BEHAVIORAL MODELS OVER RINGS—MINIMAL REPRESENTATIONS AND APPLICATIONS TO CODING AND SEQUENCES

Margreta Kuijper * **Xin-Wen Wu** *,1
Udaya Parampalli **

* *Dept. of Electrical and Electronic Engineering*
** *Dept. of Computer Science and Software Engineering*
The University of Melbourne, VIC 3010 Australia
E-mail: m.kuijper@ee.mu.oz.au, x.wu@ee.mu.oz.au, udaya@cs.mu.oz.au

Abstract: In this paper we consider polynomial kernel representations for behaviors. For behaviors over fields it is well-known that minimal representations, i.e. representations with minimal row degrees, are exactly those representations for which the polynomial matrix is row reduced. In this paper we consider behaviors over a particular type of ring, namely $\mathbb{Z}_{p^r}$, where p is a prime number and r is a positive integer. As a starting point in this investigation we focus on minimal partial realizations. These are equivalent to shortest linear recurrence relations. We present an algorithm that computes a parametrization of all shortest linear recurrence relations for a finite sequence in $\mathbb{Z}_{p^r}$. For this we extend well-known techniques developed by Reeds and Sloane in the 80's with methods from the theory of behavioral modeling.

Keywords: Behavior, shortest linear recurrence relation, systems over rings, minimality, minimal partial realization, parametrization

1. INTRODUCTION

In behavioral theory a central role is played by the set of trajectories $\mathcal{B}$ that belong to a dynamical system Σ. In fact, the dynamical system is defined as a triple $\Sigma = (\mathbb{T}, \mathbb{W}, \mathcal{B})$, where $\mathbb{T}$ is the time axis, $\mathbb{W}$ is the signal alphabet, and $\mathcal{B}$, the behavior of the system, is a subset of $\mathbb{W}^{\mathbb{T}}$. In this paper we consider dynamical systems $\Sigma = (\mathbb{Z}_+, \mathcal{R}^q, \mathcal{B})$, where $\mathcal{R}$ is the ring $\mathbb{Z}_{p^r}$ (with p a prime number and r a positive integer). We study the theory of representations for such systems, in particular kernel representations (defined below). For $r \geq 2$ the ring $\mathcal{R}$ is not a field. In this paper we see that some significant modifications are needed to the existing theory of behaviors over fields. It turns out that several issues concerning ring systems are much more complicated than their field counterparts.

This paper focuses on one of the classics of systems theory, namely the minimal partial realization problem. Its main result is a constructive solution to this problem over the finite ring $\mathcal{R} = \mathbb{Z}_{p^r}$. The result can be generalized to products of finite chain rings, such as $\mathbb{Z}_m$ with $m \in \mathbb{Z}$. The minimal partial realization problem links several discipilines. Coding-theoretic applications of the results of this paper are found in the decoding of modulation codes as well as nonlinear codes,

[1] Supported by the Australian Research Council

whereas results are also relevant to cryptographic applications of ring sequences.

For behavioral systems over fields there exists a well-developed theory of representations. We define σ, the backward shift operator, acting on elements in $\mathbb{W}^{\mathbb{T}}$ as $(\sigma w)(k) = w(k+1)$. Any behavior over a field that is linear, σ-invariant and complete admits a kernel representation, that is, a representation of the form $R(\sigma)\boldsymbol{w} = 0$, where $R(\xi)$ is a polynomial matrix in the indeterminate ξ. As an example, for the system $\Sigma = (\mathbb{Z}_+, \mathbb{R}, \mathcal{B})$ with $\mathcal{B} =$ span $\{(3, 3, 3, \cdots)\}$ a kernel representation is given by $(\sigma - 1)\boldsymbol{w} = 0$.

It has been proven in (Fagnani and Zampieri, 1996) that the above result is also true in our ring case, i.e. any linear, shift-invariant and complete behavior over the ring $\mathcal{R}$ admits a kernel representation. However, there are some differences. For example, unlike the field case, for $q = 1$ there does not necessarily exist a 1×1 kernel representation, as is illustrated by the following example.

