Kernel representations for behaviors over finite rings

Margreta Kuijper[1]
Department of Electrical and Electronic Engineering
The University of Melbourne, VIC 3052 Australia
E-mail: m.kuijper@ee.unimelb.edu.au

Raquel Pinto
Department of Mathematics
University of Aveiro
Campus Universitario de Santiago, 3810-193, Aveiro, Portugal
E-mail: raquel@mat.ua.pt

Jan Willem Polderman
Faculty of Mathematical Sciences
University of Twente
P.O.Box 217, 7500 AE Enschede, The Netherlands
E-mail: J.W.Polderman@math.utwente.nl

1 Introduction and motivation

In behavioral theory, a central role is played by the set $\mathcal{B}$ of trajectories that belong to a dynamical system Σ, see the textbook [11]. 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 where $\mathcal{B}$, 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 $\mathbb{Z}_{p^r}$. Here p is a prime number and r is a positive integer. We study the theory of representations for such systems, in particular kernel representations (defined below).

For $r \geq 2$ the ring $\mathbb{Z}_{p^r}$ is not a field. In this paper we see that several fundamental issues that are clearcut in the field case are unsolved in the ring case.

Our motivation for considering systems over $\mathbb{Z}_{p^r}$ stems entirely from applications in the communications area. The communications literature has dedicated considerable attention to error-correcting codes and sequences over $\mathbb{Z}_{p^r}$. Firstly, error-correcting codes over $\mathbb{Z}_{p^r}$ have been found useful for socalled "coded modulation" schemes. These consist of block codes where the resulting codewords from $\mathbb{Z}_{p^r}^n$ are mapped onto phase-shift-keying (PSK) modulation signal sets. The mapping is such that distances between modulation points are preserved under additive operations in $\mathbb{Z}_{p^r}$. The latter property defines the modulation code to be "geometrically uniform", see [12]. Secondly, the 1994 breakthrough paper [6] puts codes over the ring $\mathbb{Z}_4$ on the stage after showing that several efficient nonlinear binary codes are images of linear $\mathbb{Z}_4$ codes under a Gray map. A final motivation stems from sequence theory. It was found in [2] and [13] that certain families of sequences over $\mathbb{Z}_4$ outperform field sequences in their correlation properties.

An outline of the paper is as follows. In the next section we present some preliminary results from the algebraic theory of $\mathbb{Z}_{p^r}$. In section 3 we present the problem statements and main results. Section 4 follows with conclusions.

[1]This work was carried out during a 6 month stay at The University of Twente that was supported by the Dutch Organization for Scientific Research (NWO). The first author is also supported in part by the Australian Research Council.

2 Preliminary results on the finite ring $\mathbb{Z}_{p^r}$

In this section we outline some general results from algebraic theory of $\mathbb{Z}_{p^r}$. We use these results later on. We start off with some results on the ring $\mathbb{Z}_{p^r}$ itself. In the sequel $[A]_p$ denotes A modulo p, where A is a polynomial matrix.

Property 2.1 *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 a unique integer with $0 \leq u \leq r-1$.*

Property 2.2 *Any nonzero $a \in \mathbb{Z}_{p^r}$ can be written uniquely as $a = \theta_0 + \theta_1 p + \cdots + \theta^{r-1} p^{r-1}$, where θ_i is a unit in $\mathbb{Z}_{p^r}$ for $i = 0, \ldots, r-1$.*

Property 2.3 *A number $a \in \mathbb{Z}_{p^r}$ is a unit iff $[a]_p \neq 0$.*

Next we continue with some general results from [1] on constant matrices over $\mathbb{Z}_{p^r}$. The next lemma generalizes Property 2.3 to the matrix case.

Lemma 2.1 *Let A be a matrix in ${\mathbb{Z}_{p^r}}^{n\times n}$. The following statements are equivalent:*

- *A is invertible*
- *$\det A$ is a unit*
- *$[A]_p$ is invertible as a matrix in ${\mathbb{Z}_p}^{n\times n}$.*

In fact, the inverse U of $[A]_p$ in ${\mathbb{Z}_p}^{n\times n}$ can be "lifted" to an inverse V of A in ${\mathbb{Z}_{p^r}}^{n\times n}$ as follows. Let B in $\mathbb{Z}_{p^r}^{n\times n}$ be such that $UA = I - pB$. Then the inverse of A in $\mathbb{Z}_{p^r}^{n\times n}$ is given by $V = (I + pB + p^2B^2 + \cdots + p^{r-1}B^{r-1})U$. Note that $[V]_p = U$.

