Extensions of the Berlekamp-Massey algorithm*

Itziar Baragaña[1] and Alicia Roca[2]

Abstract— **Given a finite sequence of scalars, the Berlekamp-Massey algorithm solves the problem of finding a linear feedback shift register of minimal length which generates it. When instead of a sequence of scalars, we are given a sequence of matrices, it can be interpreted as the problem of finding a minimal partial realization and also as the problem of finding a minimal length right (left) matrix generator of the sequence. We generalize the main result on which the Berlekamp-Massey algorithm is based in terms of the partial Brunovsky indices of a finite sequence of matrices and design a strategy to obtain them for sequences of vectors. Once they are known, we can compute a minimal partial realization and a minimal length right (left) matrix generator of the sequence.**

I. Introduction

A *linear feedback shift register* (LFSR) of length L with connection polynomial $C(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_L D^L$ and initial state $(y_0, \ldots, y_{L-1})$ generates a sequence of scalars $\mathcal{Y}^N = (y_0, y_1, \ldots, y_{N-1})$, $y_i \in \mathbb{F}$, $\mathbb{F}$ a field, according to the recursion

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

The Berlekamp-Massey algorithm ([11]) solves the problem of finding the shortest LFSR which generates a given finite sequence of scalars. The result is based on an iterative algorithm for decoding BCH codes introduced in [5]. The extension of this problem to sequences of matrices has been analyzed from different points of view ([1], [2], [7]–[10], [12] among others).

We generalize this problem to the matrix case in different ways. Observe that if $\mathcal{Y}^N = (y_0, y_1, \ldots, y_{N-1})$ is generated by a LFSR with connection polynomial $C(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_L D^L$ and

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & c_L \\ 1 & 0 & 0 & \ldots & 0 & c_{L-1} \\ 0 & 1 & 0 & \ldots & 0 & c_{L-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & c_1 \end{bmatrix}, \; B = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

$$C = \begin{bmatrix} y_0 & y_1 & \ldots & y_{L-2} & y_{L-1} \end{bmatrix},$$

then

$$CA^j B = y_j, \quad L \leq j \leq N-1.$$

It means that (A, B, C) is a *partial realization of* $\mathcal{Y}^N$ in reduced controllability form.

Then, in the matrix case, a natural generalization of the problem solved by the Berlekamp-Massey algorithm is:

Given a finite sequence of matrices $\mathcal{Y}^N = (Y_0, Y_1, \ldots, Y_{N-1})$, $Y_j \in \mathbb{F}^{p\times m}$, find a minimal partial realization of $\mathcal{Y}^N$, i.e. find a matrix triple (A, B, C), $A \in \mathbb{F}^{d\times d}$, $B \in \mathbb{F}^{d\times m}$, $C \in \mathbb{F}^{p\times d}$ of least possible order d such that

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

A LFSR can also be considered as a right (left) matrix generator. We say that $C_R(D) = I_m + R_1 D + \cdots + R_\rho D^\rho \in \mathbb{F}[D]^{m\times m}$ is a *right matrix generator* of length ρ of $\mathcal{Y}^N$ if

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

Analogously, $C_L(D) = I_m + L_1 D + \cdots + L_\rho D^\rho \in \mathbb{F}[D]^{p\times p}$ is a *left matrix generator of* $\mathcal{Y}^N$ if

$$Y_j = L_1 Y_{j-1} + \cdots + L_\rho Y_{j-\rho}, \quad \rho \leq j \leq N-1.$$

We pose the following problem:

Given a finite sequence of matrices $\mathcal{Y}^N = (Y_0, \ldots, Y_{N-1})$, $Y_j \in \mathbb{F}^{p\times m}$, find a right (left) matrix generator of $\mathcal{Y}^N$ of minimal length.

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 when $m = p = 1$ both problems are equivalent to that of finding a LFSR which generates $\mathcal{Y}^N$. In the general case, given a right (left) matrix generator of length δ of $\mathcal{Y}^N$ we can easily obtain a partial realization of it of order $m\delta$ ($p\delta$). Hence, if d and g are, respectively, the order of a minimal partial realization and the minimal length of a right (left) matrix generator of $\mathcal{Y}^N$, then $d \leq mg$ ($d \leq pg$). On the other hand, knowing a minimal partial realization of $\mathcal{Y}^N$, with additional calculations, we can obtain a minimal length right (left) matrix generator (a procedure is described in [4]).

