ON CONSTRUCTING A SHORTEST LINEAR RECURRENCE RELATION

Margreet Kuijper
Dept. of EE Engineering
University of Melbourne
Parkville, Vic., 3052
Australia
m.kuijper@ee.mu.oz.au

Jan C. Willems
Dept. of Mathematics
University of Groningen
P.O. Box 800, 9700 AV Groningen
The Netherlands
j.c.willems@math.rug.nl

Abstract

In 1968, Berlekamp and Massey presented an algorithm to compute a shortest linear recurrence relation for a finite sequence of numbers. It was originally designed for the purpose of decoding certain types of block codes. It later became important for cryptographic applications, namely for determining the complexity profile of a sequence of numbers. Here, we interpret the Berlekamp-Massey algorithm in a system-theoretic way. We explicitly present the algorithm as an iterative procedure to construct a behavior. We conclude that this procedure is the most efficient method for solving the scalar minimal partial realization problem.

1. Introduction

The present paper deals with the scalar minimal partial realization problem. This problem essentially coincides with the problem of finding a shortest linear recurrence relation for a given sequence of real numbers $a_1, a_2, \dots, a_N$, as will be explained below. Shortest linear recurrence relations are relevant in a coding theoretic context, namely for decoding BCH codes (see e.g. [5]) as well as in a cryptographic context, namely for defining the complexity profile of a sequence of numbers, see [11]. The connection between error-correction and minimal partial realizations is discussed in [12, 6, 1]. The length of the recurrence relation corresponds to the number of errors that have occurred in transmitting a message. It has to be minimized in maximum likelihood decoding when errors are assumed to be independent.

The problem of finding a shortest linear recurrence relation for a sequence $a_1, a_2, \dots, a_N$ is the following: find real numbers $c_1, c_2, \dots, c_L$, such that

$$a_{j+L} + c_1 a_{j+L-1} + \dots + c_L a_j = 0 \text{ for } j = 1, \dots, N-L. \quad (1)$$

Here L should be as small as possible in order to capture as much as possible of the structure underlying $a_1, a_2, \dots, a_N$. If $a_1, a_2, \dots, a_N$ does not allow any relation of the type (1) for $L < N$, then we set

$L = N$ and consider (1) to be trivially satisfied for any $c_1, c_2, \dots, c_N$. In the sequel, we denote a linear recurrence relation for $a_1, a_2, \dots, a_N$ by the polynomial $e(s) := s^L + c_1 s^{L-1} + \dots + c_L$; a shortest linear recurrence relation has minimal degree. Note that the polynomial e together with the initial values $a_1, a_2, \dots, a_L$ completely defines the original sequence. One can therefore view the problem of finding a shortest linear recurrence relation as a problem of data reduction.

The scalar minimal partial realization problem for a sequence $a_0, a_1, \dots, a_N$ is the following: find polynomials e and h for which

$$\frac{h(s)}{e(s)} = a_0 + a_1 s^{-1} + \dots + a_N s^{-N} + \phi(s) s^{-(N+1)},$$

such that $\deg e$ is as small as possible and ϕ is proper rational. It is not difficult to see that the denominator e of a minimal partial realization is a shortest linear recurrence relation for $a_1, a_2, \dots, a_N$. Vice versa, a shortest linear recurrence relation e for $a_1, a_2, \dots, a_N$ gives rise to a minimal partial realization for $a_0, a_1, \dots, a_N$ by defining $h(s) := p_0 s^L + p_1 s^{L-1} + \dots + p_L$ where, for $j = 0, 1, \dots, L$,

$$p_j := a_j + c_1 a_{j-1} + \dots + c_{j-1} a_1 + c_j a_0. \quad (2)$$

In this paper, we reformulate the above problem in a behavioral setting. This reformulation then provides a natural basis for an iterative solution, which we present in full detail. This solution is the Berlekamp-Massey algorithm from information theory. Here, we adhere to the version as presented in [5, p. 180], which is the original algorithm from [4, p. 184] with a modification from [10]. Our approach has enabled a system-theoretic explanation of the algorithm. For details on this and the connection with coding theory, the reader is referred to [7].