Example 1. Consider $\Sigma = (\mathbb{Z}_+, \mathbb{Z}_9, \mathcal{B})$ (i.e. $p = 3; r = 2$) with $\mathcal{B} =$ span $\{(3, 3, 3, \cdots)\}$. Then a kernel representation is given by

$$\begin{bmatrix} \sigma - 1 \\ 3 \end{bmatrix} \boldsymbol{w} = 0.$$

There exists no single polynomial $r(\xi)$ such that $\mathcal{B}$ is given by $r(\sigma)\boldsymbol{w} = 0$. Briefly, the reason for this is that the 1×2-matrix $[3 \quad 1 - \xi]$ cannot be extended to a 2×2-polynomial matrix that is unimodular over $\mathbb{Z}_9[\xi]$.

Thus we see that the existence of non-invertible elements in $\mathcal{R}$ has a considerable impact on the fundamentals of behavioral theory. Some of the issues have been addressed in (Fagnani and Zampieri, 1996; Fagnani and Zampieri, 1997; Fagnani and Zampieri, 2001).

In this paper we are interested in the further development of a theory of kernel representations for systems over $\mathcal{R}$. In particular we ask ourselves the following **Questions**:

(1) Given two behaviors $\mathcal{B}_1$ and $\mathcal{B}_2$ with kernel representations $R_1(\sigma)\boldsymbol{w} = 0$ and $R_2(\sigma)\boldsymbol{w} = 0$ respectively and $\mathcal{B}_1 \subseteq \mathcal{B}_2$, how are the polynomial matrices $R_1(\xi)$ and $R_2(\xi)$ related?

(2) (a corollary of 1)) Given a behavior $\mathcal{B}$ represented by $R_1(\sigma)\boldsymbol{w} = 0$ as well as $R_2(\sigma)\boldsymbol{w} = 0$, how are the polynomial matrices $R_1(\xi)$ and $R_2(\xi)$ related?

(3) Among all kernel representations of a behavior $\mathcal{B}$, how can we characterize a kernel representation $R(\sigma)\boldsymbol{w} = 0$ such that the row degrees of $R(\xi)$ are minimal?

The latter question relates to an open problem posed in (Fagnani and Zampieri, 1997), namely to derive a theory of row reduced kernel representations for systems over the ring $\mathcal{R}$.

In (Kuijper and Willems, 1997) the theory of kernel representations for behavioral systems over fields was employed to yield a constructive algorithm that solves the scalar minimal partial realization problem, see also (Antoulas, 1994). The algorithm was generalized to the multivariable case in (Kuijper, 1997). It is well-known that scalar minimal partial realizations are equivalent to shortest linear recurrence relations, a topic that is relevant to coding and cryptographic applications. In (Kuijper and Willems, 1997; Kuijper, 2001; Kuijper and Polderman, 2004) behavioral modeling and row reduced kernel representations were the main players in constructing a behavioral framework for several decoding methods for Reed-Solomon codes over fields.

Let us here present some definitions:

Definition 2. Let $a_1, a_2, \ldots, a_N$ be a finite sequence such that for $j = 1, 2, \ldots, N - L$

$$c_0 a_{j+L} + c_1 a_{j+L-1} + \cdots + c_L a_j = 0.$$

Then $c(\xi) := c_0 + c_1\xi + \cdots + c_L\xi^L$ is called an *annihilator* of length L for $a_1, \ldots, a_N$. An annihilator $c(\xi)$ for which $c_0 = 1$ is called a *linear recurrence relation* of length L for $a_1, \ldots, a_N$. In case L is minimal among all such linear recurrence relations, we call $c(\xi)$ a *shortest* linear recurrence relation for $a_1, \ldots, a_N$. The *linear complexity* of $a_1, \ldots, a_N$ is then defined as L.

Linear recurrence relations and annihilators over rings behave differently from their counterparts over fields, as illustrated by the next two examples.