We continue with some general results from [9] on polynomials in $\mathbb{Z}_{p^r}[\xi]$.

Definition 2.1 *A polynomial is called* **regular** *if it is not a zero divisor in $\mathbb{Z}_{p^r}[\xi]$.*

Lemma 2.2 *([9, Thm XIII 2c]) A polynomial $f \in \mathbb{Z}_{p^r}[\xi]$, written as $f(\xi) = f_0 + f_1\xi + \ldots + f_n\xi^n$, is regular iff there exists $i \in \{0, 1, \ldots, n\}$ such that f_i is a unit in $\mathbb{Z}_{p^r}$.*

Definition 2.2 *The* **order** *of a regular polynomial $f \in \mathbb{Z}_{p^r}[\xi]$ is defined as*

$$\text{ord}\,(f) = \max\{i \mid f_i \text{ is a unit in } \mathbb{Z}_{p^r}\}.$$

Definition 2.3 *A polynomial $g \in \mathbb{Z}_{p^r}[\xi]$, written as $g(\xi) = g_0 + g_1\xi + \ldots + g_n\xi^n$, is called* **monic** *if its leading coefficient $g_n = 1$.*

Definition 2.4 *A polynomial $u \in \mathbb{Z}_{p^r}[\xi]$ is called a unit polynomial if there exists a polynomial $v \in \mathbb{Z}_{p^r}[\xi]$ such that $uv \equiv 1$.*

Lemma 2.3 *A polynomial $u \in \mathbb{Z}_{p^r}[\xi]$ is a unit polynomial iff* $\text{ord}\,(u) = 0$.

The following theorem shows how the higher order powers with zero divisor coefficients of a regular polynomial can be eliminated through multiplication by a unit polynomial. The theorem is a special instance of a powerful result in number theory, namely Hensel's Lemma. For completeness we also provide a proof.

Theorem 2.1 *([9, Thm XIII.6]) Let $f \in \mathbb{Z}_{p^r}[\xi]$ be a regular polynomial of order m. Let us assume, without restrictions, that $[f]_p$ is monic. Then there exists a unit polynomial u and a monic polynomial g such that*

$$f = ug.$$

Proof We prove by induction that, for $k = 1, \ldots, r$ there exist polynomials u_k and g_k in $\mathbb{Z}_{p^k}[\xi]$ such that

(i) $[f]_{p^k} = [u_k g_k]_{p^k}$

(ii) u_k is a unit polynomial with $[u_k]_p \equiv 1$

(iii) g_k is a monic polynomial of degree m with $[g_k]_p = [f]_p$.

Firstly, the above statement is trivially satisfied for $k = 1$: simply take $u_1 \equiv 1$ and $g_1 = [f]_p$. Next, assume that the statement holds for k. We now prove that it then also holds for $k + 1$. By the induction hypothesis (i) there exists $q_k \in \mathbb{Z}_p[\xi]$ such that

$$[f - u_k g_k]_{p^{k+1}} = p^k q_k.$$

By division in $\mathbb{Z}_p[\xi]$ polynomials ℓ_k and r_k in $\mathbb{Z}_p[\xi]$ can be determined such that

$$q_k = \ell_k g_1 + r_k \quad \text{where } \deg r_k < \deg g_1 = m.$$

Now define

$$\begin{aligned} u_{k+1} &= u_k + p^k \ell_k \\ g_{k+1} &= g_k + p^k r_k. \end{aligned}$$

Then clearly (using the induction hypotheses (ii) and (iii)) $[u_{k+1}]_p = [u_k]_p \equiv 1$, $[g_{k+1}]_p = [g_k]_p = g_1$ and $\deg g_{k+1} = \deg g_k = m$. Further,

$$\begin{aligned} [u_{k+1} g_{k+1}]_{p^{k+1}} &= [u_k g_k + p^k (u_k r_k + g_k \ell_k)]_{p^{k+1}} \\ &= [f - p^k q_k + p^k (u_1 r_k + g_1 \ell_k)]_{p^{k+1}} \\ &= [f - p^k q_k + p^k q_k]_{p^{k+1}} \\ &= [f]_{p^{k+1}}. \end{aligned}$$

The theorem is now proven by taking $u = u_r$ and $g = g_r$. □

We conclude this section with some results on polynomial matrices over $\mathbb{Z}_{p^r}$. The next lemma generalizes Lemma 2.3 to the matrix case.