In the sequel, we put ideas from [14] to work. We take a behavioral point of view and first need to introduce some basic ideas of the behavioral approach.

2. Preliminaries on modeling of behaviors

In the behavioral approach [13]–[15], a system is essentially defined as a behavior $\mathcal{B}$ which is a set of trajectories; in this paper we consider linear, shift-invariant behaviors on the time-set $\mathbf{Z}_+$ of the form $\mathcal{B} = \ker R(\sigma)$, where R is a polynomial $g \times q$ -matrix and σ is the backward shift operator. In other words, $\mathcal{B}$ consists of trajectories $w : \mathbf{Z}_+ \mapsto \mathbf{R}^q$, for which

$$R(\sigma)w = 0. \quad (3)$$

The representation (3) is called a *kernel representation* of $\mathcal{B}$.

In the next section, we also need to consider behaviors on $\mathbf{Z}$. However, in this section, the time-set is assumed to be $\mathbf{Z}_+$. Let us repeat some notions from [13], and start with the following lemma (see e.g. [8, Th. 3.9] for a detailed proof).

Lemma 1 Let $R_1 \in \mathbf{R}^{g_1 \times q}[s]$ and $R_2 \in \mathbf{R}^{g_2 \times q}[s]$. Then

$$\ker R_1(\sigma) \subset \ker R_2(\sigma)$$

if and only if there exists a polynomial matrix $F \in \mathbf{R}^{g_2 \times g_1}[s]$ such that

$$R_2 = FR_1.$$

◇

It is a corollary of the above lemma that polynomial matrices R_1 and R_2 of full row rank represent the same behavior if and only if there exists a unimodular matrix U (i.e., a polynomial matrix with constant nonzero determinant) such that $R_1 = UR_2$.

The behavioral approach can be used for obtaining models from a set of observed time series. The general ideas stem from [14]. In this section, we restrict ourselves to exact modeling of discrete-time series, as presented in [15]. In the following, we briefly recall the basic concepts.

Let us assume that we have a *data set* $\mathbf{D} = \{\tilde{w}_0, \tilde{w}_1, \dots, \tilde{w}_N\}$ where $\tilde{w}_i \in (\mathbf{R}^q)^{\mathbf{Z}_+}$ are observed trajectories ($i = 0, 1, \dots, N$). A behavior $\mathcal{B}$ is called an *unfalsified model* for $\mathbf{D}$ if $\mathbf{D} \subseteq \mathcal{B}$. A model $\mathcal{B}_1$ is called *more powerful* than a model $\mathcal{B}_2$ if $\mathcal{B}_1 \subseteq \mathcal{B}_2$. A model $\mathcal{B}^*$ is called the *most powerful unfalsified model (MPUM)* for $\mathbf{D}$, if $\mathcal{B}^*$ is unfalsified for $\mathbf{D}$ and $\mathbf{D} \subseteq \mathcal{B} \implies \mathcal{B}^* \subseteq \mathcal{B}$. It has been shown in [14] that a unique MPUM $\mathcal{B}^*$ exists for $\mathbf{D}$. Note, however, that a kernel representation (3) of $\mathcal{B}^*$ is far from unique. In fact, any other kernel representation can be obtained by left multiplication by a unimodular matrix.

Example 2 ($\mathbf{T} = \mathbf{Z}_+$ and $q = 2$) Let $\mathbf{D} = \{\tilde{w}_0\}$, with

$$\tilde{w}_0 = \left(\begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots \right).$$

The MPUM is a three-dimensional vector space: $\mathcal{B}^* = \text{span} \{\tilde{w}_0, \sigma\tilde{w}_0, \sigma^2\tilde{w}_0\}$. A kernel representation of $\mathcal{B}^*$ is given by

$$\begin{bmatrix} 1 & -1 - 2\sigma - 3\sigma^2 \\ 0 & \sigma^3 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Alternative kernel representations of $\mathcal{B}^*$ are e.g.

$$\begin{bmatrix} 1 - 2\sigma + \sigma^2 & -1 \\ \sigma^3 & 0 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 2 - 3\sigma & -2 - \sigma \\ -\sigma + 2\sigma^2 & \sigma \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \quad (4)$$

◇

We are now ready to present the procedure of [15, p. 289], which underlies the iterative partial realization algorithm of section 4. The procedure provides a framework for the iterative construction of a kernel representation of the MPUM for $\mathbf{D} = \{\tilde{w}_0, \tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_N\}$. It can be easily understood from Lemma 1.