Example 3. $N = 2$; $a_1 = 9, a_2 = 3$. Over the field $\mathbb{R}$ this sequence has complexity 1 and has a unique shortest linear recurrence relation, namely $c(\xi) = 1 - \frac{1}{3}\xi$. However, over the ring $\mathbb{Z}_{27}$ it has complexity 2; any polynomial $c(\xi)$ of degree 2 for which $c(0) = 1$ serves as a shortest linear recurrence relation. On the other hand a shortest annihilator is $c(\xi) = 9$, which has length 0.

Example 4. $N = 2$; $a_1 = 6, a_2 = 3$. Over the field $\mathbb{R}$ this sequence has complexity 1 and has a unique shortest linear recurrence relation, namely $c(\xi) = 1 - \frac{1}{2}\xi$. Over the ring $\mathbb{Z}_9$ the sequence also has complexity 1 but no unique shortest linear recurrence relation. Indeed, the polynomials $1 -$

5ξ, $1-2\xi$ and $1-8\xi$ all serve as a shortest linear recurrence relation for this sequence.

In this paper we address the problem of constructing a shortest linear recurrence relation. For sequences over a field this problem is solved by several well-known methods, e.g. the Berlekamp-Massey algorithm (Berlekamp, 1968; Massey, 1969). For sequences over the ring $\mathcal{R}$ an algorithm was presented in (Reeds and Sloane, 1985). In this paper we extend the techniques of (Reeds and Sloane, 1985) with methods from the theory of behavioral modeling to arrive at an explicit behavioral model of the data. This then has the advantage that it allows for the derivation of a parametrization of *all* shortest linear recurrence relations for a sequence over $\mathcal{R}$. The parametrization problem was posed as an open problem in (Norton, 1999). In section 4 we present the parametrization.

In addressing the above specific problem we consider a specific system namely $\Sigma = (\mathbb{Z}_+, \mathcal{R}^2, \mathcal{B})$ with

$$\mathcal{B} = \text{ span } \{\boldsymbol{b}, \sigma\boldsymbol{b}, \sigma^2\boldsymbol{b}, , \ldots, \sigma^N\boldsymbol{b}\}, \qquad (1)$$

where

$$\boldsymbol{b} = \left(\begin{bmatrix} a_N \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots \right). \qquad (2)$$

Note that $\boldsymbol{b}$ is defined as in the field case (Kuijper and Willems, 1997) and can be interpreted as an inverted and truncated impulse response. In the context of the search for shortest linear recurrence relations for $a_1, \ldots, a_N$ we then address the above Questions **(1)**-**(3)**.

2. SOME GENERAL RESULTS ON BEHAVIORS OVER THE RING $\mathcal{R}$

Several results from the field case directly carry over to the ring case. One of these is the next lemma which gives the answer to Question **(1)** of the previous section and is a generalization of a result in (Schumacher, 1988), see also Th. 3.7 in (Kuijper, 1994).

Lemma 5. For $i = 1, 2$ let $R_i(\xi) \in \mathcal{R}^{g_i \times q}[\xi]$ and denote the corresponding behaviors by $\mathcal{B}_i = \ker R_i(\sigma)$. If $\mathcal{B}_1 \subset \mathcal{B}_2$, then there exists a matrix $F(\xi) \in \mathcal{R}^{g_2 \times g_1}[\xi]$ such that $R_2(\xi) = F(\xi)R_1(\xi)$.

The next lemma answers Question **(2)** of the previous section.

Lemma 6. For $i = 1, 2$ let $R_i(\xi) \in \mathcal{R}^{g_i \times q}[\xi]$ with $g_2 \geq g_1$. Then $R_1(\sigma)\boldsymbol{w} = 0$ and $R_2(\sigma)\boldsymbol{w} = 0$ represent the same behavior iff there exists a matrix $F(\xi) \in \mathcal{R}^{g_2 \times g_1}[\xi]$ such that

$$R_2(\xi) = F(\xi)R_1(\xi)$$

with $\ker F(\sigma) \cap \text{ im } R_1(\sigma) = \{0\}$.

