots & \vdots & \ddots & \vdots \\ Z_{N-1} & Z_N & \dots & Z_{N+\rho-2} \end{bmatrix},$$

therefore,

$$\begin{bmatrix} C_R B_R \\ C_R A_R B_R \\ \vdots \\ C_R A_R^{N-1} B_R \end{bmatrix} = \begin{bmatrix} C_R \\ C_R A_R \\ \vdots \\ C_R A_R^{N-1} \end{bmatrix} B_R = \begin{bmatrix} Z_0 \\ Z_1 \\ \vdots \\ Z_{N-1} \end{bmatrix}.$$

Then, $C_R(D)$ is a right matrix generator of $\mathcal{Y}^N$ if and only if

$$Y_j = Z_j = C_R A_R^j B_R, \quad \rho \leq j \leq N-1.$$

□

For a given ρ, the following results characterize the existence of a right matrix generator of length ρ of $\mathcal{Y}^N$ and provide us with a method to obtain it.

Proposition 4.2 *There exists a right matrix generator $C_R(D) \in \mathbb{F}[D]^{m\times m}$ of length ρ of $\mathcal{Y}^N$ if and only if*

$$\operatorname{rank} H_{N-\rho,\rho+1}(\mathcal{Y}^N) = \operatorname{rank} H_{N-\rho,\rho}(\mathcal{Y}^N). \tag{5}$$

Proof. There exists a right matrix generator if and only if there exist matrices $R_1, \dots, R_\rho \in \mathbb{F}^{m\times m}$ such that

$$Y_j = Y_{j-1}R_1 + \cdots + Y_{j-\rho}R_\rho, \quad \rho \leq j \leq N-1,$$

if and only if

$$\operatorname{rank} \begin{bmatrix} Y_0 & Y_1 & \dots & Y_{\rho-1} & Y_\rho \\ Y_1 & Y_2 & \dots & Y_\rho & Y_{\rho+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Y_{N-\rho-1} & Y_{N-\rho} & \dots & Y_{N-2} & Y_{N-1} \end{bmatrix} = \operatorname{rank} \begin{bmatrix} Y_0 & Y_1 & \dots & Y_{\rho-1} \\ Y_1 & Y_2 & \dots & Y_\rho \\ \vdots & \vdots & \ddots & \vdots \\ Y_{N-\rho-1} & Y_{N-\rho} & \dots & Y_{N-2} \end{bmatrix}.$$

□

Proposition 4.3 *If (5) holds, then a right matrix generator of Y^N is $C_R(D) = I_m + R_1 D + \cdots + R_\rho D^\rho$, where $R_1, \dots, R_\rho \in \mathbb{F}^{m\times m}$ are matrices such that*

$$H_{n-\rho,\rho}(\mathcal{Y}^N) \begin{bmatrix} R_\rho \\ \vdots \\ R_1 \end{bmatrix} = H_{n-\rho,\rho+1}(\mathcal{Y}^N).$$

Proof. Straightforward. □

Recall that the partial Brunovsky column indices of $\mathcal{Y}^N$ are

$$r_1 \geq \cdots \geq r_{\beta_N} > 0 = r_{\beta_N+1} = \cdots = r_N = 0,$$

and that

$$r_i = \operatorname{rank} H_{N+1-i,i}(\mathcal{Y}^N) - \operatorname{rank} H_{N+1-i,i-1}(\mathcal{Y}^N), \quad 1 \leq i \leq N.$$

Then, condition (5) is equivalent to $r_{\rho+1} = 0$. As a consequence, if we denote by g_N the minimal length of the right matrix generators of $\mathcal{Y}^N$, we have the following characterization of g_N.

Proposition 4.4 *The minimal length g_N of the right matrix generators of $\mathcal{Y}^N$ is $g_N = \beta_N$.*

Once β_N is calculated, Proposition 4.3 allows us to obtain a right matrix generator of minimal length.

Nevertheless, instead of using Proposition 4.3, we show next another method to obtain a minimal length right matrix generator of $\mathcal{Y}^N$, taking advantage of a minimal partial realization of the sequence.

Let (A, B, C) be a minimal partial realization of $\mathcal{Y}^N$. By Theorem 3.2, the Brunovsky indices of controllability of (A, B, C) are $r_1 \geq \cdots \geq r_{\beta_N} > 0 = r_{\beta_N+1} = \cdots = r_N = 0$. Then,

$$0 = r_{\beta_N+1} = \operatorname{rank} \mathcal{C}_{\beta_N+1}(A, B) - \operatorname{rank} \mathcal{C}_{\beta_N}(A, B),$$

it implies that there there exist $R_1, \ldots, R_{\beta_N} \in \mathbb{F}^{m\times m}$ such that

$$A^{\beta_N} B = \mathcal{C}_{\beta_N}(A, B) \begin{bmatrix} R_{\beta_N} \\ \vdots \\ R_1 \end{bmatrix}. \tag{6}$$

Proposition 4.5 *Let (A, B, C) be a minimal partial realization of $\mathcal{Y}^N$ and let $R_1, \ldots, R_{\beta_N} \in \mathbb{F}^{m\times m}$ be matrices satisfying (6). Then*

$$A_R = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & R_{\beta_N} \\ I_m & 0 & 0 & \ldots & 0 & R_{\beta_N-1} \\ 0 & I_m & 0 & \ldots & 0 & R_{\beta_N-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & I_m & R_1 \end{bmatrix}, \; B_R = \begin{bmatrix} I_m \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; C_R = \begin{bmatrix} Y_0 & Y_1 & \ldots & Y_{\beta_N-1} \end{bmatrix}$$

is a partial realization of $\mathcal{Y}$.

Proof. First, let us prove by induction on i that

$$A^i\mathcal{C}_{\beta_N}(A,B) = \mathcal{C}_{\beta_N}(A,B)A_R^i, \quad i \geq 0. \tag{7}$$

For $i=0$, (7) trivially holds. Assume now that $A^k\mathcal{C}_{\beta_N}(A,B) = \mathcal{C}_{\beta_N}(A,B)A_R^k$. By (6) and the definition of A_R, $\mathcal{C}_{\beta_N}(A,B)A_R = \begin{bmatrix} AB & A^2B & \dots & A^{\beta_N}B \end{bmatrix}$. Thus,

$$A^{k+1}\mathcal{C}_{\beta_N}(A,B) = A\mathcal{C}_{\beta_N}(A,B)A_R^k = \begin{bmatrix} AB & A^2B & \dots & A^{\beta_N}B \end{bmatrix} A_R^k = \mathcal{C}_{\beta_N}(A,B)A_R^{k+1}.$$

On the other hand, since (A,B,C) is a partial realization of $\mathcal{Y}^N$, $C_R = C\mathcal{C}_{\beta_N}(A,B)$. Then, from (7) we deduce

$$C_RA_R^iB_R = C\mathcal{C}_{\beta_N}(A,B)A_R^iB_R = CA^i\mathcal{C}_{\beta_N}(A,B)\begin{bmatrix} I_m \\ 0 \\ \vdots \\ 0 \end{bmatrix} = CA^iB = Y_i, \quad 0 \leq i \leq N-1.$$

□

Now, from Proposition 4.1 we obtain the next result.