In Section II we present the theorem by Massey ([11]) standing the Berlekamp-Massey algorithm, we introduce the partial Brunovsky indices of a sequence and some previous results about partial realizations. In Section III we state the main result, which relates the order of minimal partial realizations and the minimal length of right (left) matrix generators of $\mathcal{Y}^{N+1}$ with those of $\mathcal{Y}^N$, and sketch the steps to be followed to obtain them for sequences of vectors ($m = 1$ or $p = 1$). We also (briefly) indicate how to obtain minimal partial realizations of $\mathcal{Y}^N$ in reduced controllability and

*This work was partially supported by MINECO: MTM2017-83624-P, MTM2017-90682-REDT, and UPV/EHU: GIU16/42.

[1] Itziar Baragaña is with the Departamento de Ciencia de la Computación e I.A., Facultad de Informática, Universidad del País Vasco, UPV/EHU, Apartado 649, 20080 Donostia-San Sebastián, Spain itziar.baragana@ehu.eus

[2] Alicia Roca is with the Departamento de Matemática Aplicada, IMM, Universitat Politècnica València, 46021 València, Spain aroca@mat.upv.es

observability forms. In Section IV we present an example of how to obtain the partial Brunovsky indices of a given finite sequence of vectors, a minimal partial realization and a minimal length right and left matrix generator of it. Finally, in Section V we summarize the achievements of the paper.

II. Previous results

The Berlekamp-Massey algorithm is an iterative adaptive procedure which is based on the result of the next theorem ([11, Theorem 2]), where given $\mathcal{Y} = (y_0, y_1, \ldots)$, L_i denotes the length of the shortest register generating $\mathcal{Y}^i = (y_0, y_1, \ldots, y_{i-1})$, for $i \geq 1$.

Theorem 2.1: 1) If some LFSR of length L_N generates the sequences $\mathcal{Y}^N$ and $\mathcal{Y}^{N+1}$, then $L_{N+1} = L_N$.

2) If some LFSR of length L_N generates the sequence $\mathcal{Y}^N$ but not the sequence $\mathcal{Y}^{N+1}$, then

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

Our aim is to generalize this result.

Given a sequence of matrices $\mathcal{Y}^N = (Y_0, Y_1, \ldots, Y_{N-1})$, the order of the minimal partial realizations of $\mathcal{Y}^N$ can be stated in terms of the partial Kronecker row indices or the partial Kronecker column indices of $\mathcal{Y}^N$ (see [6, Theorem 2.1]). Moreover, if α_N and β_N are the largest partial Kronecker row and column indices of $\mathcal{Y}^N$, respectively, we will see that the minimal length of the right (left) matrix generators of $\mathcal{Y}^N$ is β_N (α_N).

Given a partition $a = (a_1, a_2, \ldots, a_m)$ of nonnegative integers, the *conjugate partition* of a, $\overline{a} = (\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_N)$, is defined as $\overline{a}_k := \#\{i : a_i \geq k\}$, $1 \leq k \leq N$. The conjugate partitions of the partial Kronecker row and column indices of $\mathcal{Y}^N$ are called the *partial Brunovsky row and column indices of* $\mathcal{Y}^N$, respectively ([3]). In what follows, results are stated in terms of the partial Brunovsky indices. They are sequences of integers $s_1 \geq s_2 \geq \cdots \geq s_{\alpha_N} > 0 = s_{\alpha_N+1} = \cdots = s_N$ and $r_1 \geq r_2 \geq \cdots \geq r_{\beta_N} > 0 = r_{\beta_N+1} = \cdots = r_N$, which can be defined as

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

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

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

for $1 \leq i \leq N$, $1 \leq j \leq N+1-i$ (we take $\operatorname{rank} H_{0,N}(\mathcal{Y}^N) = \operatorname{rank} H_{N,0}(\mathcal{Y}^N) = 0$).

The order of minimal partial realizations of $\mathcal{Y}^N$ is given in the next proposition ([6, Theorem 2.1]).

Proposition 2.2: The order d_N of minimal partial realizations of $\mathcal{Y}^N$ is

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

The following proposition is straightforward.

Proposition 2.3: 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

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

i.e., if and only if $r_{\rho+1} = 0$.

Consequently,

Proposition 2.4: The minimal length of the right matrix generators of $\mathcal{Y}^N$ is the largest partial Kronecker column index of $\mathcal{Y}^N$.