Procedure 3 ([15]) Initially define

$$R_{-1} := I \quad (\text{where } I \text{ is the identity matrix}).$$

Proceed iteratively as follows for $k = 0, \dots, N$. Define, after receiving $\{\tilde{w}_0, \tilde{w}_1, \dots, \tilde{w}_k\}$, the *k-th error trajectory* $\tilde{e}_k$ as

$$\tilde{e}_k := R_{k-1}(\sigma)\tilde{w}_k.$$

Compute a kernel representation $V_k(\sigma)w = 0$ of the MPUM for $\{\tilde{e}_k\}$. Then define

$$R_k := V_k R_{k-1}.$$

◇

Theorem 4 ([15]) For $k = 0, \dots, N$, the kernel representation $R_k(\sigma)w = 0$ of the above procedure, represents the MPUM for $\{\tilde{w}_0, \tilde{w}_1, \dots, \tilde{w}_k\}$. ◇

Next, we recall the notion of *controllability* from [13]. For the purpose of this paper, we consider the following as a definition: a behavior $\mathcal{B} = \ker R(\sigma)$ on $\mathbf{Z}_+$ is controllable if $R(s)$ has constant rank for all $s \in \mathbf{C}$. For the specific case that $q = 2$, it follows from Lemma 1 that two distinct nontrivial controllable models $\mathcal{B}_1$ and $\mathcal{B}_2$ that are unfalsified for the same data set, are “incomparable”, i.e., neither $\mathcal{B}_1 \subseteq \mathcal{B}_2$ nor $\mathcal{B}_2 \subseteq \mathcal{B}_1$. However, an ordering can still be introduced on the basis of the “complexity” of a model. As a measure of complexity we introduce the *order* $n(\mathcal{B})$ of a behavior. Since this concept will also be important for noncontrollable behaviors, we give

a general definition: the order $n(\mathcal{B})$ is defined as the minimum value of the sum of the row degrees of R where the minimum is taken over all possible kernel representations (3) of $\mathcal{B}$. This minimum is attained exactly when R is "row reduced".

Definition 5 Let $R \in \mathbb{R}^{q \times q}[s]$ have full row rank. Let $R_d \in \mathbb{R}^{q \times q}$ to be the *leading row coefficient matrix* of R , i.e., the constant matrix that consists of the coefficients of the highest degree terms in each row of R . Define R to be *row reduced* if R_d has full row rank. $\diamond$

When a matrix R is not row reduced, a unimodular matrix U can be found such that UR is row reduced. A procedure is given in [16, p. 27], see also [8, p. 24] where it is shown that not only the sum of the minimal row degrees is an invariant of a behavior, but also the minimal row degrees themselves are invariants of a behavior. For example, the minimal row degrees of $\mathcal{B}$ in Example 2 are 1 and 2; this can be seen from the row reduced representation (4).

In accordance with [2], for $q = 2$, we call a model $\mathcal{B}$ a *controllable-minimal complexity unfalsified model (C-MCUM)* for $\mathbf{D}$ if $\mathcal{B}$ is controllable, unfalsified for $\mathbf{D}$ and of least order among all controllable unfalsified models for $\mathbf{D}$.

3. Partial realization as exact modeling

In this section, we put the minimal partial realization problem in a behavioral framework. Let us first define an *impulse response extension* of $a_0, a_1, \dots, a_N$ as a trajectory $\mathbf{i}$ from $\mathbf{Z}$ to $\mathbb{R}^2$ which satisfies

$$\begin{aligned} \mathbf{i}(t) &= \begin{bmatrix} 0 \\ 0 \end{bmatrix} & \text{for } t < 0 \\ \mathbf{i}(0) &= \begin{bmatrix} a_0 \\ 1 \end{bmatrix} \\ \mathbf{i}(t) &= \begin{bmatrix} a_t \\ 0 \end{bmatrix} & \text{for } t = 1, \dots, N. \end{aligned}$$