Let us finally repeat some standard notions and terminology from (Willems, 1986; Willems, 1991) and assume that we have a *data set* $\mathbf{D} = \{\boldsymbol{b_1}, \ldots, \boldsymbol{b}_\nu\}$ where $\boldsymbol{b}_i \in (\mathcal{R}^q)^{\mathbb{Z}_+}$ are observed trajectories ($i = 1, \ldots, \nu$). 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 $\mathbf{D} \subseteq \mathcal{B} \implies \mathcal{B}^* \subseteq \mathcal{B}$. In this paper we focus on the MPUM $\mathcal{B}$ of the simple data set $\mathbf{D} = \{\boldsymbol{b}\}$, where $\boldsymbol{b}$ is defined by (2). Of course $\mathbf{D}$ can also be written as $\mathbf{D} = \{\boldsymbol{b}, \sigma\boldsymbol{b}, \sigma^2\boldsymbol{b}, , \ldots, \sigma^N\boldsymbol{b}\}$. In the next section we seek to iteratively model $\mathbf{D}$, i.e. first consider the MPUM of $\{\sigma^N\boldsymbol{b}\}$, then extend this behaviour to the MPUM of $\{\sigma^N\boldsymbol{b}, \sigma^{N-1}\boldsymbol{b}\}$, etcetera. We use the iterative modeling procedure of (Willems, 1991) to ultimately construct a kernel representation of $\mathcal{B}$.

We conclude this section with a fundamental result on the ring $\mathcal{R} = \mathbb{Z}_{p^r}$ that will be instrumental later on.

Property 1 Any nonzero $a \in \mathbb{Z}_{p^r}$ can be written as $a = \theta p^u$, where θ is a unit in $\mathbb{Z}_{p^r}$ and u is an integer with $0 \leq u \leq r-1$.

3. MODELLING THE IMPULSE RESPONSE BEHAVIOR

In this section we concentrate on the impulse response behavior $\mathcal{B} = \text{ span } \{\boldsymbol{b}, \sigma\boldsymbol{b}, \sigma^2\boldsymbol{b}, , \ldots, \sigma^N\boldsymbol{b}\}$, where $\boldsymbol{b}$ is defined as in (2). The next lemma establishes the relationship between annihilators for $a_1, \ldots, a_N$ (as introduced in Definition 2) and difference equations involving trajectories of time.

Lemma 7. The polynomial $c(\xi)$ is an annihilator of length L for $a_1, \ldots, a_N$ iff there exists a polynomial $\omega(\xi)$ such that row deg $[c(\xi) \quad \omega(\xi)] = L$, i.e. max $\{$ deg $c(\xi)$, deg $\omega(\xi)\} = L$, and

$$[c(\sigma) \quad \omega(\sigma)]\,\boldsymbol{b} = 0.$$

Thus searching for a shortest linear recurrence relation amounts to searching for a 1×2 kernel representation $[c(\sigma) \quad \omega(\sigma)]\,\boldsymbol{w} = 0$ whose behavior contains $\mathcal{B}$. This kernel representation should have minimal row degree and satisfy $c(0) = 1$.

Our strategy is now as follows: we construct a $g \times 2$ representation $R(\sigma)\boldsymbol{w} = 0$ of $\mathcal{B}$ such that the first

row of $R(\xi)$ gives the desired shortest linear recurrence relation. Of course a trivial representation for $\mathcal{B}$ is given by $A(\sigma)\boldsymbol{w} = 0$, where

$$A(\xi) = \begin{bmatrix} 1 & -(a_1\xi + \cdots + a_N\xi^N) \\ 0 & \xi^{N+1} \end{bmatrix}.$$

The first row of $A(\xi)$ is not necessarily a shortest linear recurrence relation. In fact, in our ring case it might not be possible to construct a 2×2 kernel representation with a shortest linear recurrence relation in the first row. Thus, unlike the field case, $g = 2$ is not a good choice, as is illustrated by the following example.