Analogously, the minimal length of the left matrix generators of $\mathcal{Y}^N$ is largest partial Kronecker row index of $\mathcal{Y}^N$.

Using the properties of the Hankel matrices, we are able to relate the partial Brunovsky indices of $\mathcal{Y}^{N+1}$ with those of $\mathcal{Y}^N$, which allow us to generalize Theorem 2.1. The result is presented in Section III. From it, we can obtain iteratively the partial Brunovsky indices of a given sequence of vectors, and then a minimal realization and a minimal length matrix generator of the sequence. We will sketch an example in Section IV.

III. Main result

In this section we state a generalization of Theorem 2.1 (see [4]). Given $\mathcal{Y} = (Y_0, Y_1, \ldots)$, $Y_j \in \mathbb{F}^{p \times m}$, for $i \geq 1$, d_i denotes the order of the minimal partial realizations of $\mathcal{Y}^i = (Y_0, Y_1, \ldots, Y_{i-1})$, and α_i, β_i the number of positive Brunovsky row and column indices of $\mathcal{Y}^i$, respectively (equivalently, the minimal length of the left and right matrix generators of $\mathcal{Y}^i$, respectively).

Theorem 3.1: 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 $m = 1$ then

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

and if $p = 1$, then

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

As a consequence, as announced, we can iteratively compute β_N, α_N and the set of partial Brunovsky indices of $\mathcal{Y}^N$, $N \geq 1$, for sequences of vectors ($m = 1$ or $p = 1$).

We sketch the steps to be followed when $m = 1$ (for details see [4]).

Assume that $\mathcal{Y} = (Y_0, Y_1, \dots,)$, $Y_i \in \mathbb{F}^{p\times 1}$, then, for $i \geq 1$, $\beta_i = d_i$. The partial row Brunovsky indices $(s_1^i, \dots, s_i^i)$ of $\mathcal{Y}^i$ satisfy

$$s_j^i \geq s_j^{i-1}, \quad i \geq 1, \quad 1 \leq j \leq i \quad (s_i^{i-1} = 0).$$

Observe that if $\beta_N = \beta_{N-1}$, then $\alpha_N = \alpha_{N-1}$. And, if $\beta_N > \beta_{N-1}$, then it can be seen that

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

Hence, if for some $i \in \{1, \dots N-1\}$, $s_{i-1}^{N-1} = s_i^{N-1}$, then $\beta_N \neq N+1-i$.

When $N = 0$, take $\beta = 0$, $\alpha = 0$, $s = (0)$.

At step $i = N$, we first find the set $\mathcal{I} = \{i : 1 \leq i \leq \min\{N-\beta, \alpha+1\}, \ s_{i-1} \neq s_i\}$, where $s_0 = p$. 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 $t = \rho$ for all $j \in \mathcal{I}$, then $\beta = \beta$, $\alpha = \alpha$, $s = s$.

If for some $j \in \mathcal{I}$ we have $t > \rho$, then $\alpha = \max\{N-\beta, \alpha\}$, $s_i = s_i + 1$ for $j \leq i \leq N-\beta$, $\beta = N+1-j$, and we obtain the set of indices $\mathcal{R} = \{i : s_{i-1} = s_i\}$.

Once the partial Brunovsky indices are known, we can obtain minimal partial realizations of $\mathcal{Y}^N$ in controllability and observability reduced forms (see [4] for details): As $r_{\beta_N+1} = 0$, we have that $\operatorname{rank} H_{N-\beta_N,\beta_N+1}(\mathcal{Y}^N) = \operatorname{rank} H_{N-\beta_N,\beta_N}(\mathcal{Y}^N)$, which means that the last column of $H_{N-\beta_N,\beta_N+1}(\mathcal{Y}^N)$ is a linear combination of the columns of $H_{N-\beta_N,\beta_N}(\mathcal{Y}^N)$. The coefficients of the linear combination will be the parameters appearing in the controlability reduced form (see Example in the next Section).

Similarly, for each $1 \leq i \leq \alpha_N + 1$, in the last block row of $H_{i,N+1-i}(\mathcal{Y}^N)$ there are $s_{i-1} - s_i$ rows which depend linearly on the rest of rows of $H_{i,N+1-i}(\mathcal{Y}^N)$. The coefficients of the linear combinations will be the parameters appearing in the observability reduced form (see Example in the next Section).