Let e be a linear recurrence relation for $a_1, a_2, \dots, a_N$ and let h be defined by (2). Then there exists an impulse response extension $\mathbf{i}$, for which

$$\begin{bmatrix} e(\sigma) & -h(\sigma) \end{bmatrix} \mathbf{i} = 0. \quad (5)$$

For sake of completeness, we mention that for $t = N + 1, \dots$ $\mathbf{i}(t)$ will be given by

$$\mathbf{i}(t) = \begin{bmatrix} -(c_1 a_{t-1} + \dots + c_L a_{t-L}) \\ 0 \end{bmatrix}.$$

The polynomials e and h are necessarily coprime if e is a shortest linear recurrence relation. A behavioral reformulation of the minimal partial realization problem is thus to find a (controllable) representation

$$\begin{bmatrix} e(\sigma) & -h(\sigma) \end{bmatrix} \mathbf{w} = 0$$

of minimal degree that models an impulse response extension of $a_0, a_1, \dots, a_N$. We now work towards a reformulation in terms of trajectories on $\mathbf{Z}_+$ rather than $\mathbf{Z}$. The idea of reformulating partial realizations in terms of behaviors on a half-axis can also be found in [3], where the choice is made for $\mathbf{Z}_-$ rather than $\mathbf{Z}_+$.

As a first step, we observe that the above problem is essentially a problem on the time-set $\mathbf{T} = (-\infty, N]$. Indeed, (5) implies that

$$(\sigma^*)^L \begin{bmatrix} e(\sigma) & -h(\sigma) \end{bmatrix} \mathbf{i}_{(-\infty, N]} = 0, \quad (6)$$

where σ^* is the forward shift and $\mathbf{i}_{(-\infty, N]}$ is the truncated impulse response, defined on $(-\infty, N]$ as

$$\mathbf{i}_{(-\infty, N]} = \left(\dots, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} a_0 \\ 1 \end{bmatrix}, \begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} a_N \\ 0 \end{bmatrix} \right).$$

Defining the *reciprocal* $V^r(s)$ of a polynomial matrix $V(s) = V_n s^n + V_{n-1} s^{n-1} + \dots + V_1 s + V_0$ ($V_n \neq 0$) by $V^r(s) := V_n + V_{n-1} s + \dots + V_1 s^{n-1} + V_0 s^n$, we introduce polynomials c and p by

$$\begin{bmatrix} c & p \end{bmatrix} := \begin{bmatrix} e & h \end{bmatrix}^r.$$

Note that then $c(0) \neq 0$, the row degree of $\begin{bmatrix} c & p \end{bmatrix}$ equals the row degree of $\begin{bmatrix} e & h \end{bmatrix}$ and that coprimeness of e and h implies coprimeness of c and p . Equation (6) is rewritten as

$$\begin{bmatrix} c(\sigma^*) & -p(\sigma^*) \end{bmatrix} \mathbf{i}_{(-\infty, N]} = 0. \quad (7)$$

For notational purposes, we now reverse time and replace the time-set $(-\infty, N]$ by $\mathbf{Z}_+$. We define the trajectory $\tilde{\mathbf{w}}_N$ from $\mathbf{Z}_+$ to $\mathbb{R}^2$ by

$$\tilde{\mathbf{w}}_N = \left(\begin{bmatrix} a_N \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \begin{bmatrix} a_0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots \right). \quad (8)$$

Then (7) translates to

$$\begin{bmatrix} c(\sigma) & -p(\sigma) \end{bmatrix} \tilde{\mathbf{w}}_N = 0.$$

At this stage the following theorem is easy to prove:

Theorem 6 Let $\tilde{\mathbf{w}}_N$ be defined by (8). Let

$$\begin{bmatrix} c(\sigma) & -p(\sigma) \end{bmatrix} \mathbf{w} = 0$$

be a kernel representation of degree L of a C-MCUM for $\{\tilde{\mathbf{w}}_N\}$ with $c(0) \neq 0$. Define polynomials e and h by $\begin{bmatrix} e & h \end{bmatrix} := \begin{bmatrix} c & p \end{bmatrix}^r$. Then e is a shortest linear recurrence relation for $a_1, a_2, \dots, a_N$ and h/e is a minimal partial realization for $a_0, a_1, \dots, a_N$. $\diamond$

Our final reformulation of the minimal partial realization problem is therefore:

Problem Statement: find a C-MCUM on $\mathbf{Z}_+$ for $\{\tilde{\mathbf{w}}_N\}$.