Example 8. Let $p = 3$, $r = 2$ and $N = 2$. Consider the sequence a_1, a_2 in $\mathbb{Z}_9$ defined by $a_1 = a_2 = 3$. Then a shortest linear recurrence relation is represented by

$$[c(\xi) \quad \omega(\xi)] = [1 - \xi \quad -3\xi].$$

Thus $[c(\sigma) \quad \omega(\sigma)]\,\boldsymbol{b} = 0$ with

$$\boldsymbol{b} = \left(\begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots \right).$$

It can now be shown that there do not exist polynomials $a(\xi)$ and $b(\xi)$ such that

$$\begin{bmatrix} c(\sigma) & \omega(\sigma) \\ a(\sigma) & b(\sigma) \end{bmatrix} \boldsymbol{w} = 0$$

represents $\mathcal{B} = \text{ span } \{\boldsymbol{b}, \sigma\boldsymbol{b}, \sigma^2\boldsymbol{b}\}$. Briefly, the reason for this is that the 1×2-matrix $[1 - \xi \quad -3]$ cannot be extended to a 2×2-polynomial matrix that is unimodular over $\mathbb{Z}_9[\xi]$.

It follows that we need to choose $g > 2$ and this leads us to call $R(\sigma)\boldsymbol{w} = 0$ a *redundant kernel representation* of $\mathcal{B}$. It turns out that $g = 2r$ is a good choice. In the sequel we present an algorithm that constructs a $2r \times 2$ kernel representation $R(\sigma)\boldsymbol{w} = 0$ of $\mathcal{B}$ such that the first row of $R(\xi)$ constitutes a shortest linear recurrence relation. More specifically, the algorithm processes the data iteratively, constructing a $2r \times 2$ polynomial matrix

$$R_k(\xi) = \begin{bmatrix} c_0^{(k)}(\xi) & \omega_0^{(k)}(\xi) \\ \vdots & \vdots \\ c_{r-1}^{(k)}(\xi) & \omega_{r-1}^{(k)}(\xi) \\ \tilde{c}_0^{(k)}(\xi) & \tilde{\omega}_0^{(k)}(\xi) \\ \vdots & \vdots \\ \tilde{c}_{r-1}^{(k)}(\xi) & \tilde{\omega}_{r-1}^{(k)}(\xi) \end{bmatrix}$$

at each step, making sure that for all $k = 1, \dots, N$ and all $j = 0, \dots, r-1$

- $R_k(\sigma)\boldsymbol{b}_k = 0$, where $\boldsymbol{b}_k = \sigma^{N-k}\boldsymbol{b}$
- $\begin{bmatrix} \tilde{c}_j^{(k)}(\sigma) & \tilde{\omega}_j^{(k)}(\sigma) \end{bmatrix} \boldsymbol{b}_{k+1} = (p^j, 0, 0, \cdots)$ for any value of a_{k+1}.
- $L_j^{(k)} + \tilde{L}_{r-j-1}^{(k)} = k + 1$
- the sequences $\{L_j^{(k)}\}_j$ and $\{\tilde{L}_j^{(k)}\}_j$ are non-decreasing,

where $L_0^{(k)}, \dots, L_{r-1}^{(k)}, \tilde{L}_0^{(k)}, \dots, \tilde{L}_{r-1}^{(k)}$ are the row degrees of $R_k(\xi)$.

We next specify the algorithm—note that it processes the numbers $a_1, a_2, \dots, a_N$ iteratively.

Algorithm 1. Initially define

$$R_0(\xi) := \begin{bmatrix} 1 & 0 \\ p & 0 \\ \vdots & \vdots \\ p^{r-1} & 0 \\ 0 & \xi \\ 0 & p\xi \\ \vdots & \vdots \\ 0 & p^{r-1}\xi \end{bmatrix}$$

and $L_0^{(0)} = L_1^{(0)} = \cdots = L_{r-1}^{(0)} = 0$; $\tilde{L}_0^{(0)} = \tilde{L}_1^{(0)} = \cdots = \tilde{L}_{r-1}^{(0)} = 1$.