Corollary 4.6 *Let (A,B,C) be a minimal partial realization of $\mathcal{Y}^N$. Then a right matrix generator of minimal length of Y^N is $C_R(D) = I_m + R_1D + \cdots + R_{\beta_N}D^{\beta_N}$, where $R_1, \dots, R_{\beta_N} \in \mathbb{F}^{m\times m}$ are matrices satisfying (6).*

Example 4.7 *With the data of Example 3.5, a right matrix generator of minimal length of $\mathcal{Y}^5$ is $C(D) = 1 + R_1D + R_2D^2 + R_3D^3 + R_4D^4$ where $R_i \in \mathbb{F}^{2\times 2}$ are matices such that*

$$A_c^4B_c = \mathcal{C}_4(A_c,B_c)\begin{bmatrix} R_4 \\ R_3 \\ R_2 \\ R_1 \end{bmatrix}.$$

Let b_1, b_2 be the columns of B_c. Then

$$A_c^4b_1 = \begin{bmatrix} b_1 & b_2 & A_cb_1 & A_c^2b_1 & A_c^3b_1 \end{bmatrix}\begin{bmatrix} b_{11} \\ b_{21} \\ b_{31} \\ b_{41} \\ b_{51} \end{bmatrix} = C_4(A_c,B_c)X_1, \text{ where } X_1 = \left[\begin{array}{c} b_{11} \\ b_{21} \\ \hline b_{31} \\ 0 \\ \hline b_{41} \\ 0 \\ \hline b_{51} \\ 0 \end{array}\right].$$

$$A_cb_2 = \begin{bmatrix} b_1 & b_2 & A_cb_1 \end{bmatrix}\begin{bmatrix} b_{12} \\ b_{22} \\ b_{32} \end{bmatrix}, \text{ from where } A_c^4b_2 = \begin{bmatrix} A_c^3b_1 & A_c^3b_2 & A_c^4b_1 \end{bmatrix}\begin{bmatrix} b_{12} \\ b_{22} \\ b_{32} \end{bmatrix}.$$

Then

$$A_c^4 b_2 = \begin{bmatrix} A_c^3 b_1 & A_c^3 b_2 \end{bmatrix} \begin{bmatrix} b_{12} \\ b_{22} \end{bmatrix} + A_c^4 b_1 b_{32} = \mathcal{C}_4(A_c, B_c) X_2, \text{ where } X_2 = \left[\begin{array}{c} 0 \\ 0 \\ \hline 0 \\ 0 \\ \hline 0 \\ 0 \\ \hline b_{12} \\ b_{22} \end{array}\right] + X_1 b_{32}.$$

Let

$$\begin{bmatrix} R_4 \\ R_3 \\ R_2 \\ R_1 \end{bmatrix} := \begin{bmatrix} X_1 & X_2 \end{bmatrix} = \left[\begin{array}{cc} b_{11} & b_{11} b_{32} \\ b_{21} & b_{21} b_{32} \\ \hline b_{31} & b_{31} b_{32} \\ 0 & 0 \\ \hline b_{41} & b_{41} b_{32} \\ 0 & 0 \\ \hline b_{51} & b_{12} + b_{51} b_{32} \\ 0 & b_{22} \end{array}\right],$$

Then, $C(D) = 1 + R_1 D + R_2 D^2 + R_3 D^3 + R_4 D^4$ *is a right matrix generator of minimal length of* $\mathcal{Y}^5$*.* □

5 Partial indices of sequences and subsequences

Our aim in this section is to generalize Theorem 2.1. To achieve it, we study the relation between the partial indices of a sequence $Y^{N+1} = (Y_0, \dots, Y_N)$, $Y_i \in \mathbb{F}^{p \times m}$, and those of the subsequence $\mathcal{Y}^N = (Y_0, \dots, Y_{N-1})$.

The next lemma follows from Proposition 3.1.

Lemma 5.1 *Let* $\mathcal{Y}^n = (Y_0, \dots, Y_{n-1})$ *be a sequence of matrices and let* $(r_1, \dots, r_n)$ *and* $(s_1, \dots, s_n)$ *be its partial Brunovsky column and row indices, respectively. Then*

1.

$$r_i - s_{n+1-i} = \operatorname{rank} H_{n-i,i}(\mathcal{Y}^n) - \operatorname{rank} H_{n+1-i,i-1}(\mathcal{Y}^n), \quad 1 \le i \le n.$$

2.

$$r_i - s_{n+2-i} = \operatorname{rank} H_{n+1-i,i}(\mathcal{Y}^n) - \operatorname{rank} H_{n+2-i,i-1}(\mathcal{Y}^n), \quad 2 \le i \le n.$$

In the rest of the section, $\mathcal{Y} = (Y_0, Y_1, \dots,)$, $Y_i \in \mathbb{F}^{p \times m}$, will be a sequence of matrices and for $i \ge 1$ we will denote by $(r_1^i, \dots, r_i^i)$ and $(s_1^i, \dots, s_i^i)$ the partial

Brunovsky column and row indices of $\mathcal{Y}^i = (Y_0, \dots, Y_{i-1})$, respectively. We will assume that

$$m \geq r_1^i \geq \cdots \geq r_{\beta_i}^i > 0 = r_{\beta_i+1}^i = \cdots = r_i^i = 0,$$

$$p \geq s_1^i \geq \cdots \geq s_{\alpha_i}^i > 0 = s_{\alpha_i+1}^i = \cdots = s_i^i = 0,$$

$$\sum_{j=1}^{i} r_j^i = \sum_{j=1}^{i} s_j^i = d_i.$$

Proposition 5.2

1.

$$r_i^{N+1} \geq r_i^N, \quad s_i^{N+1} \geq s_i^N, \quad 1 \leq i \leq N+1 \quad (r_{N+1}^N = s_{N+1}^N = 0),$$

and as a consequence,

$$\alpha_{N+1} \geq \alpha_N, \quad \beta_{N+1} \geq \beta_N.$$

2.

$$r_i^{N+1} = r_i^N + s_{N+2-i}^{N+1} - s_{N+2-i}^N, \quad 1 \leq i \leq N+1. \tag{8}$$

Equivalently,

$$s_i^{N+1} = s_i^N + r_{N+2-i}^{N+1} - r_{N+2-i}^N, \quad 1 \leq i \leq N+1. \tag{9}$$

Proof.