The MPUM for $\{\tilde{w}_N\}$ simply equals

$$\text{span } \{\sigma^N \tilde{w}_N, \sigma^{N-1} \tilde{w}_N, \dots, \sigma \tilde{w}_N, \tilde{w}_N\}.$$

As noted in [3], a kernel representation for it is given by $A(\sigma)w = 0$, where

$$A(s) = \begin{bmatrix} 1 & -(a_0 + a_1 s + \dots + a_N s^N) \\ 0 & s^{N+1} \end{bmatrix}. \quad (9)$$

Approach: construct a row reduced representation of the MPUM for $\{\tilde{w}_N\}$.

One of the rows of that representation represents the C-MCUM for $\{\tilde{w}_N\}$, see also [2, 3]. The details are given in the next theorem.

Theorem 7 Let $\tilde{w}_N$ be defined by (8). Let the MPUM for $\{\tilde{w}_N\}$ be given by

$$R(\sigma)w = 0 \quad \text{with } R = \begin{bmatrix} c & -p \\ f & -g \end{bmatrix}. \quad (10)$$

Assume that $c(0) \neq 0$ and that R is row reduced with row degrees κ_1 and κ_2 . If $\kappa_1 \leq \kappa_2$ and/or $f(0) = 0$, then

$$\begin{bmatrix} c(\sigma) & -p(\sigma) \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = 0 \quad (11)$$

represents a C-MCUM for $\{\tilde{w}_N\}$.

Proof First observe that, by Lemma 1, there exists a unimodular matrix U , such that

$$R(s) = U(s) \begin{bmatrix} 1 & -(a_0 + a_1 s + \dots + a_N s^N) \\ 0 & s^{N+1} \end{bmatrix}.$$

As a result, $R(s)$ can only lose rank at $s = 0$, so that f and g have no common zeros, except possibly at $s = 0$. We have to prove that a representation

$$\begin{bmatrix} d(\sigma) & -n(\sigma) \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = 0$$

that constitutes a controllable unfalsified model for $\{\tilde{w}_N\}$, necessarily has row degree $\geq \kappa_1$. If

$$\det \begin{bmatrix} d & -n \\ f & -g \end{bmatrix} \neq 0, \quad (12)$$

then this would give rise to an unfalsified finite-dimensional model for $\{\tilde{w}_N\}$, which necessarily has first row degree $\geq \kappa_1$, because of the assumption that R is row reduced. Now, if $f(0) = 0$, then necessarily (12) holds, since otherwise $\deg [d \quad -n] < \kappa_2$, so that

$$\begin{bmatrix} c(\sigma) & -p(\sigma) \\ d(\sigma) & -n(\sigma) \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

would be an unfalsified finite-dimensional model for $\{\tilde{w}_N\}$ of order $< \kappa_1 + \kappa_2$, which contradicts the rowreducedness of R . Next, if $f(0) \neq 0$, then (12) can only

hold if $\deg [d \quad -n] = \kappa_2$. By assumption, we have that in this case, $\kappa_2 \geq \kappa_1$, so that $\deg [d \quad -n] \geq \kappa_1$. $\diamond$

For constructing a row reduced representation of the MPUM, one can take two different approaches.

- (I) make the polynomial matrix A in (9) row reduced, i.e., construct a unimodular matrix U such that UA is row reduced
- (II) Use the data $a_0, a_1, \dots, a_N$ iteratively: at each step, construct a row reduced representation of the MPUM corresponding to $a_0, a_1, \dots, a_k$ ($k = 0, \dots, N$). For this, use the iterative modeling Procedure 3, applied to $\{\sigma^N \tilde{w}_N, \sigma^{N-1} \tilde{w}_N, \dots, \sigma \tilde{w}_N, \tilde{w}_N\}$.