IV. Example

Let $\mathbb{F} = \mathbb{R}$, $p = 4$,

$$\begin{aligned} \mathcal{Y}^{21} = \ & (e_3, e_3, 0, e_4, e_1+e_4, 0, e_2+e_3, e_2, e_1, e_3, 0, \\ & 0, 0, 0, 0, e_4, 0, 0, e_1, 0, 0), \end{aligned}$$

where, for $i = 1, \dots, 4$, e_i are the unit vectors in $\mathbb{R}^4$.

For this example, some of the intermediate results of the whole calculation appear in the next table:

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	$\beta_2 = 1,$	$\alpha_2 = 1,$	$s^2 = (1)$
8	$\beta_8 = 7,$	$\alpha_8 = 2,$	$s^8 = (4,3)$
9	$\beta_9 = 8,$	$\alpha_9 = 2,$	$s^9 = (4,4)$
10	$\beta_{10} = 8,$	$\alpha_{10} = 2,$	$s^{10} = (4,4)$
16	$\beta_{16} = 13,$	$\alpha_{16} = 6,$	$s^{16} = (4,4,2,1,1,1)$
17	$\beta_{17} = 15,$	$\alpha_{17} = 6,$	$s^{17} = (4,4,3,2,1,1)$
20	$\beta_{20} = 16,$	$\alpha_{20} = 6,$	$s^{20} = (4,4,3,3,1,1)$
21	$\beta_{21} = 17,$	$\alpha_{21} = 6,$	$s^{21} = (4,4,3,3,2,1)$

We explain next the calculations performed in some steps:

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

  $$\begin{aligned} \mathcal{I} = \ & \{i : 1 \leq i \leq \min\{N-\beta, \alpha+1\}\} \setminus \mathcal{R} \\ = \ & \{i : 1 \leq i \leq \min\{1,1\}\} \setminus \emptyset = \{1\}. \end{aligned}$$

  For $j = 1$, $\rho = s_1 = 0$, $t = \operatorname{rank} H_{1,1}(\mathcal{Y}^1) = \operatorname{rank} \begin{bmatrix} e_3 \end{bmatrix} > \rho$. 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 $N = 2$ (in step 1, $\beta = \beta_1 = 1$, $\alpha = \alpha_1 = 1$, $s = s^1 = (1)$, $\mathcal{R} = \emptyset$),

  $$\mathcal{I} = \{i : 1 \leq i \leq 1\} \setminus \emptyset = \{1\}.$$

  For $j = 1$, $\rho = s_1 = 1$, $t = \operatorname{rank} H_{1,2}(\mathcal{Y}^2) = \rho$.
  Then, $\beta = 1$, $\alpha = 1$, $s = (1)$, $\mathcal{R} = \emptyset$.
- At $N = 9$ (in step 8, $\beta = \beta_8 = 7$, $\alpha = \alpha_8 = 2$, $s = s^8 = (4,3)$, $\mathcal{R} = \{1\}$),

  $$\mathcal{I} = \{i : 1 \leq i \leq 2\} \setminus \{1\} = \{2\}.$$

  For $j = 2$, $\rho = s_1 + s_2 = 7$, $t = \operatorname{rank} H_{2,8}(\mathcal{Y}^9) = 8 > \rho$. Then $\alpha = \max\{9-7, 2\} = 2$, $s_i = s_i + 1$ for $2 \leq i \leq 2$, i.e. $s = (4,4)$, $\beta = 8$, and $\mathcal{R} = \{1,2\}$.
- At $N = 10$ (in step 9, $\beta = \beta_9 = 8$, $\alpha = \alpha_9 = 2$, $s = s^9 = (4,4)$, $\mathcal{R} = \{1,2\}$),

  $$\mathcal{I} = \{i : 1 \leq i \leq 2\} \setminus \{1,2\} = \emptyset.$$

  Then, $\beta = 8$, $\alpha = 2$, $s = (4,4)$, $\mathcal{R} = \{1,2\}$.
- At $N = 17$ (in step 16, $\beta = \beta_{16} = 13$, $\alpha = \alpha_{16} = 6$, $s = s^{16} = (4,4,2,1,1,1)$, $\mathcal{R} = \{1,2,5,6\}$),