1. For $1 \leq i \leq N+1$, let us consider the matrix

$$H_{N+2-i,i}(\mathcal{Y}^{N+1}) = \begin{bmatrix} Y_0 & \dots & Y_{i-2} & Y_{i-1} \\ \vdots & \ddots & \vdots & \\ Y_{N-i} & \dots & Y_{N-2} & Y_{N-1} \\ Y_{N+1-i} & \dots & Y_{N-1} & Y_N \end{bmatrix}.$$

Observe that r_i^{N+1} is the number of independent columns of the last block column $\begin{bmatrix} Y_{i-1} \\ Y_i \\ \vdots \\ Y_{N-1} \\ Y_N \end{bmatrix}$ which are linearly independent from the previous ones, that is, from the columns of $H_{N+2-i,i-1}(\mathcal{Y}^{N+1})$. In the same way, for $1 \leq i \leq N$, r_i^N is the number of independent columns of $\begin{bmatrix} Y_{i-1} \\ Y_i \\ \vdots \\ Y_{N-1} \end{bmatrix}$

which are linearly independent from the columns of $H_{N+1-i,i-1}(\mathcal{Y}^N)$.

Notice that if a column of $\begin{bmatrix} Y_{i-1} \\ Y_i \\ \vdots \\ Y_{N-1} \\ Y_N \end{bmatrix}$ depends linearly on the columns of $H_{N+2-i,i-1}(\mathcal{Y}^{N+1})$, then the same column in $\begin{bmatrix} Y_{i-1} \\ Y_i \\ \vdots \\ Y_{N-1} \end{bmatrix}$ depends linearly on the columns of $H_{N+1-i,i-1}(\mathcal{Y}^N)$. Thus, $m - r_i^N \geq m - r_i^{N+1}$, therefore $r_i^{N+1} \geq r_i^N$. Analogously, $s_i^{N+1} \geq s_i^N$, $1 \leq i \leq N$.

2. By Lemma 5.1, for $1 \leq i \leq N+1$,

$$r_i^{N+1} - s_{N+2-i}^{N+1} = \operatorname{rank} H_{N+1-i,i}(\mathcal{Y}^{N+1}) - \operatorname{rank} H_{N+2-i,i-1}(\mathcal{Y}^{N+1}).$$

But $H_{N+1-i,i}(\mathcal{Y}^{N+1}) = H_{N+1-i,i}(\mathcal{Y}^N)$ and $H_{N+2-i,i-1}(\mathcal{Y}^{N+1}) = H_{N+2-i,i-1}(\mathcal{Y}^N)$. Therefore

$$r_i^{N+1} - s_{N+2-i}^{N+1} = \operatorname{rank} H_{N+1-i,i}(\mathcal{Y}^N) - \operatorname{rank} H_{N+2-i,i-1}(\mathcal{Y}^N) = r_i^N - s_{N+2-i}^N.$$

□

Corollary 5.3 *If $\alpha_N + \beta_N \leq N$, then*

1. *If $r_{\beta_N}^{N+1} = r_{\beta_N}^N$ then $r_i^{N+1} = r_i^N$, $1 \leq i \leq \beta_N$. Similarly, if $s_{\alpha_N}^{N+1} = s_{\alpha_N}^N$ then $s_i^{N+1} = s_i^N$, $1 \leq i \leq \alpha_N$.*
2. *$r_{\beta_N+1}^{N+1} = \cdots = r_{N+1-\alpha_N}^{N+1} = s_{\alpha_N+1}^{N+1} = \cdots = s_{N+1-\beta_N}^{N+1}$.*
3. *$\alpha_{N+1} = \alpha_N$ if and only if $\beta_{N+1} = \beta_N$. In this case*

$$r_i^{N+1} = r_i^N, \quad 1 \leq i \leq \beta_N, \quad \text{and} \quad s_i^{N+1} = s_i^N, \quad 1 \leq i \leq \alpha_N.$$

4. *$\alpha_{N+1} > \alpha_N$ if and only if $\beta_{N+1} > \beta_N$. In this case*

$$\alpha_{N+1} \geq N + 1 - \beta_N, \quad \beta_{N+1} \geq N + 1 - \alpha_N.$$

5. *If $\alpha_{N+1} > \alpha_N$ and $r_{\beta_N}^{N+1} = r_{\beta_N}^N$, then $\alpha_{N+1} = N + 1 - \beta_N$. Similarly, if $\beta_{N+1} > \beta_N$ and $s_{\alpha_N}^{N+1} = s_{\alpha_N}^N$, then $\beta_{N+1} = N + 1 - \alpha_N$.*
6. *If $\alpha_{N+1} > \alpha_N$ and $r_{\beta_N}^N = m$, then $\alpha_{N+1} = N + 1 - \beta_N$. Similarly, if $\beta_{N+1} > \beta_N$ and $s_{\alpha_N}^N = p$, then $\beta_{N+1} = N + 1 - \alpha_N$.*

Proof. If $\alpha_N + \beta_N \le N$, conditions (8)-(9) are

$$r_i^{N+1} = \begin{cases} r_i^N + s_{N+2-i}^{N+1}, & 1 \le i \le \beta_N, \\ s_{N+2-i}^{N+1}, & \beta_N + 1 \le i \le N+1-\alpha_N, \\ s_{N+2-i}^{N+1} - s_{N+2-i}^N, & N+2-\alpha_N \le i \le N+1, \end{cases}$$

$$s_i^{N+1} = \begin{cases} s_i^N + r_{N+2-i}^{N+1}, & 1 \le i \le \alpha_N, \\ r_{N+2-i}^{N+1}, & \alpha_N + 1 \le i \le N+1-\beta_N, \\ r_{N+2-i}^{N+1} - r_{N+2-i}^N, & N+2-\beta_N \le i \le N+1. \end{cases}$$

1. If $r_{\beta_N}^{N+1} = r_{\beta_N}^N$,

   $$0 \le r_i^{N+1} - r_i^N = s_{N+2-i}^{N+1} \le s_{N+2-\beta_N}^{N+1} = r_{\beta_N}^{N+1} - r_{\beta_N}^N = 0, \quad 1 \le i \le \beta_N.$$

2. We have that $s_{N+1-\beta_N}^{N+1} = r_{\beta_N+1}^{N+1} \ge r_{N+1-\alpha_N}^{N+1} = s_{\alpha_N+1}^{N+1} \ge s_{N+1-\beta_N}^{N+1}$, hence

   $$r_{\beta_N+1}^{N+1} = r_{N+1-\alpha_N}^{N+1} = s_{\alpha_N+1}^{N+1} = s_{N+1-\beta_N}^{N+1}.$$

3. By item 2,

   $$\alpha_{N+1} = \alpha_N \Leftrightarrow s_{\alpha_N+1}^{N+1} = 0 \Leftrightarrow r_{\beta_N+1}^{N+1} = 0 \Leftrightarrow \beta_{N+1} = \beta_N.$$

   In this case, $s_{N+2-i}^{N+1} = 0$ for $1 \le i \le \beta_N$, and $r_{N+2-i}^{N+1} = 0$ for $1 \le i \le \alpha_N$.