For (I), the procedure of [16] can be used. The algorithm is then essentially the euclidean algorithm, applied to the polynomials s^{N+1} and $a_0 + a_1 s + \dots + a_N s^N$, as shown in detail in [9]. For (II), the row of R_k of smallest degree that does not lose rank at $s = 0$, represents the C-MCUM at step k . One can therefore think of an iterative procedure that requires a check on the value at $s = 0$ and the row degrees at each step, as in [2, p. 1795] and [3]. However, such a check is not needed if we choose the V_k 's in such a way that the R_k 's are not only row reduced, but also have a second row that loses rank at $s = 0$. Then, by Theorem 7, the C-MCUM at step k is *unambiguously* given by the first row of R_k . This is the clever idea behind the iterative algorithm of the next section, which is the Berlekamp-Massey algorithm: the most efficient algorithm for solving the scalar minimal partial realization problem.

Remark 8 If a representation (10) of the MPUM for $\{\tilde{w}_N\}$ is row reduced and $f(0) = 0$, then a parametrization of all C-MCUM's, represented by

$$\begin{bmatrix} d(\sigma) & -n(\sigma) \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = 0,$$

is given by

$$\begin{bmatrix} d & -n \end{bmatrix} = \begin{bmatrix} 1 & \alpha \end{bmatrix} \begin{bmatrix} c & -p \\ f & -g \end{bmatrix}.$$

Here α is a polynomial with $\deg \alpha = 2\kappa_1 - (N+1)$ for $\kappa_1 \geq (N+1)/2$ and $\alpha = 0$ for $\kappa_1 < (N+1)/2$. In particular, a C-MCUM is unique if and only if $\kappa_1 < (N+1)/2$. The above parametrization can also be found in [2, 10]. $\diamond$

4. An iterative algorithm

In this section, we present our main result by working out the above option (II) in detail.

For $k = 0, \dots, N$, let $\tilde{w}_k := \sigma^{N-k} \tilde{w}_N$, where $\tilde{w}_N$ is defined by (8). Applying Procedure 3 to the data set $\{\tilde{w}_0, \tilde{w}_1, \dots, \tilde{w}_N\}$, we get error trajectories $\tilde{e}_k$, for which

$$\sigma \tilde{e}_k = \sigma R_{k-1}(\sigma) \tilde{w}_k = R_{k-1}(\sigma) \tilde{w}_{k-1} = 0.$$

Consequently, $\tilde{e}_k$ is of the simple form

$$\tilde{e}_k = \left(\begin{bmatrix} \Delta_k \\ \tilde{\Delta}_k \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots \right).$$

Define L_k and $\tilde{L}_k$ as the degree of the first and the second row of R_k , respectively. Define the update matrix V_k as

$$V_k(s) := \begin{bmatrix} \tilde{\Delta}_k & -\Delta_k \\ 0 & s \end{bmatrix} \quad \text{if } \Delta_k = 0$$

or $L_{k-1} > \tilde{L}_{k-1}$,

$$V_k(s) := \begin{bmatrix} \tilde{\Delta}_k & -\Delta_k \\ s/\Delta_k & 0 \end{bmatrix} \quad \text{otherwise.}$$

Clearly, in both cases, $V_k(\sigma)w = 0$ represents the MPUM for $\{\tilde{e}_k\}$. Consequently, $R_k(\sigma)w = 0$ represents the MPUM for $\{\tilde{w}_k\}$ (Theorem 4). It can be proven by induction that $\tilde{\Delta}_k = 1$ for $k = 0, \dots, N$. It also follows by induction that the above choice of the V_k 's ensures that each R_k is row reduced ($k = -1, 0, \dots, N$). Indeed, R_{-1} is trivially row reduced and the assumption that R_{k-1} is row reduced, implies that R_k is row reduced: if $\Delta_k = 0$ or

$$L_{k-1} > \tilde{L}_{k-1}, \quad (13)$$

then

$$R_k(s) = \begin{bmatrix} 1 & -\Delta_k \\ 0 & s \end{bmatrix} R_{k-1}(s)$$

is clearly row reduced again; note that then $L_k = L_{k-1}$. If $\Delta_k \neq 0$ and $L_{k-1} \leq \tilde{L}_{k-1}$, then