Proceed iteratively as follows.
Define, after receiving $a_1, a_2, \dots, a_{k+1}$, the error trajectory $\boldsymbol{e}_k$ as

$$R_k(\sigma)\left(\begin{bmatrix} a_{k+1} \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots \right).$$

Now define the vector $\Delta^{(k)}$ of length r by $\Delta^{(k)} = [I_r \quad 0]\,\boldsymbol{e}_k(0)$. For $j = 0, \cdots, r-1$ (using Property 1) write its nonzero components as $\Delta_j^{(k)} = \theta_j^{(k)} p^{u_j^{(k)}}$, where $\theta_j^{(k)}$ is a unit in $\mathcal{R}$ and $u_j^{(k)}$ is an integer with $0 \le u_j^{(k)} \le r-1$. For $j = 0, \cdots, r-1$, if existent, let $n_j^{(k)}$ be the largest integer such that $u_{n_j^{(k)}}^{(k)} = j$.

Now compute $R_{k+1}(\xi)$ as

$$R_{k+1}(\xi) := E_k(\xi)R_k(\xi),$$

where $E_k(\xi)$ is the $2r \times 2r$ polynomial update matrix, that is defined as

$$\begin{bmatrix} I_r & 0 \\ 0 & \xi I_r \end{bmatrix},$$

except for the following entries:

–For $j = 0, \cdots, r-1$, if $\Delta_j^{(k)} \neq 0$ then define the $(j+1, r+u_j^{(k)}+1)$-entry as $-\theta_j^{(k)}$ and update its row degree as $L_j^{(k+1)} = \max\{L_j^{(k)}, \tilde{L}_{u_j^{(k)}}^{(k)}\}$; otherwise update the row degree as $L_j^{(k+1)} = L_j^{(k)}$.

–For $j = 0, \cdots, r-1$, whenever $n_j^{(k)}$ is defined and $L^{(k)}_{n_j^{(k)}} < \tilde{L}_j^{(k)}$, define the $(r+j+1, n_j^{(k)}+1)$-entry as $\xi/\theta^{(k)}_{n_j^{(k)}}$ and the $(r+j+1, r+j+1)$-entry as zero; update the row degree as $\tilde{L}_j^{(k+1)} = L^{(k)}_{n_j^{(k)}} + 1$, otherwise update the row degree as $\tilde{L}_j^{(k+1)} = \tilde{L}_j^{(k)} + 1$.

Example 9. Operating Algorithm 1 on the sequence $a_1, a_2, a_3, a_4, a_5 = 6, 3, 1, 5, 6$ in $\mathbb{Z}_9$ (i.e. data as in (Reeds and Sloane, 1985)) we obtain

$$R_5(\xi) = \begin{bmatrix} 1+4\xi+7\xi^2+\xi^3 & -6\xi-\xi^3 \\ 3+3\xi^2+5\xi^3 & -3\xi^3 \\ 3\xi+\xi^3 & 0 \\ 3\xi^3 & 0 \end{bmatrix}.$$

Theorem 10. Let the above algorithm operate on the finite sequence $a_1, \ldots, a_N$ in $\mathcal{R}$; define $R(\xi)$ as the $2r \times 2$ polynomial matrix $R_N(\xi)$ that is finally produced by the algorithm. Then for $j = 1, \ldots, r-1$, the $(j+1)$-th row of $R(\xi)$ constitutes an annihilator $[c_j(\xi) \quad \omega_j(\xi)]$ for $a_1, \ldots, a_N$ with $c_j(0) = p^j$, that has minimal length among all such annihilators. In particular, the first row of $R(\xi)$ constitutes a shortest linear recurrence relation for $a_1, \ldots, a_N$.

To prove the above theorem we show that the matrices specified in the algorithm satisfy the four requirements mentioned before Algorithm 1. Minimality then follows from Lemma 2 of (Reeds and Sloane, 1985). For reasons of space limitations the full proof is here omitted. Note that for $r = 1$, i.e. the field case, the above algorithm coincides with the Berlekamp-Massey algorithm, producing a 2×2 polynomial matrix, as in (Kuijper and Willems, 1997).