4. It follows from items 3 and 2.
5. It follows from item 4 and $s_{N+2-\beta_N}^{N+1} = r_{\beta_N}^{N+1} - r_{\beta_N}^N = 0$.
6. If follows from item 5, bearing in mind that $m \ge r_{\beta_N}^{N+1} \ge r_{\beta_N}^N$.

□

Corollary 5.4 *If $N < \alpha_N + \beta_N$, then*

1. *If $r_{N+1-\alpha_N}^{N+1} = r_{N+1-\alpha_N}^N$, then $r_i^{N+1} = r_i^N$, $1 \le i \le N+1-\alpha_N$. Similarly, if $s_{N+1-\beta_N}^{N+1} = s_{N+1-\beta_N}^N$ then $s_i^{N+1} = s_i^N$, $1 \le i \le N+1-\beta_N$.*
2. *$\beta_{N+1} > \beta_N$ if and only if $s_{N+1-\beta_N}^{N+1} > s_{N+1-\beta_N}^N$ and $\alpha_{N+1} > \alpha_N$ if and only if $r_{N+1-\alpha_N}^{N+1} > r_{N+1-\alpha_N}^N$.*
3. *If $s_{N+1-\beta_N}^N = p$ then $\beta_{N+1} = \beta_N$. Similarly, if $r_{N+1-\alpha_N}^N = m$, then $\alpha_{N+1} = \alpha_N$.*

Proof. If $N < \alpha_N + \beta_N$, conditions (8)-(9) are

$$r_i^{N+1} = \begin{cases} r_i^N + s_{N+2-i}^{N+1}, & 1 \leq i \leq N+1-\alpha_N, \\ r_i^N + s_{N+2-i}^{N+1} - s_{N+2-i}^N, & N+2-\alpha_N \leq i \leq \beta_N, \\ s_{N+2-i}^{N+1} - s_{N+2-i}^N, & \beta_N + 1 \leq i \leq N+1, \end{cases}$$

$$s_i^{N+1} = \begin{cases} s_i^N + r_{N+2-i}^{N+1}, & 1 \leq i \leq N+1-\beta_N, \\ s_i^N + r_{N+2-i}^{N+1} - r_{N+2-i}^N, & N+2-\beta_N \leq i \leq \alpha_N, \\ r_{N+2-i}^{N+1} - r_{N+2-i}^N, & \alpha_N + 1 \leq i \leq N+1. \end{cases}$$

(If $\alpha_N + \beta_N = N+1$, the second condition vanishes).

1. If $r_{N+1-\alpha_N}^{N+1} = r_{N+1-\alpha_N}^N$, then

   $$0 \leq r_i^{N+1} - r_i^N = s_{N+2-i}^{N+1} \leq s_{\alpha_N+1}^{N+1} = r_{N+1-\alpha_N}^{N+1} - r_{N+1-\alpha_N}^N = 0, \quad 1 \leq i \leq N+1-\alpha_N.$$

2. $$\beta_{N+1} > \beta_N \Leftrightarrow r_{\beta_N+1}^{N+1} > 0 \Leftrightarrow s_{N+1-\beta_N}^{N+1} - s_{N+1-\beta_N}^N > 0.$$

3. It follows from item 2, bearing in mind that $p \geq s_{N+1-\beta_N}^{N+1} \geq s_{N+1-\beta_N}^N$.

□

The following result is a generalization of Theorem 2.1.

Theorem 5.5 *Let (A, B, C) be a minimal partial realization of $\mathcal{Y}^N$.*

1. *If $CA^NB = Y_N$ (i. e., (A, B, C) is a realization of $\mathcal{Y}^{N+1}$), then*

   $$\alpha_{N+1} = \alpha_N, \quad \beta_{N+1} = \beta_N, \quad d_{N+1} = d_N.$$

2. *If $CA^NB \neq Y_N$ (i. e., (A, B, C) is not a realization of $\mathcal{Y}^{N+1}$), then*

   $$\alpha_{N+1} \geq \max\{\alpha_N, N+1-\beta_N\}, \ \beta_{N+1} \geq \max\{\beta_N, N+1-\alpha_N\}, \ d_{N+1} \geq d_N.$$

   Moreover, if $r_{\beta_N}^N = m$, then

   $$\alpha_{N+1} = \max\{\alpha_N, N+1-\beta_N\}, \quad d_{N+1} = d_N + \sum_{i=\beta_N+1}^{\beta_{N+1}} r_i^{N+1}.$$

   Similarly, if $s_{\alpha_N}^N = p$, then

   $$\beta_{N+1} = \max\{\beta_N, N+1-\alpha_N\}, \quad d_{N+1} = d_N + \sum_{i=\alpha_N+1}^{\alpha_{N+1}} s_i^{N+1}.$$

Proof. It is clear that $d_N = \sum_{i=1}^{N} r_i^N \leq \sum_{i=1}^{N+1} r_i^{N+1} = d_{N+1}$.

1. The order of (A, B, C) is d_N and the order of the minimal partial realizations of $\mathcal{Y}^{N+1}$ is d_{N+1}. Therefore, if (A, B, C) is a realization of $\mathcal{Y}^{N+1}$, then $d_{N+1} \leq d_N$. Hence, $d_{N+1} = d_N$ and (A, B, C) is a minimal partial realization of $\mathcal{Y}^{N+1}$. By Theorem 3.2, $\alpha_{N+1} = \alpha_N$ and $\beta_{N+1} = \beta_N$.

2. Assume that (A, B, C) is not a realization of $\mathcal{Y}^{N+1}$.

   If $N < \alpha_N + \beta_N$, taking into account Proposition 5.2,

   $$\alpha_{N+1} \geq \alpha_N = \max\{\alpha_N, N+1-\beta_N\}, \quad \beta_{N+1} \geq \beta_N = \max\{\beta_N, N+1-\alpha_N\}.$$

   When $r_{\beta_N}^N = m$, since $m \geq r_{N+1-\alpha_N}^N \geq r_{\beta_N}^N = m$, we have that $r_{N+1-\alpha_N}^N = m$, and, by Corollary 5.4 (item 3),

   $$\alpha_{N+1} = \alpha_N = \max\{\alpha_N, N+1-\beta_N\}.$$

   If $N \geq \alpha_N + \beta_N$, then $\max\{\alpha_N, N+1-\beta_N\} = N+1-\beta_N$. Let us see that $\alpha_{N+1} > \alpha_N$. If $\alpha_{N+1} = \alpha_N$, then, by Corollary 5.3 (item 3), $\beta_{N+1} = \beta_N$ and $d_{N+1} = d_N$.