Lemma 2.4 *Let U be a matrix in ${\mathbb{Z}_{p^r}}^{n \times n}[\xi]$. The following statements are equivalent:*

- *U is unimodular*
- *$\det U$ is a unit*
- *$[U]_p$ is a unimodular matrix in ${\mathbb{Z}_p}^{n \times n}[\xi]$.*

3 Fundamental results on kernel representations

For behavioral systems over fields there exists a well-developed theory of representations, see e.g. [11, 15, 16, 17]. 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 (i.e., closed in the topology of pointwise convergence) 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 was shown in [3] that the above result is also true in our ring case, i.e., any linear, shift-invariant and complete behavior over the ring $\mathcal{R} = \mathbb{Z}_{p^r}$ admits a kernel representation. However, there are some important differences. For example, unlike the field case, for $q = 1$ there does not necessarily exist a 1×1 kernel representation, as illustrated by the following example.

Example 3.1 *Consider* $\Sigma = (\mathbb{Z}_+, \mathbb{Z}_9, \mathcal{B})$ *(i.e.* $p = 3; r = 2$*) with* $\mathcal{B} = \text{span}\{(3, 3, 3, \cdots)\}$. *Then a kernel representation is given by*

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

There does not exist a single polynomial $r \in \mathcal{R}[\xi]$ *such that* $\mathcal{B}$ *is given by* $r(\sigma)\boldsymbol{w} = 0$. *The reason for this is that the Bezout identity does not hold in the polynomial ring* $\mathcal{R}[\xi]$.

The above example also illustrates that in the ring case we cannot restrict ourselves to behaviors that are represented by a kernel representation of full row rank. In this paper we shall see that this simple fact has major implications for the fundamental theory of representations.

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:

Question 1) Given two behaviors $\mathcal{B}$ and $\tilde{\mathcal{B}}$ with kernel representations $R(\sigma)\boldsymbol{w} = 0$ and $\tilde{R}(\sigma)\boldsymbol{w} = 0$ respectively and $\mathcal{B} \subseteq \tilde{\mathcal{B}}$, how are the polynomial matrices R and $\tilde{R}$ related?

Question 2) Given a behavior $\mathcal{B}$ represented by $R(\sigma)\boldsymbol{w} = 0$ as well as $\tilde{R}(\sigma)\boldsymbol{w} = 0$, how are the polynomial matrices R and $\tilde{R}$ related?

Question 3) ("minimal equations"-problem) Among all kernel representations of a behavior $\mathcal{B}$, can we characterize a kernel representation $R(\sigma)\boldsymbol{w} = 0$ with a minimal number of rows?

Question 4) ("minimal lag"-problem) Among all kernel representations of a behavior $\mathcal{B}$, 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 [3], namely to derive a theory of row reduced kernel representations for systems over the ring $\mathcal{R}$.

Several results from the field case directly carry over to the ring case. One of these is the next theorem which gives the answer to **Question 1)** above. This theorem is implicitly underlying many of the results in [3], where it is connected with Pontryagin duality theory.

Theorem 3.1 *Let a behavior* $\mathcal{B}$ *be given by* $R(\sigma)\boldsymbol{w} = 0$ *and let* $\tilde{\mathcal{B}}$ *be given by* $\tilde{R}(\sigma)\boldsymbol{w} = 0$. *Suppose that* $\mathcal{B} \subset \tilde{\mathcal{B}}$. *Then there exists a polynomial matrix* F *such that* $\tilde{R} = FR$.

Proof This is due to $\mathbb{Z}_{p^r}$ being a finite Quasi-Frobenius ring, see [8, Theorem 2.8]. Recall that a Quasi-Frobenius ring is a ring in which for each ideal I we have $\text{ann}(\text{ann}(I)) = I$, where $\text{ann}(I)$ denotes the ideal of annihilators of I.

Another result that directly carries over from the field case is the following (thus partly answering **Question 2)** above). Recall that $[R]_p$ denotes R mod p.