  $$\mathcal{I} = \{i : 1 \leq i \leq 4\} \setminus \{1,2,5,6\} = \{3,4\}.$$

  For $j = 3$, $\rho = s_1 + s_2 + s_3 = 10$, $t = \operatorname{rank} H_{3,15}(\mathcal{Y}^{17}) = 11 > \rho$.
  Then $\alpha = \max\{17-13, 6\} = 6$, $s_i = s_i + 1$ for $3 \leq i \leq 4$, i.e. $s = (4,4,3,2,1,1)$, $\beta = 15$, and $\mathcal{R} = \{1,2,6\}$.
- At $N = 21$ (in step 20, $\beta = \beta_{20} = 16$, $\alpha = \alpha_{20} = 6$, $s = s^{20} = (4,4,3,3,1,1)$, $\mathcal{R} = \{1,2,4,6\}$),

  $$\mathcal{I} = \{i : 1 \leq i \leq 5\} \setminus \{1,2,4,6\} = \{3,5\}.$$

  For $j = 3$, $\rho = s_1 + s_2 + s_3 = 11$, $t = \operatorname{rank} H_{3,19}(\mathcal{Y}^{21}) = 11 = \rho$.
  For $j = 5$, $\rho = s_1 + \cdots + s_5 = 15$, $t = \operatorname{rank} H_{5,17}(\mathcal{Y}^{21}) = 16 > \rho$.
  Then $\alpha = \max\{21-16, 6\} = 6$, $s_i = s_i + 1$ for $5 \leq i \leq 5$, i.e. $s = (4,4,3,3,2,1)$, $\beta = 17$, and $\mathcal{R} = \{1,2,4\}$.

As an example, we obtain a minimal partial realization and a right and a left matrix generators of $\mathcal{Y}^8$ ($\beta_8 = 7$, $\alpha_8 = 2$, $s^8 = (4,3)$).

As $\beta_8 = 7$, we know that $\operatorname{rank} H_{1,8}(\mathcal{Y}^8) = \operatorname{rank} H_{1,7}(\mathcal{Y}^8)$, which means that $Y_7 = e_2$ is a linear combination of the columns of $H_{1,7}(\mathcal{Y}^8)$. Solving the system

$$H_{1,7}(\mathcal{Y}^8) \begin{bmatrix} b_7 \\ \vdots \\ b_1 \end{bmatrix} = e_2,$$

the solution depends on 3 free parameters $a, b, c \in \mathbb{R}$:

$$b_7 = a,\ b_6 = -1-a,\ b_5 = b,\ b_4 = b_3 = 0,\ b_2 = c, b_1 = 1.$$

Then, all the minimal partial realizations of $\mathcal{Y}^8$ in reduced controllability form are

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

$$C_c = \begin{bmatrix} e_3 & e_3 & 0 & e_4 & e_1 + e_4 & 0 & e_2 + e_3 \end{bmatrix},$$

with $a, b, c \in \mathbb{R}$. Equivalently, all the rigth matrix generators of minimal length of $\mathcal{Y}^8$ are

$$C_R(D) = 1 + D + cD^2 + bD^5 + (-1-a)D^6 + aD^7,\ a, b, c \in \mathbb{R}.$$

To find the minimal partial realizations in reduced observability form, we proceed analogously by rows. If $\hat{H}_2(\mathcal{Y}^8) = H_2(\mathcal{Y}^8)(\{1,2,3,4,6,7,8\}, :)$ and $\hat{H}_3(\mathcal{Y}^8) = H_3(\mathcal{Y}^8)(\{1,2,3,4,6,7,8\}, :)$, then

$$H_2(\mathcal{Y}^8)(5, :) = \begin{bmatrix} -1 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \hat{H}_2(\mathcal{Y}^8),$$

$$H_3(\mathcal{Y}^8)(\{10, 11, 12\}, :) = \begin{bmatrix} 1 & a & 0 & 0 & 1 & 0 & 0 \\ 1 & b & 0 & 0 & 0 & 0 & 0 \\ 1 & c & 1 & -1 & 1 & -1 & 1 \end{bmatrix} \hat{H}_3(\mathcal{Y}^8),$$

with $a, b, c \in \mathbb{R}$. Then, all the minimal partial realizations of $\mathcal{Y}^8$ in reduced observability form are:

$$A_o = \begin{bmatrix} -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & a & 0 & 0 & 1 & 0 & 0 \\ 1 & b & 0 & 0 & 0 & 0 & 0 \\ 1 & c & 1 & -1 & 1 & -1 & 1 \end{bmatrix},\ B_o = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix},\ a, b, c \in \mathbb{R}$$