   Let (A', B', C') be a minimal partial realization of $\mathcal{Y}^{N+1}$. Then, (A', B', C') is a realization of $\mathcal{Y}^N$ of order $d_{N+1} = d_N$, therefore it is also a minimal partial realization of $\mathcal{Y}^N$. By Proposition 3.3, (A, B, C) is similar to (A', B', C'), from where (A, B, C) is also a minimal partial realization of $\mathcal{Y}^{N+1}$, which is a contradiction.

   Therefore, $\alpha_{N+1} > \alpha_N$ and, by Corollary 5.3 (item 4), we have that

   $$\alpha_{N+1} \geq N+1-\beta_N = \max\{\alpha_N, N+1-\beta_N\},$$

   $$\beta_{N+1} \geq N+1-\alpha_N = \max\{\beta_N, N+1-\alpha_N\}.$$

   When $r_{\beta_N}^N = m$, by Corollary 5.3 (item 6), we have that

   $$\alpha_{N+1} = N+1-\beta_N = \max\{\alpha_N, N+1-\beta_N\}.$$

   Moreover, if $r_{\beta_N}^N = m$, then $d_N = m\beta_N$ and

   $$m \geq r_i^{N+1} \geq r_{\beta_N}^{N+1} \geq r_{\beta_N}^N = m, \quad 1 \leq i \leq \beta_N.$$

   Then,

   $$d_{N+1} = m\beta_N + \sum_{i=\beta_N+1}^{\beta_{N+1}} r_i^{N+1} = d_N + \sum_{i=\beta_N+1}^{\beta_{N+1}} r_i^{N+1}.$$

□

Recall that if $m = 1$, then $d_N = \beta_N$ and, if $p = 1$, then $d_N = \alpha_N$.

Corollary 5.6 *Let (A, B, C) be a minimal partial realization of $\mathcal{Y}^N$. If (A, B, C) is not a partial realization of $\mathcal{Y}^{N+1}$, then*

1. *If $m = 1$, then*
$$\alpha_{N+1} = \max\{\alpha_N, N + 1 - \beta_N\} = \max\{\alpha_N, N + 1 - d_N\},$$
$$\beta_{N+1} = d_{N+1} \geq \max\{\beta_N, N + 1 - \alpha_N\} = \max\{d_N, N + 1 - \alpha_N\}.$$
2. *If $p = 1$, then*
$$\beta_{N+1} = \max\{\beta_N, N + 1 - \alpha_N\} = \max\{\beta_N, N + 1 - d_N\},$$
$$\alpha_{N+1} = d_{N+1} \geq \max\{\alpha_N, N + 1 - \beta_N\} = \max\{d_N, N + 1 - \beta_N\}.$$
3. *If $m = p = 1$, then $\alpha_N = \beta_N = d_N$ and*
$$\alpha_{N+1} = \beta_{N+1} = d_{N+1} = \max\{d_N, N + 1 - d_N\}.$$

Proof. It follows directly from Theorem 5.5 bearing in mind that if $m = 1$, then $r_{\beta_N} = 1$, and if $p = 1$ then $s_{\alpha_N} = 1$.

□

Corollary 5.7

1. *If $m = 1$ and $N < \alpha_N + \beta_N$, then*
$$\alpha_i = \alpha_N, \quad N \leq i \leq \alpha_N + \beta_N.$$
2. *If $p = 1$ and $N < \alpha_N + \beta_N$, then*
$$\beta_i = \beta_N, \quad N \leq i \leq \alpha_N + \beta_N.$$
3. *If $m = p = 1$ and $N < 2d_N$, then*
$$d_i = d_N, \quad N \leq i \leq 2d_N.$$

Proof. Assume that $N < \alpha_N + \beta_N$. By Proposition 5.2,
$$\alpha_i \geq \alpha_N, \quad \beta_i \geq \beta_N, \quad N \leq i \leq \alpha_N + \beta_N,$$
$$\alpha_{i-1} + \beta_{i-1} \geq \alpha_N + \beta_N \geq i > i - 1, \qquad N + 1 \leq i \leq \alpha_N + \beta_N.$$

1. If $m = 1$, by Corollary 5.6,
$$\alpha_i = \alpha_{i-1}, \quad N + 1 \leq i \leq \alpha_N + \beta_N.$$
2. If $p = 1$, by Corollary 5.6,
$$\beta_i = \beta_{i-1}, \quad N + 1 \leq i \leq \alpha_N + \beta_N.$$
3. It follows from item 1, bearing in mind that $\alpha_i = \beta_i = d_i$ for $1 \leq i \leq N$.

□

6 Obtention of the partial Brunovsky indices of sequences of vectors

In this section we propose an algorithm to compute the partial Brunovsky indices of a given sequence of vectors $\mathcal{Y}^n = (Y_0, \ldots, Y_{n-1})$, $Y_i \in \mathbb{F}^{p\times 1}$. Therefore, throughout this section we have $m = 1$. Obviously, the same strategy will apply for the case $p = 1$.

From the results of the previous section we derive the next proposition, which summarizes some key properties for developing the algorithm. For convenience, we put $s_0^i = p$ for $i \geq 0$.

Proposition 6.1 *Assume that $\beta_N > \beta_{N-1}$. Then, taking $\beta_0 = 0, \alpha_0 = 0, s^{(0)} = (0)$, the following conditions are satified*

1.

$$1 \leq N + 1 - \beta_N \leq \min\{N - \beta_{N-1}, \alpha_{N-1} + 1\}.$$

2.

$$s_i^N = \begin{cases} s_i^{N-1} + 1, & N + 1 - \beta_N \leq i \leq N - \beta_{N-1}, \\ s_i^{N-1}, & 1 \leq i \leq N - \beta_N \quad \textit{or} \quad N - \beta_{N-1} + 1 \leq i \leq N. \end{cases}$$

3. If for some $i \in \{1, \ldots, N-1\}$, $s_{i-1}^{N-1} = s_i^{N-1}$, then $N + 1 - \beta_N \neq i$.

4. Let $\mathcal{I}$ be the set of indices

$$\mathcal{I} = \left\{i \;:\; 1 \leq i \leq \min\{N - \beta_{N-1}, \alpha_{N-1} + 1\},\; s_{i-1}^{N-1} \neq s_i^{N-1}\right\}.$$

Then, $\beta_N = N + 1 - j$ where

$$j = \min\left\{i \in \mathcal{I} \;:\; \operatorname{rank} H_{i,N+1-i}(\mathcal{Y}^N) > \sum_{k=1}^{i} s_k^{N-1}\right\}.$$

Proof.