4. PARAMETRIZATION

In the previous section we showed that $\boldsymbol{b}$ is included in the behavior defined by $R(\sigma)\boldsymbol{w} = 0$ with $R(\xi)$ the final output of Algorithm 1. Note however that, unlike the field case, the update representation $E_k(\sigma)\boldsymbol{w} = 0$ does not necessarily represent the MPUM of the error trajectory $\boldsymbol{e}_k$. Nevertheless, in this section we show that $R_k(\sigma)\boldsymbol{w} = 0$ does represent the MPUM of $\sigma^{N-k}\boldsymbol{b}$. This is of importance for the parametrization of Theorem 12 below. Thus, in this section we step beyond the results of (Reeds and Sloane, 1985).

Theorem 11. For $k = 1, \ldots, N$ let $\mathcal{B}_k$ be defined as $\mathcal{B}_k = \text{ span } \{\sigma^{N-k}\boldsymbol{b}, \sigma^{N-k+1}\boldsymbol{b}, \cdots, \sigma^N\boldsymbol{b}\}$ and let $R_k(\xi)$ be as in Algorithm 1. Then $R_k(\sigma)\boldsymbol{w} = 0$ represents $\mathcal{B}_k$.

The proof is by induction and here omitted. The next theorem follows immediately from Theorem 11 and Lemma 5.

Theorem 12. Let $R(\xi)$ be the final output of Algorithm 1. Denote the row degrees of $R(\xi)$ by $L_0, \ldots, L_{r-1}, \tilde{L}_0, \ldots, \tilde{L}_{r-1}$. A parametrization of all shortest linear recurrence relations is given by

$$[c(\xi) \quad \omega(\xi)] = \begin{bmatrix} Q(\xi) & \tilde{Q}(\xi) \end{bmatrix} R(\xi), \qquad (3)$$

where the $1 \times r$ polynomial matrices

$$Q(\xi) = [1 \quad \xi q_1(\xi) \quad \cdots \quad \xi q_{r-1}(\xi)]$$

and

$$\tilde{Q}(\xi) = [\tilde{q}_0(\xi) \quad \cdots \quad \tilde{q}_{r-1}(\xi)]$$

are such that deg $[c(\xi) \quad \omega(\xi)] = L_0$.

Example 13. The sequence of Example 9 has complexity 3. By inspecting the rows of the matrix $R_5(\xi)$ carefully we conclude from the above theorem that a parametrization of all shortest linear recurrence relations is given by $1+4\xi+7\xi^2+\xi^3+a(3\xi+\xi^3)+3b\xi^3$ where $a, b \in \mathbb{Z}_9$.

Extending the sequence with the additional data point $a_6 = 6$, Algorithm 1 yields

$$R_6(\xi) = \begin{bmatrix} 1+4\xi+7\xi^2-2\xi^3 & -6\xi-\xi^3 \\ 3+3\xi+3\xi^2+3\xi^3 & -3\xi^3 \\ 3\xi^2+\xi^4 & 0 \\ 3\xi^4 & 0 \end{bmatrix}.$$

Again inspecting the rows of the matrix $R_5(\xi)$ carefully, we conclude from Theorem 12 that the shortest linear recurrence relation $1+4\xi+7\xi^2-2\xi^3$ is unique.

In the above example we had to inspect the rows carefully in order to derive a practical formula that captures all shortest linear recurrence relations. Our conjecture is that a stronger variation of Theorem 12 holds where the matrices $Q(\xi)$ and $\tilde{Q}(\xi)$ have restricted degree as follows:

- deg $q_j(\xi) = L_0 - L_j - 1$
- deg $\tilde{q}_j(\xi) = L_0 - \tilde{L}_j$.

Such a result would immediately give a practical formula that captures all shortest linear recurrence relations and would give rise to elegant uniqueness conditions. In the field case the so-called "predictable degree property"(see (Forney, Jr., 1975) and also (Kailath, 1980, Thm 6.3-13)) for row reduced square polynomial matrices is instrumental in deriving such a practical formula (see (Kuijper and Willems, 1997)). In our ring case the predictable degree property does not hold

as nontrivial linear combinations of rows of the rectangular matrix $R(\xi)$ can even become zero, so that a different proof technique is needed. This is a topic of further research.

5. CONCLUSIONS

In this paper we addressed the issue of minimality for kernel representations of behaviors over the ring $\mathcal{R} = \mathbb{Z}_{p^r}$. We found that in order to construct a kernel representation of minimal row degree we needed to work with redundant kernel representations. These use more rows than strictly needed to represent the behavior. This is a somewhat surprising result that certainly sets the ring case apart from the field case.