Theorem 3.2 *Denote the number of rows of R and $\tilde{R}$ by g and $\tilde{g}$, respectively. Assume that $[R]_p$ has full row rank as a polynomial matrix with coefficients in $\mathbb{Z}_p$. Then $\mathcal{B} = \tilde{\mathcal{B}}$ iff $g \leq \tilde{g}$ and there exists a unimodular polynomial matrix U such that*

$$\tilde{R} = U \begin{bmatrix} R \\ 0 \end{bmatrix},$$

where there are $\tilde{g} - g$ zero rows at the right hand side.
Further, if both $[R]_p$ and $[\tilde{R}]_p$ have full row rank then $g = \tilde{g}$ and $\tilde{R} = UR$.

Proof The "if" part is trivial. In order to prove the "only if" part we first note that it follows from Theorem 3.1 that there exist polynomial matrices F and $\tilde{F}$ such that $\tilde{R} = FR$ and $R = \tilde{F}\tilde{R}$. From this it follows that

$$\left(I_g - \tilde{F}F\right) R = 0,$$

where I_g denotes the $g \times g$ identity matrix. From the assumption that $[R]_p$ has full row rank it now follows that $[\tilde{F}F]_p = I_g$. As a result (using Lemma 2.1) F is left polynomially invertible so can be extended to a unimodular matrix $U = [F \quad V]$. Now $\tilde{R} = U \begin{bmatrix} R \\ 0 \end{bmatrix}$. This proves the first statement of the theorem. In the case that both $[R]_p$ and $[\tilde{R}]_p$ have full row rank it follows by the same reasoning that not only $[\tilde{F}F]_p = I_g$ but also $[F\tilde{F}]_p = I_{\tilde{g}}$. This implies that $g = \tilde{g}$ and that F is unimodular, which proves the second statement of the theorem.

Corollary 3.1 *Consider a behavior $\mathcal{B}$ given by $f(\sigma)\boldsymbol{w} = 0$ where f is a regular polynomial of order m. Then there exists a monic polynomial g of degree m such that $\mathcal{B}$ is given by $g(\sigma)\boldsymbol{w} = 0$.*

Proof According to Theorem 2.1 there exists a unit polynomial v such that $vf = g$ for some monic polynomial g of degree m. The result is now an immediate consequence of Theorem 3.2.

The above corollary is a first step towards defining a notion of "dimension" for behaviors over $\mathbb{Z}_{p^r}$. This topic needs further investigation and an extension to the multivariable case.

In our ring case the situation with respect to input/output structure and causality of behaviors is quite different from the field case. For example, over $\mathbb{Z}_9$, the behavior defined by

$$[3\sigma \quad 1] \begin{bmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \end{bmatrix} = 0$$

has no causal input/output structure, no matter whether we take $\boldsymbol{w}_1$ or $\boldsymbol{w}_2$ as the input. Indeed, because of the presence of zero divisors $\boldsymbol{w}_2$ cannot be taken as a genuine input as it is not free. On the other hand, the system is not causal if $\boldsymbol{w}_1$ is taken as the input. The next theorem gives a sufficient condition for causality of a single-input-single-output system, represented by a 1×2 kernel representation.

Theorem 3.3 *Consider a behavior $\mathcal{B}$ given by $f(\sigma)\boldsymbol{y} = h(\sigma)\boldsymbol{u}$ where f is a regular polynomial of degree n and of order m. Then the system is causal if deg $h + (r-1)(n-m) \leq m$.*

Proof Let us assume, without restrictions, that $[f]_p$ is monic. According to Theorem 2.1 there exists a unit polynomial v such that vf is monic and of degree m. This implies that deg $v^{-1} = n - m$. Writing $v^{-1}(\xi) = 1 - pw(\xi)$ for some polynomial w with deg $w = n - m$, we have $v =$

$1 + pw(\xi) + p^2w^2(\xi) + \cdots + p^{r-1}w^{r-1}(\xi)$. As a result, deg $v \leq (r-1)(n-m)$. Next, we observe that the representation $v(\sigma)f(\sigma)\boldsymbol{y} = v(\sigma)h(\sigma)\boldsymbol{u}$ represents the same behavior, since v is a unit polynomial. Clearly causality holds if deg $vh \leq$ deg $vf = m$. The theorem now follows from deg $vh \leq (r-1)(n-m) + \deg h$. □

As demonstrated by Example 3.1, the assumption that $[R]_p$ has full row rank is restrictive in the ring case, i.e., not every behavior admits a representation of full row rank. In order to provide a complete answer to **Question 2)** we should therefore investigate the general case where neither $[R]_p$ nor $[\tilde{R}]_p$ has full row rank. If $R(\sigma)\boldsymbol{w} = 0$ and $\tilde{R}(\sigma)\boldsymbol{w} = 0$ represent the same behavior one might conjecture that necessarily $\tilde{R} = UR$ with U a unimodular matrix (assuming $g = \tilde{g}$ for the sake of simplicity). However, this is not true, as demonstrated by the next counterexample.