1. From Theorem 5.5, as $\beta_N > \beta_{N-1}$, we have that $\beta_N \geq \max\{\beta_{N-1}+1, N - \alpha_{N-1}\}$.

2. It follows from Proposition 5.2, bearing in mind that

$$r_{N+1-i}^N - r_{N+1-i}^{N-1} = \begin{cases} 0 - 0 = 0, & 1 \leq i \leq N - \beta_N, \\ 1 - 0 = 1, & N + 1 - \beta_N \leq i \leq N - \beta_{N-1}, \\ 1 - 1 = 0, & N - \beta_{N-1} + 1 \leq i \leq N. \end{cases}$$

3. Let us suppose that $s_{i-1}^{N-1} = s_i^{N-1}$. If $N+1-\beta_N = i$, then $s_i^N = s_i^{N-1}+1 = s_{i-1}^{N-1} + 1 = s_{i-1}^N + 1$, which is a contradiction because $s_i^N \leq s_{i-1}^N$.

4. From items 1 and 3, $\beta_N = N+1-j$ for some $j \in \mathcal{I}$. Moreover, by definition,

   $$\beta_N = \max\{i : r_i^N > 0\} = \max\{i : \operatorname{rank} H_{N+1-i,i}(\mathcal{Y}^N) > \operatorname{rank} H_{N+1-i,i-1}(\mathcal{Y}^N)\}.$$

   Therefore, $\beta_N = N+1-j$ where

   $$j = \min\left\{ i \in \mathcal{I} \ : \ \operatorname{rank} H_{i,N+1-i}(\mathcal{Y}^N) > \sum_{k=1}^{i} s_k^{N-1} \right\}.$$

   For $1 \leq i \leq N-1$, $H_{i,N-i}(\mathcal{Y}^N) = H_{i,N-i}(\mathcal{Y}^{N-1})$, and from Proposition 3.1,

   $$\operatorname{rank} H_{i,N-i}(\mathcal{Y}^{N-1}) = \sum_{k=1}^{i} s_k^{N-1} - \sum_{k=N+1-i}^{N-1} r_k^{N-1}.$$

   If $i \in \mathcal{I}$, then $N+1-i > \beta_{N-1}$. Hence, $\sum_{k=N+1-i}^{N-1} r_k^{N-1} = 0$ and the property follows.

□

Given $\mathcal{Y}^n = (Y_0, \ldots, Y_{n-1})$, $Y_i \in \mathbb{F}^{p\times 1}$, taking into account this Proposition and Theorem 5.5 we can iteratively compute β_N, α_N, s^N for $1 \leq N \leq n$.

After initializing the procedure, once the step $N-1$ is accomplished, we first find the set $\mathcal{I}$, then for $j \in \mathcal{I}$ we successively compute $\rho = \sum_{k=1}^{j} s_k$ and $t = \operatorname{rank} H_{j,N+1-j}(\mathcal{Y}^N)$ until $t > \rho$. If this occurs, we update α, s, β and the set of indices $\mathcal{R} = \{i \ : \ s_{i-1} = s_i\}$. If $t = \rho$ for all $j \in \mathcal{I}$, then $\beta = \beta$, $\alpha = \alpha$, $s = s$ and $\mathcal{R} = \mathcal{R}$.

Algorithm

Input: $\mathcal{Y}^n = (Y_0, \ldots, Y_{n-1})$, $Y_i \in \mathbb{F}^{p\times 1}$
Output: β_n, α_n, s^n.

```
• Do $\beta = 0$, $\alpha = 0$, $s = (0)$, $\mathcal{R} = \emptyset$.
• For $N = 1, \ldots n$
    – Calculate the set $\mathcal{I} = \{i \ : \ 1 \leq i \leq \min\{N-\beta, \alpha+1\},\ s_{i-1} \neq s_i\}$.
    – Do $stop = FALSE$
    – For each element $j \in \mathcal{I}$
          If $stop == FALSE$
            ∗ Do $\rho = \sum_{k=1}^{j} s_k$
            ∗ Do $t = \operatorname{rank} H_{j,N+1-j}(\mathcal{Y}^N)$
            ∗ If $t > \rho$
                · Do $\alpha = \max\{N-\beta, \alpha\}$
```

    - · Do $s_i = s_i + 1$ for $j \leq i \leq N - \beta$
    - · Do $\beta = N + 1 - j$
    - · Calculate the set of indices $\mathcal{R} = \{i \ : \ s_{i-1} = s_i\}$.
    - · Do *stop* $= TRUE$.

- Output: β, α, s.

Example 6.2 *Let $\mathbb{F} = \mathbb{R}$, $p = 3$,*

$$\mathcal{Y}^{12} = (e_1, e_2, 0, 0, e_1, e_2, 0, e_3, 0, 0, 0, e_1),$$

where, for $i = 1, 2, 3$, e_i are the unitary vectors in $\mathbb{R}^3$. We obtain:

N	β	α	s
0	$\beta_0 = 0,$	$\alpha_0 = 0,$	$s^0 = (0)$
1	$\beta_1 = 1,$	$\alpha_1 = 1,$	$s^1 = (1)$
2	$\beta_2 = 2,$	$\alpha_2 = 1,$	$s^2 = (2)$
3	$\beta_3 = 2,$	$\alpha_3 = 1,$	$s^3 = (2)$
4	$\beta_4 = 2,$	$\alpha_4 = 1,$	$s^4 = (2)$
5	$\beta_5 = 4,$	$\alpha_5 = 3,$	$s^5 = (2, 1, 1)$
6	$\beta_6 = 4,$	$\alpha_6 = 3,$	$s^6 = (2, 1, 1)$
7	$\beta_7 = 4,$	$\alpha_7 = 3,$	$s^7 = (2, 1, 1)$
8	$\beta_8 = 8,$	$\alpha_8 = 4,$	$s^8 = (3, 2, 2, 1)$
9	$\beta_9 = 8,$	$\alpha_9 = 4,$	$s^9 = (3, 2, 2, 1)$
10	$\beta_{10} = 8,$	$\alpha_{10} = 4,$	$s^{10} = (3, 2, 2, 1)$
11	$\beta_{11} = 8,$	$\alpha_{11} = 4,$	$s^{11} = (3, 2, 2, 1)$
12	$\beta_{12} = 9,$	$\alpha_{12} = 4,$	$s^{12} = (3, 2, 2, 2)$

Just to help understanding, we describe the calculations performed in some steps:

- *At $N = 1$ (we have $\beta = \beta_0 = 0$, $\alpha = \alpha_0 = 0$, $s = s^0 = (0)$, $\mathcal{R} = \emptyset$),*

  $$\mathcal{I} = \{i \ : \ 1 \leq i \leq \min\{N - \beta, \alpha + 1\}, \ s_{i-1} \neq s_i\} = \{1\}.$$

  For $j = 1$, $\rho = s_1 = 0$, $t = \operatorname{rank} H_{1,1}(\mathcal{Y}^1) = \operatorname{rank} \begin{bmatrix} e_1 \end{bmatrix} > \rho$. Then $\alpha = \max\{N - \beta, \alpha\} = \max\{1 - 0, 0\} = 1$, $s_i = s_i + 1$ for $1 \leq i \leq N - \beta = 1$, i.e. $s = (1)$, $\beta = N + j - 1 = 1 + 1 - 1 = 1$, and $\mathcal{R} = \emptyset$.