In the paper we perform behavioral modeling for a specific time trajectory, namely an inverted truncated impulse response that is defined from a finite sequence of numbers in $\mathcal{R}$. In this context the quest for a kernel representation of minimal row degree is equivalent to the construction of a minimal partial realization for the truncated impulse response, i.e. a shortest linear recurrence relation for the finite sequence. In the paper we recast the algorithm of (Reeds and Sloane, 1985) in a behavioral framework. In (Reeds and Sloane, 1985) certain polynomials play an implicit and supportive role. In this paper we make these polynomials explicit so that they become active players in the behavioral model. In this way we are able to construct an explicit minimal behavioral model for the data that allows for a parametrization of all shortest linear recurrence relations for the data. It is a topic of future research to strengthen this result to a parametrization formula in which the coefficient polynomials have restricted degrees. Such a result would give a more practical parametrization formula and also give rise to a characterization of uniqueness of a shortest linear recurrence relation.

We consider the ideas in this paper as inputs to more general investigations on linear systems over finite rings.

REFERENCES

Antoulas, A.C. (1994). Recursive modeling of discrete-time time series. In: *Linear Algebra for Control Theory* (P. Van Dooren and B. Wyman, Eds.). Vol. 62 of *IMA Volumes*. Springer-Verlag. pp. 1–20.

Berlekamp, E.R. (1968). *Algebraic Coding Theory*. McGraw-Hill. New York.

Fagnani, F. and S. Zampieri (1996). Dynamical systems and convolutional codes over finite abelian groups. *IEEE Trans. Inf. Th* **42**, 1892–1912.

Fagnani, F. and S. Zampieri (1997). Canonical kernel representations for behaviors over finite abelian groups. *Systems & Control Letters* **32**, 271–282.

Fagnani, F. and S. Zampieri (2001). Convolutional codes over finite abelian groups: some basic results. In: *Codes, Systems, and Graphical Models* (Brian Marcus and Joachim Rosenthal, Eds.). Vol. 123 of *The IMA Volumes in Mathematics and its Applications*. Springer-Verlag. pp. 327–346.

Forney, Jr., G.D. (1975). Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control* **13**, 493–520.

Kailath, T. (1980). *Linear Systems*. Prentice Hall. Englewood Cliffs, N.J.

Kuijper, M. (1994). *First-Order Representations of Linear Systems*. Systems and Control: Foundations and Applications. Birkhäuser. Boston, USA.

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

Kuijper, M. (2001). Algorithms for decoding and interpolation. In: *Codes, Systems, and Graphical Models* (Brian Marcus and Joachim Rosenthal, Eds.). Vol. 123 of *The IMA Volumes in Mathematics and its Applications*. Springer-Verlag. pp. 265–282.

Kuijper, M. and J.C. Willems (1997). On constructing a shortest linear recurrence relation. *IEEE Trans. Aut. Control* **42**, 1554–1558.

Kuijper, M. and J.W. Polderman (2004). Reed-Solomon list decoding from a system theoretic perspective. *IEEE Trans. Inf. Th.* **IT-50**, 259–271.

Massey, J.L. (1969). Shift-register synthesis and BCH decoding. *IEEE Trans. Info. Theory* **IT-15**, 122–127.

Norton, G. (1999). On minimal realization over a finite chain ring. *Designs, Codes and Cryptography* **16**, 161–178.

Reeds, J.A. and N.J.A. Sloane (1985). Shift-register synthesis (modulo m). *SIAM J. Computing* **14**, 505–513.

Schumacher, J.M. (1988). Transformations of linear systems under external equivalence. *Linear Algebra and its Applications* **102**, 1–33.

Willems, J.C. (1986). From time series to linear system. part ii: Exact modelling. *Automatica* **22**, 675–694.

Willems, J.C. (1991). Paradigms and puzzles in the theory of dynamical systems. *IEEE Trans. Aut. Control* **36**, 259–294.