Example 3.2 *Consider $\Sigma = (\mathbb{Z}_+, \mathbb{Z}_9, \mathcal{B})$ (i.e. $p = 3; r = 2$). Let $\mathcal{B}$ be represented by $R(\sigma)\boldsymbol{w} = 0$, where*

$$R(\xi) = \begin{bmatrix} \xi^2 + \xi \\ 3 \end{bmatrix}.$$

Let $\tilde{\mathcal{B}}$ be represented by $\tilde{R}(\sigma)\boldsymbol{w} = 0$, where

$$\tilde{R}(\xi) = \begin{bmatrix} \xi^2 + \xi \\ 3(\xi - 1) \end{bmatrix}.$$

Then it is easily verified that $\mathcal{B} = \tilde{\mathcal{B}}$. Indeed, $\mathcal{B} \subset \tilde{\mathcal{B}}$ is trivial whereas $\tilde{\mathcal{B}} \subset \mathcal{B}$ follows from the fact that $\ker(\sigma - 1) \cap \ker(\sigma^2 + \sigma) = \{0\}$. *We will now show that there does not exist a unimodular polynomial matrix U such that $\tilde{R} = UR$. For any matrix $U(\xi) = \begin{bmatrix} u_{11}(\xi) & u_{12}(\xi) \\ u_{21}(\xi) & u_{22}(\xi) \end{bmatrix}$ such that*

$$\begin{bmatrix} u_{11}(\xi) & u_{12}(\xi) \\ u_{21}(\xi) & u_{22}(\xi) \end{bmatrix} \begin{bmatrix} \xi^2 + \xi \\ 3 \end{bmatrix} = \begin{bmatrix} \xi^2 + \xi \\ 3(\xi - 1) \end{bmatrix}$$

it follows that

$$\begin{bmatrix} [u_{11}(\xi)]_p \\ [u_{21}(\xi)]_p \end{bmatrix} (\xi^2 + \xi) = \begin{bmatrix} \xi^2 + \xi \\ 0 \end{bmatrix}.$$

This implies that $[u_{11}]_p \equiv 1$ and $[u_{21}]_p \equiv 0$. From this it follows that U is unimodular iff u_{22} is a unit polynomial. Further, writing $u_{21}(\xi) = 3q(\xi)$ it follows that $3((\xi^2+\xi)q(\xi) + u_{22}(\xi) - (\xi - 1)) \equiv 0$. Therefore there exists a polynomial $m(\xi)$ such that $(\xi^2+\xi)q(\xi)+u_{22}(\xi)-(\xi-1) = 3m(\xi)$. Substituting $\xi = 0$ we obtain

$$u_{22}(0) = -1 + 3m(0). \tag{1}$$

Substituting $\xi = -1$ we obtain

$$u_{22}(-1) = -2 + 3m(-1). \tag{2}$$

From (1)–(2) it follows that u_{22} is not a unit polynomial and this again implies that U is not unimodular.

Note that adding an extra zero row alters the situation: there exists a 3×3 unimodular matrix U such that

$$U \begin{bmatrix} R \\ 0 \end{bmatrix} = \begin{bmatrix} \tilde{R} \\ 0 \end{bmatrix},$$

namely

$$U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \xi - 1 & 5 \\ 6 & \xi^2 + \xi & 1 - 4\xi \end{bmatrix}.$$

The above example shows that the theory of kernel representations in the ring case is much less straightforward than in the field case. Let us now concentrate on kernel representations of a specific form, namely the "adapted form", as introduced in [3].

A kernel representation $R(\sigma)\boldsymbol{w} = 0$ is called an *adapted representation* if the polynomial matrix R can be written as

$$R = \begin{bmatrix} N_0 \\ pN_1 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix},$$

where

1) $[N_i]_p$ has full row rank as a matrix over $\mathbb{Z}_p[\xi]$ for $i = 0, \ldots, r-1$ and

2) there exists a block upper triangular polynomial matrix H such that

$$\begin{bmatrix} pN_0 \\ p^2N_1 \\ \vdots \\ p^{r-1}N_{r-2} \end{bmatrix} = H \begin{bmatrix} pN_1 \\ p^2N_2 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix}. \tag{3}$$

It has been shown in [3] that any linear σ-invariant complete behavior over the ring $\mathbb{Z}_{p^r}$ admits an adapted kernel representation. The next theorem is another step towards answering **Question 2)**.