- *At $N = 4$ (we have $\beta = \beta_3 = 2$, $\alpha = \alpha_3 = 1$, $s = s^3 = (2)$, $\mathcal{R} = \emptyset$),*

  $$\mathcal{I} = \{i \ : \ 1 \leq i \leq \min\{N - \beta, \alpha + 1\}, \ s_{i-1} \neq s_i\} = \{1, 2\}.$$

  For $j = 1$, $\rho = s_1 = 2$, $t = \operatorname{rank} H_{1,4}(\mathcal{Y}^4) = \operatorname{rank} \begin{bmatrix} e_1 & e_2 & 0 & 0 \end{bmatrix} = 2 = \rho$.

  For $j = 2$, $\rho = s_1 + s_2 = 2$, $t = \operatorname{rank} H_{2,3}(\mathcal{Y}^4) = \operatorname{rank} \begin{bmatrix} e_1 & e_2 & 0 \\ e_2 & 0 & 0 \end{bmatrix} = 2 = \rho$.

  Then, $\beta = 2$, $\alpha = 1$, $s = (2)$, $\mathcal{R} = \emptyset$.

- *At* $N = 9$ *(we have* $\beta = \beta_8 = 8$, $\alpha = \alpha_8 = 4$, $s = s^8 = (3, 2, 2, 1)$, $\mathcal{R} = \{1, 3\}$*),*

  $$\mathcal{I} = \{i \;:\; 1 \leq i \leq \min\{N - \beta, \alpha + 1\},\; s_{i-1} \neq s_i\} = \{1\} \setminus \{1, 3\} = \emptyset.$$

  Then, $\beta = 8$, $\alpha = 4$, $s = (3, 2, 2, 1)$, $\mathcal{R} = \{1, 3\}$.

- *At* $N = 12$, *(we have* $\beta = \beta_{11} = 8$, $\alpha = \alpha_{11} = 4$, $s = s^{11} = (3, 2, 2, 1)$, $\mathcal{R} = \{1, 3\}$*),*

  $$\mathcal{I} = \{i \;:\; 1 \leq i \leq \min\{N - \beta, \alpha + 1\},\; s_{i-1} \neq s_i\} = \{1, 2, 3, 4\} \setminus \{1, 3\} = \{2, 4\}.$$

  For $j = 2$, $\rho = s_1 + s_2 = 5$, $t = \operatorname{rank} H_{2,11}(\mathcal{Y}^{12}) = 5 = \rho$.
  For $j = 4$, $\rho = s_1 + s_2 + s_3 + s_4 = 8$, $t = \operatorname{rank} H_{4,9}(\mathcal{Y}^{12}) = 9 > \rho$.
  Then $\alpha = \max\{N - \beta, \alpha\} = \max\{12 - 8, 4\} = 4$, $s_i = s_i + 1$ *for* $4 \leq i \leq 4$, *i.e.* $s = (3, 2, 2, 2)$, $\beta = N - j + 1 = 12 - 4 + 1 = 9$, *and* $\mathcal{R} = \{1, 3, 4\}$.

To obtain a minimal partial realization of $\mathcal{Y}^{12}$ *in observability reduced form (see Section 3), the only possible choice of indices is*

$$I_1 = \{1, 2, 3\}, \quad I_2 = I_3 = I_4 = \{1, 3\}.$$

Hence, we solve the systems

$$\begin{bmatrix} a_{21} & \dots & a_{25} \end{bmatrix} H_{2,11}(\mathcal{Y}^{12})(\{1, 2, 3, 4, 6\}, :) = \begin{bmatrix} e_2 & 0 & \dots & e_1 \end{bmatrix} (\{2\}, :)$$

and

$$\begin{bmatrix} a_{11} & \dots & a_{19} \\ a_{31} & \dots & a_{39} \end{bmatrix} H_{4,8}(\mathcal{Y}^{12})(\{1, 2, 3, 4, 6, 7, 9, 10, 12\}, :) = \begin{bmatrix} e_1 & e_2 & \dots & e_1 \end{bmatrix} (\{1, 3\}, :).$$

It follows that all the minimal partial realization of $\mathcal{Y}^{12}$ *in observability reduced form are*

$$A_o = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -a & 1 & 0 & 0 & 0 & a & a & -1 \\ 0 & -b & 0 & 1 & 0 & 0 & b & b & 0 \end{bmatrix}, \quad B_o = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$C_o = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad a, b \in \mathbb{F}.$$

The number of free parameters is $s_4 r_9 = 2$.

Given $a, b \in \mathbb{F}$, we can obtain a left matrix generator of minimal length $C_L(D) = I_3 + L_1D + L_2D^2 + L_3D^3 + L_4D^4$ of $\mathcal{Y}^{12}$ solving the system (see Section 4)

$$C_oA_o^4 = \begin{bmatrix} L_4 & L_3 & L_2 & L_1 \end{bmatrix} \mathcal{O}_4(C, A).$$

If c_1, c_2, c_3 are the rows of C_o, then

$$\begin{bmatrix} c_1A_o^4 \\ c_3A_o^4 \end{bmatrix} = \left[\begin{array}{ccc|cc|cc|cc} 1 & -a & 1 & 0 & 0 & 0 & a & a & -1 \\ 0 & -b & 0 & 1 & 0 & 0 & b & b & 0 \end{array}\right] \left[\begin{array}{c} c_1 \\ c_2 \\ c_3 \\ \hline c_1A_o \\ c_3A_o \\ \hline c_1A_o^2 \\ c_3A_o^2 \\ \hline c_1A_o^3 \\ c_3A_o^3 \end{array}\right].$$

Therefore,

$$\begin{bmatrix} c_1A_o^4 \\ c_3A_o^4 \end{bmatrix} = X_1\mathcal{O}_4(C, A), \ \text{where } X_1 = \left[\begin{array}{ccc|ccc|ccc|ccc} 1 & -a & 1 & 0 & 0 & 0 & 0 & 0 & a & a & 0 & -1 \\ 0 & -b & 0 & 1 & 0 & 0 & 0 & 0 & b & b & 0 & 0 \end{array}\right].$$

$$c_2A_o = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 0 \end{array}\right] \left[\begin{array}{c} c_1 \\ c_2 \\ c_3 \\ \hline c_1A_o \\ c_3A_o \end{array}\right].$$

Hence

$$c_2A_o^4 = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 0 \end{array}\right] \left[\begin{array}{c} c_1A_o^3 \\ c_2A_o^3 \\ c_3A_o^3 \\ \hline c_1A_o^4 \\ c_3A_o^4 \end{array}\right] = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} c_1A_o^3 \\ c_2A_o^3 \\ c_3A_o^3 \end{bmatrix} + \begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} c_1A_o^4 \\ c_3A_o^4 \end{bmatrix} = X_2\mathcal{O}_4(C_o, A_o),$$

where

$$\begin{aligned} X_2 = & \left[\begin{array}{ccc|ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right] + \begin{bmatrix} 0 & 0 \end{bmatrix} X_1 \\ = & \left[\begin{array}{ccc|ccc|ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right]. \end{aligned}$$

Let

$$\begin{bmatrix} L_4 & L_3 & L_2 & L_1 \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc|ccc} 1 & -a & 1 & 0 & 0 & 0 & 0 & 0 & a & a & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -b & 0 & 1 & 0 & 0 & 0 & 0 & b & b & 0 & 0 \end{array}\right].$$

Then $C_L(D) = I_3 + L_1D + L_2D^2 + L_3D^3 + L_4D^4$ is a left matrix generator of minimal length of $\mathcal{Y}^{12}$.