$$R_k(s) = \begin{bmatrix} 1 & -\Delta_k \\ s/\Delta_k & 0 \end{bmatrix} R_{k-1}(s)$$

is again row reduced; note that then

$$L_k = \tilde{L}_{k-1}. \quad (14)$$

Finally, it can be proven by induction that

$$R_k(0) = \begin{bmatrix} 1 & -a_0 \\ 0 & 0 \end{bmatrix} \quad \text{for } k = 0, \dots, N, \quad (15)$$

so that, by Theorem 7, we may conclude that the first row of R_k gives rise to a C-MCUM for $\{\tilde{w}_k\}$.

In order to be able to write the algorithm in compact form, we note that $\det R_k(s) = s^{k+1}$, so that

$$L_k + \tilde{L}_k = k + 1. \quad (16)$$

As a result, condition (13) coincides with the condition $L_{k-1} > k/2$, whereas the "jump" (14) translates into $L_k = k - L_{k-1}$. Let us denote

$$R_k := \begin{bmatrix} c_k & -p_k \\ f_k & -g_k \end{bmatrix}.$$

By definition, the number Δ_k is the coefficient of s^k in $(a_0 + a_1s + \dots + a_k s^k)c_{k-1}(s) - p_{k-1}(s)$. This equals the coefficient of s^k in $(a_0 + a_1s + \dots + a_k s^k)c_{k-1}(s)$ because of the fact that $\deg p_{k-1} < k$ (use (15) and (16)).

Below, we rewrite the above algorithm in compact form. The resulting algorithm is a slightly generalized version of the Berlekamp-Massey algorithm, in the sense that a_0 is not fixed (the Berlekamp-Massey algorithm sets $a_0 = 1$).

Algorithm 9

Denote $c_k := \begin{bmatrix} 1 & 0 \end{bmatrix} R_k \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Initially define

$$R_{-1} := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ and } L_{-1} := 0.$$

Proceed iteratively as follows for $k = 0, \dots, N$. Define, after receiving $a_0, a_1, \dots, a_k$, the number Δ_k as the coefficient of s^k in $(a_0 + a_1s + \dots + a_k s^k)c_{k-1}(s)$.

Compute the matrix R_k and the integer L_k as follows:

$$R_k := V_k R_{k-1},$$

where, if $\Delta_k = 0$ or $L_{k-1} > k/2$,

$$V_k(s) := \begin{bmatrix} 1 & -\Delta_k \\ 0 & s \end{bmatrix}; \quad L_k := L_{k-1},$$

and, if otherwise,

$$V_k(s) := \begin{bmatrix} 1 & -\Delta_k \\ s/\Delta_k & 0 \end{bmatrix}; \quad L_k := k - L_{k-1}$$

Then the first row of R_k represents a C-MCUM for $\{\tilde{w}_k\}$; the reciprocal of that row yields a minimal partial realization as in Theorem 6. $\diamond$

Example 10 Let $(a_0, a_1, a_2, a_3, a_4) = (0, 0, 1, 1, 0)$.

Application of the above algorithm yields:

$$\Delta_0 = 0, L_0 = 0, R_0 = \begin{bmatrix} 1 & 0 \\ 0 & s \end{bmatrix} R_{-1} = \begin{bmatrix} 1 & 0 \\ 0 & s \end{bmatrix},$$

$$\Delta_1 = 0, L_1 = 0, R_1 = \begin{bmatrix} 1 & 0 \\ 0 & s \end{bmatrix} R_0 = \begin{bmatrix} 1 & 0 \\ 0 & s^2 \end{bmatrix},$$

$$\Delta_2 = 1, L_2 = 2, R_2 = \begin{bmatrix} 1 & -1 \\ s & 0 \end{bmatrix} R_1 = \begin{bmatrix} 1 & -s^2 \\ s & 0 \end{bmatrix},$$

$$\begin{aligned}\Delta_3 = 1, L_3 = 2, R_3 &= \begin{bmatrix} 1 & -1 \\ 0 & s \end{bmatrix} R_2 \\ &= \begin{bmatrix} 1-s & -s^2 \\ s^2 & 0 \end{bmatrix},\end{aligned}$$

$$\begin{aligned}\Delta_4 = -1, L_4 = 2, R_4 &= \begin{bmatrix} 1 & 1 \\ -s & 0 \end{bmatrix} R_3 \\ &= \begin{bmatrix} 1-s+s^2 & -s^2 \\ -s+s^2 & s^3 \end{bmatrix}.\end{aligned}$$