Theorem 3.4 *([3, Prop. 5]) Let $R(\sigma)\boldsymbol{w} = 0$ and $\tilde{R}(\sigma)\boldsymbol{w} = 0$ be two adapted kernel representations, written as*

$$R = \begin{bmatrix} N_0 \\ pN_1 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix},$$

and

$$\tilde{R} = \begin{bmatrix} \tilde{N}_0 \\ p\tilde{N}_1 \\ \vdots \\ p^{r-1}\tilde{N}_{r-1} \end{bmatrix}.$$

Then they represent the same behaviour if and only if $\tilde{g}_i = g_i$ $(i = 0, \ldots, r-1)$ and there exists a unimodular polynomial matrix U such that

$$\begin{bmatrix} \tilde{N}_0 \\ p\tilde{N}_1 \\ \vdots \\ p^{r-1}\tilde{N}_{r-1} \end{bmatrix} = U \begin{bmatrix} N_0 \\ pN_1 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix}.$$

Furthermore, the matrix U can be chosen block upper triangular.

Proof The "if" part is trivial. In order to prove the "only if" part we first note that it follows from Theorem 3.1 that there exist polynomial matrices F and $\tilde{F}$ such that

$$\begin{bmatrix} \tilde{N}_0 \\ p\tilde{N}_1 \\ \vdots \\ p^{r-1}\tilde{N}_{r-1} \end{bmatrix} = F \begin{bmatrix} N_0 \\ pN_1 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} N_0 \\ pN_1 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix} = \tilde{F} \begin{bmatrix} \tilde{N}_0 \\ p\tilde{N}_1 \\ \vdots \\ p^{r-1}\tilde{N}_{r-1} \end{bmatrix}.$$

Because of the second property (3) of the adapted form it is easily seen that here both F and $\tilde{F}$ can be chosen to be block upper triangular, with diagonal blocks F_i and $\tilde{F}_i$, respectively ($i = 0, \ldots, r-1$). As a result

$$\left(I_g - \tilde{F}F\right) \begin{bmatrix} N_0 \\ pN_1 \\ \vdots \\ p^{r-1}N_{r-1} \end{bmatrix} = 0,$$

where $I_g - \tilde{F}F$ is a block upper triangular polynomial matrix with diagonal blocks $I_{g_i} - \tilde{F}_i F_i$. For $i = 0, \ldots, r-1$ this implies that

$$p^{r-i-1}\left(I_{g_i} - \tilde{F}_i F_i\right) p^i N_i = 0.$$

Then necessarily

$$[\left(I_{g_i} - \tilde{F}_i F_i\right) N_i]_p = 0$$

for $i = 0, \ldots, r-1$. From the first property of the adapted form, i.e. the property that $[N_i]_p$ has full row rank, it now follows that $[\tilde{F}_i F_i]_p = I_{g_i}$. Analogously we can prove that $[F_i \tilde{F}_i]_p = I_{\tilde{g}_i}$. It now follows that $g_i = \tilde{g}_i$ and that F_i is unimodular for $i = 0, \ldots, r-1$. As a result F is unimodular which proves the theorem.

In a way the rows of an adapted representation behave as the polynomial equivalent of a "p-generator sequence", as defined for constant vectors over $\mathbb{Z}_{p^r}$ in [14].

The question now arises whether there exists an algebraic operation that brings any polynomial matrix R into adapted form, while leaving the corresponding behavior intact. First note that it is easy to achieve a representation that satifies only the first condition of the adapted representation. Indeed, this can be achieved by repeated premultiplication by unimodular $\mathbb{Z}_p$-matrices. Similarly we can easily achieve a representation that satifies only the second condition as follows:

$$U \begin{bmatrix} R \\ 0 \end{bmatrix} = \begin{bmatrix} R \\ pR \\ \vdots \\ p^{r-1}R \end{bmatrix} \quad \text{where } U = \begin{bmatrix} I & & & \\ pI & I & & \\ \vdots & & \ddots & \\ p^{r-1}I & & & I \end{bmatrix}.$$

However, it is far from trivial to achieve a representation that satisfies both condition 1) and condition 2) of the adapted form. It turns out that in general this may not be achievable by premultiplication by a unimodular matrix. In the following procedure from [4, Appendix] a polynomial matrix F_1 is constructed such that $F_1 R$ is in adapted form, say N. The construction is such that there also exists a polynomial matrix F_2 such that $R = F_2 N$. By Theorem 3.1 it then follows that $N(\sigma)\boldsymbol{w} = 0$ represents the same behavior as $R(\sigma)\boldsymbol{w} = 0$. The procedure consists of repeated " full row rank operations" over the underlying field and is fairly easy to carry out.