It can be checked that all the left matrix generators of minimal length of $\mathcal{Y}^{12}$ *are* $C_L(D) = I_3 + L_1D + L_2D^2 + L_3D^3 + L_4D^4$ *with*

$$\begin{bmatrix} L_4 & L_3 & L_2 & L_1 \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc|ccc} 1-x_1 & -a & 1 & -x_2 & x_1 & 0 & -x_3 & x_2 & a & a & x_3 & -1 \\ -y_1 & 0 & 0 & -y_2 & y_1 & 0 & -y_3 & y_2 & 0 & 1 & y_3 & 0 \\ -z_1 & -b & 0 & 1-z_2 & z_1 & 0 & -z_3 & z_2 & b & b & z_3 & 0 \end{array}\right],$$

for $x_i, y_i, z_i \in \mathbb{F}$.

Dually, to obtain a minimal partial realization of $\mathcal{Y}^{12}$ *in controllability reduced form we solve*

$$H_{3,9}(\mathcal{Y}^{12}) \begin{bmatrix} b_9 \\ \vdots \\ b_1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ e_1 \end{bmatrix}.$$

The solution depends on $2 = s_4 r_9$ *free parameters:*

$$b_7 = 1, \quad b_5 = -b_9, \quad b_2 = b_3 = b_4 = b_6 = b_8 = 0.$$

It follows that all the minimal partial realizations of $\mathcal{Y}^{12}$ *in controllability reduced form are*

$$A_c = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -a \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b \end{bmatrix}, \quad B_c = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$C_c = \begin{bmatrix} e_1 & e_2 & 0 & 0 & e_1 & e_2 & 0 & e_3 & 0 \end{bmatrix}, \quad a, b \in \mathbb{F}.$$

Equivalently, all the right matrix generators of minimal length of $\mathcal{Y}^{12}$ *are*

$$C_R(D) = 1 + bD - aD^5 + D^7 + aD^9, \quad a, b \in \mathbb{F}.$$

□

Acknowledgments

The first author is partially supported by grants MINECO MTM2013-40960-P, MTM2017-90682-REDT, and UPV/EHU GIU16/42. The second author is partially supported by grants MINECO MTM2013-40960-P and MTM2017-90682-REDT.

References

[1] J. Althaler, A. Dür, Finite Linear Recurring Sequences and Homogeneous Ideals, AAECC 7 (1996) 377-390.

[2] J. Althaler, A. Dür, A Generalization of the Massey-Ding Algorithm, AAECC 9 (1998) 1-14.

[3] A.C. Antoulas, On Recursiveness and Related Topics in Linear Systems, IEEE Transactions on Automatic Control, AC-31 (12) (1986) 1121–1135.

[4] A.C. Antoulas, Recursive modeling of discrete-time time series, Linear Algebra for Control Theory, IMA (62), Berlin: Springer, 1994, 1–20.

[5] I. Baragaña, F. Puerta, I. Zaballa, On the geometry of realizable Markov parameters by SIMO and MISO Systems. Linear Algebra Appl. 518 (2017) 97–143

[6] I. Baragaña, F. Puerta, Versal Deformation of Realizable Markov Parameters, to appear in International Journal of Control, DOI: 10.1080/00207179.2017.1414311.

[7] E.R. Berlekamp, Nonbinary BCH decoding, presented at the 1967 International Symp. on Information Theory, San Remo, Italy. Algebraic Coding Theory, New York: McGraw-Hill, 1968, chs 7 and 10.

[8] O.H. Bosgra, On parametrizations for the minimal partial realization problem, Systems & Control Letters, 3 (1983) 181-187.

[9] P. Brunovsky, Classification of linear controllable systems, Kybernetica (Praga), 3 (6) (1970) 173–188.

[10] B.W. Dickinson, M. Morf, T. Kailath, A Minimal Realization Algorithm for Matrix Sequences, IEEE Transactions on Automatic Control, AC-19 (1) (1974) 31–38.

[11] C. Ding, Proof of Massey's conjetured algorithm, In: Guenther, C.G. (ed.) Advances in Cryptology-EUROCRYPT'88, 345-349. Lecture Notes in Computer Sciences, Vol. 330, Berlin, Heidelberg, New York: Springer 1988.

[12] G.-L. Feng, K.K. Tzeng, A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes, IEEE Transactions on Information Theory, 37 (5) (1991) 1274–1287.

[13] W.B. Gragg, A. Lindquist, On the Partial Realization Problem, Linear Algebra Appl. 50 (1983) 277–319.

[14] B.L. Ho, R.E. Kalman, Effective construction of linear state-variable models from input/output functions, Regelungstechnik 14 (1966) 543–5488.

[15] E. Jonckheere, C. Ma, A simple Hankel interpretation of the Berlekamp-Massey algorithm, Linear Algebra Appl. 125 (1989) 65–76.

[16] E. Kaltofen, G. Yuhasz, On the Matrix Berlekamp-Massey Algorithm, ACM Transactions on Algorithms, 9, 4 (2013) Article 33, 24 pages.

[17] M. Kuijper, An algorithm for constructing a minimal partial realization in the multivariable case, Systems & Control Letters, 31 (1997) 225–233.

[18] J.L. Massey, Shift-Register Synthesis and BCH Decoding, IEEE Transactions on Information Theory, IT-15, 1 (1969) 122–127.

[19] J. Rissanen, Recursive Identification of Linear Systems, SIAM J. Control, 9 (3) (1971) 420–430.

[20] S. Sakata, Finding a Minimal Set of Linear Recurring Relations Capable of Generating a Given Finite Two-dimensional Array, J. Symbolic Computation, 5 (1988) 321–337.

[21] S. Sakata, Extension of the Berlekamp-Massey Algorithm to N Dimensions, Information and Computation, 84 (1990), 201–239.

[22] G. Yuhasz, Berlekamp/Massey Algorithms for Linearly Generated Matrix Sequences, PhD, North Carolina State University, 2009.