As a result,

$$\begin{bmatrix} 1-\sigma+\sigma^2 & -\sigma^2 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = 0$$

represents a C-MCUM for $\{\tilde{w}_4\}$. Taking the reciprocal row vector, we get the (unique) minimal partial realization $1/(s^2 - s + 1)$. $\diamond$

5. Conclusions

The scalar partial realization problem has been considered as an instance of exact modeling of a behavior on a half-axis, as in [3]. Solutions within this framework are based on polynomials rather than Hankel matrices. A central role is played by systems that have no inputs. It is for this reason that the notion of a behavior rather than a transfer function is essential to the approach. We put the theory to work in deriving an efficient iterative solution: the celebrated Berlekamp-Massey algorithm. An interesting feature of the algorithm is that its efficiency is enhanced by the update at each step of four polynomials rather than two. It is a topic of future research to put this idea to work for identification purposes, in the context of approximate modeling. We believe that our approach presents a clear explanation of the Berlekamp-Massey algorithm.

6. Acknowledgement

We thank Jim L. Massey for pointing out the relevance of the Berlekamp-Massey algorithm for cryptographic applications.

References

- [1] Antoulas, A.C. (1986), On recursiveness and related topics in linear systems, *IEEE Trans. Aut. Control*, Vol. 31, No. 12, pp. 1121-1135
- [2] Antoulas, A.C. and J.C. Willems (1993), A behavioral approach to linear exact modeling, *IEEE Trans. Aut. Control*, Vol. 38, No. 12, pp. 1776-1802
- [3] Antoulas, A.C. (1994): Recursive modeling of discrete-time time series, in *Linear Algebra for Control Theory*, P. Van Dooren and B. Wyman (eds.), Springer-Verlag, IMA Vol. 62, pp. 1-20
- [4] Berlekamp, E.R. (1968) : *Algebraic Coding Theory*, New York, McGraw-Hill
- [5] Blahut, R.E. (1983) *Theory and Practice of Error Control Codes*, Addison-Wesley
- [6] Gragg, W.B. and A. Lindquist (1983): On the partial realization problem, *Lin. Alg. Appl.*, Vol. 50, pp. 277-319
- [7] Kuijper, M. and J.C. Willems (1995): The Berlekamp-Massey algorithm explained as iterative modeling of a behavior, submitted to *IEEE Trans. Info. Theory*
- [8] Kuijper, M. (1994): *First-Order Representations of Linear Systems*, Series on "Systems and Control: Foundations and Applications", Birkhäuser, Boston
- [9] Kuijper, M. (1995): Partial realization and the euclidean algorithm, submitted to *SIAM J. Control Opt.*
- [10] Massey, J.L. (1969): Shift-register synthesis and BCH decoding, *IEEE Trans. Inf. Theory*, Vol. IT-15, pp. 122-127
- [11] Rueppel, R.A. (1986): *Analysis and Design of Stream Ciphers*, Springer-Verlag
- [12] Sain, M.K. (1975): Minimal torsion spaces and the partial input/output problem, *Information and Control*, Vol. 29, No. 2, pp. 103-124
- [13] Willems, J.C. (1986): From time series to linear system. Part I: Finite-dimensional linear time invariant systems, *Automatica*, Vol. 22, pp. 561-580
- [14] Willems, J.C. (1986) : From time series to linear system. Part II: Exact modelling, *Automatica*, Vol. 22, No. 6, pp. 675-694
- [15] Willems, J.C. (1991) : Paradigms and puzzles in the theory of dynamical systems, *IEEE Trans. Aut. Control*, Vol. AC-36, pp. 259-294
- [16] Wolovich, W.A. (1974) : *Linear Multivariable Systems*, Springer Verlag, New York