4 Conclusions

In this paper we adopted a systematic approach to develop a fundamental theory for kernel representations of linear discrete-time behaviors over the ring $\mathbb{Z}_{p^r}$. We presented answers to some of the most fundamental questions incorporating results that were already available in the literature, notably in the work of Fagnani and Zampieri [3, 4].

Our work is meant as a first step towards further development of this theory. In particular Corollary 3.1 is a first step towards defining a notion of "dimension" for behaviors over $\mathbb{Z}_{p^r}$ i.e., a characterization of the minimal number of trajectories that generate a behavior. This needs further investigation and an extension to the multivariable case.

Further, it is clear from Example 3.1 that, compared to the field case, the characterization of a "minimal" number of equations (**Question 3**) no longer depends only on the row rank of a kernel representation, as in the field case. Its exact characterization in the ring case is still an open problem.

A further topic of research is to determine a minimal lag representation (**Question 4**). Results from the recent paper [7] suggest that the adapted form introduced in [3, 4] is not suitable in this context.

Other outstanding issues include the characterization of input/output structure and of causality. For this, Theorem 3.3 provides a first step in giving a sufficient condition for causality of a single-input-single-output system.

Finally, it should be noted that the results of this paper hold more generally for any finite chain ring i.e., a ring in which all ideals are ordered by inclusion [5, 10]. Generalizations to finite commutative rings (see [9]) and finite abelian groups (as in [14, Sect. IX-C] and [3]) are then also possible.

5 Acknowledgement

The first author would like to thank Serdar Boztaş for providing a reference for Theorem 2.1.

References

[1] M. Artin. *Algebra*. Prentice Hall, 1991.

[2] S. Boztaş, R. Hammons, and P.V. Kumar. 4-Phase sequences with near-opimum correlation properties. *IEEE Trans. Inf. Th.*, 38:1101–1113, 1992.

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

[4] F. Fagnani and S. Zampieri. System-theoretic properties of convolutional codes over rings. *IEEE Trans. Inf. Th*, 47:2256–2274, 2001.

[5] R. Gilmer. *Multiplicative Ideal Theory*. Marcel Dekker, 1972.

[6] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Th.*, 40:301–319, 1994.

[7] M. Kuijper, X. Wu, and U. Parampalli. Behavioral models over rings—minimal representations and applications to coding and sequences. In *Proceedings of the 16th IFAC World Congress*, pages 1–6, Prague, Czech Republic, July 4-8, 2005.

[8] P. Lu, M. Liu, and U. Oberst. Linear recurring arrays, linear systems and multidimensional cyclic codes over Quasi-Frobenius rings. *Acta Applicandae Mathematicae*, 80:175–198, 2004.

[9] B.R. McDonald. *Finite rings with identity*. Marcel Dekker, New York, 1974.

[10] G. Norton. On minimal realization over a finite chain ring. *Designs, Codes and Cryptography*, 16:161–178, 1999.

[11] J.W. Polderman and J.C. Willems. *Introduction to mathematical systems theory: a behavioral approach*, volume 26 of *Texts in Applied Mathematics*. Springer, New York NY, USA, 1997.

[12] D. Sridhara and T.E. Fuja. LDPC codes over rings for PSK modulation. *IEEE Trans. Inf. Th.*, 51(9):3209–3220, 2005.

[13] P. Udaya and M.U. Siddiqi. Generalized GMW quadriphase sequences satisfying the Welch bound with equality. *Appl. Algebra Engrg. Comm. Comput.*, 10:203–225, 2000.

[14] V.V. Vazirani, H. Saran, and B.S. Rajan. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th.*, 42:1839–1854, 1996.

[15] J.C. Willems. From time series to linear system. part I: Finite-dimensional linear time invariant systems. *Automatica*, 22:561–580, 1986.

[16] J.C. Willems. From time series to linear system. part II: Exact modelling. *Automatica*, 22:675–694, 1986.

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