$$C_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

We know that the minimal length of a left matrix generator of $\mathcal{Y}^8$ is $\alpha_8 = 2$. And, from the dependence relations of some of the rows of the observability matrix of (A_o, B_o, C_o) it can be seen that (see [4]), if

$$\begin{bmatrix} L_2 & L_1 \end{bmatrix} = \left[\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \\ 1 & a & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & c & 1 & -1 & 0 & 1 & -1 & 1 \end{array}\right],$$

then

$$\begin{bmatrix} Y_2 & Y_3 & \dots & Y_7 \end{bmatrix} = \begin{bmatrix} L_2 & L_1 \end{bmatrix} \begin{bmatrix} Y_0 & Y_1 & \dots & Y_5 \\ Y_1 & Y_2 & \dots & Y_6 \end{bmatrix}. \quad (1)$$

Hence, a left matrix generator of minimal length of $\mathcal{Y}^8$ is

$$C_L(D) = I_4 + L_1 D + L_2 D^2.$$

In fact, solving the system (1) we obtain that all the left matrix generators of minimal length of $\mathcal{Y}^8$ are $C_L(D) = I_4 + L_1 D + L_2 D^2$ with

$$\begin{bmatrix} L_2 & L_1 \end{bmatrix} = \left[\begin{array}{cccc|cccc} a_1 & b_1 & 0 & -a_1 & a_1 - 1 & 0 & 0 & 1 \\ a_2 & b_2 & 0 & 1 - a_2 & a_2 - 1 & 1 & 0 & 0 \\ a_3 & b_3 & 0 & 1 - a_3 & a_3 - 1 & 0 & 0 & 0 \\ a_4 & b_4 & 1 & -a_4 & a_4 - 1 & 1 & -1 & 1 \end{array}\right],$$

for $a_i, b_i \in \mathbb{R},\ 1 \leq i \leq 4$.

V. Conclusions

When extended to sequences of matrices, the Berlekamp-Massey algorithm can be interpreted as the problem of finding a minimal length right (left) matrix generator or a minimal realization of the sequence. We analyze these extensions and the relations between them.

Our work is strongly based on the paper [6]. We relate the partial Kronecker indices of a sequence with those of a subsequence. It allows us to characterize the length of the shortest right and left matrix generators of a sequence of matrices, and to extend the fundamental theorem on which the Berlekamp-Massey algorithm is based (Theorem 2.1), showing that in the matrix case the role of the minimal length of a register is split into the two parameters α and β (see Theorem 3.1). As far as we know, this is the first time that the relation between the partial Kronecker indices of a sequence and those of a subsequence has been analyzed.

We also provide an iterative method for obtaining α and β and the partial Kronecker indices of a sequence of vectors. Thanks to Theorem 3.1, the calculations in some steps can be skipped. Then, we can find minimal realizations in reduced controllability and observability forms. And from them, we also obtain minimal length right and left matrix generators of the sequence.

References

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

[2] A.C. Antoulas, On Recursiveness and Related Topics in Linear Systems, IEEE Transactions on Automatic Control, vol. AC-31, NO. 12, pp. 1121–1135, Dec. 1986.

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

[4] I. Baragaña, A. Roca, Linear feedback shift registers and the minimal realization problem, Submitted to Linear Algebra Appl.

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

[6] O.H. Bosgra, On parametrizations for the minimal partial realization problem, Systems & Control Letters, vol. 3, pp. 181-187, Sept. 1983.

[7] 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, vol. 37, NO. 5, pp. 1274–1287, Sept. 1991.

[8] E. Jonckheere, C. Ma, A simple Hankel interpretation of the Berlekamp-Massey algorithm, Linear Algebra Appl. vol. 125, pp. 65–76, Dec. 1989.

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

[10] M. Kuijper, An algorithm for constructing a minimal partial realization in the multivariable case, Systems & Control Letters, vol. 31, pp. 225–233, Sept. 1997.

[11] J.L. Massey, Shift-Register Synthesis and BCH Decoding, IEEE Transactions on Information Theory, vol. IT-15, NO. 1, pp. 122–127, Jan. 1969.

[12] S. Sakata, Extension of the Berlekamp-Massey Algorithm to N Dimensions, Information and Computation, vol. 84, pp. 207–239, Feb. 1990.