Proceedings of the
46th IEEE Conference on Decision and Control
New Orleans, LA, USA, Dec. 12-14, 2007

Row reduced representations of behaviors over finite rings

Margreta Kuijper
Dep. El. and Electr. Eng.
The University of Melbourne
Australia
m.kuijper@ee.unimelb.edu.au

Raquel Pinto
Dep. Math.
University of Aveiro
Portugal
raquel@ua.pt

Jan Willem Polderman
Dep. Appl. Math.
University of Twente
The Netherlands
j.w.polderman@math.utwente.nl

Abstract— **Row reduced representations of behaviors over fields posses a number of useful properties. Perhaps the most important feature is the predictable degree property. This property allows a finite parametrization of the module generated by the rows of the row reduced matrix with prior computable bounds. In this paper we study row-reducedness of representations of behaviors over rings of the form $\mathbb{Z}_{p^r}$, where p is a prime number. Using a restricted calculus within $\mathbb{Z}_{p^r}$ we derive a meaningful and computable notion of row-reducedness.**

I. Motivation and problem statements

In the behavioral theory, the central role is played by the set $\mathcal{B}$ of trajectories that characterize a dynamical system Σ, see the textbook [11]. In fact, a 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 of these systems, in particular kernel representations, see also [7], [5].

For $r \geq 2$ the ring $\mathbb{Z}_{p^r}$ is not a field. All multiples of p in $\mathbb{Z}_{p^r}$ are zero divisors and this induces several difficulties. Classical fundamental results for systems over a field are open problems for systems over the ring $\mathbb{Z}_{p^r}$. One of these open problems is the development of a theory of row reduced representations and accompanying parametrization results.

For behavioral systems over fields there exists a well-developed theory of representations, see e.g. [11], [14], [15], [16]. 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 point wise 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 $\mathcal{B} = \text{span}\ \{(3, 3, 3, \cdots)\}$ a kernel representation is given by $(\sigma - 1)\boldsymbol{w} = 0$.

Example 1.1: 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

$$A(\sigma)\boldsymbol{w} = 0 \quad \text{where} \quad A(\xi) = \begin{bmatrix} \xi - 1 & 3 \end{bmatrix}^{\mathrm{T}}.$$

In contrast to what would hold in the field case, there does not exist a single polynomial $a(\xi) \in \mathcal{R}[\xi]$ such that $\mathcal{B}$ is given by $a(\sigma)\boldsymbol{w} = 0$. $\diamond$

The 1997 paper [1] introduces a specific type of kernel representation, called the "adapted form". It is shown in [1] that any linear σ-invariant complete behavior over the ring $\mathbb{Z}_{p^r}$ admits an adapted kernel representation. In this paper we address and solve the open problem, posed in [1], of deriving a theory of *row-reduced* kernel representations for systems over $\mathbb{Z}_{p^r}$.

For polynomial matrices over a field $\mathbb{F}$, the concept of row reducedness is alternatively formulated in terms of the *predictable-degree property* (terminology from Forney's paper [2]), which is defined below. Recall that the row degree of a row polynomial vector is defined as the maximum of the degrees of its components.

Definition 1.2: Let the matrix $R(\xi) \in \mathbb{F}^{g\times q}[\xi]$ with row degrees $d_1, \ldots, d_g$. $R(\xi)$ is said to have the *predictable-degree property* if for any nonzero polynomial vector $a(\xi) = \begin{bmatrix} a_1(\xi) & \cdots & a_g(\xi) \end{bmatrix} \in \mathbb{F}^g[\xi]$ there holds that row degree of $a(\xi)R(\xi) = \max_{1\leq i\leq g}\ (d_i + \deg a_i(\xi))$. $\diamond$

Thus the row degree of $a(\xi)R(\xi)$ can be *predicted* from the degrees in $a(\xi)$ and the row degrees of $R(\xi)$. For the field case it is proven in [2] and in [4, Thm 6.3-13] that the above property is equivalent to the property that the *leading row coefficient matrix* of $R(\xi)$ has full row rank, i.e., that $R(\xi)$ is *row reduced*. See also [13]. This provides an easy test to establish whether a kernel representation has the predictable-degree property or not. Furthermore, for any behavior over a field that can be represented by a kernel representation, there exists a row reduced kernel representation.

In this paper we define a concept of "p-predictable-degree property" that is tailored to $\mathbb{Z}_{p^r}$ and seeks to exploit the field properties of the subset $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$. At the same time, we also introduce a particular type of kernel representation, the "composed form", that resembles the above adapted form but is less restrictive. We show that the combination of this composed form and the p-predictable-degree property provides the appropriate setting for the ring case, in the sense that we are able to extend several classical results from the field case to the ring case. More

Partly supported by the Australian Research Council (ARC) as well as the Dutch Organization for Scientific Research (NWO).

Supported in part by the Portuguese Science Foundation (FCT) through the Unidade de Investigacao Matematica e Aplicacoes of the University of Aveiro, Portugal.

1-4244-1498-9/07/$25.00 ©2007 IEEE.

specifically, we develop a practical "p-row reducedness"-test that generalizes the rank test on the leading row coefficient matrix from the field case. We also show that any behavior over $\mathbb{Z}_{p^r}$ that can be represented by a kernel representation, admits a p-row reduced kernel representation in composed form and give an algorithm to construct such a representation.

Our motivation for considering systems over $\mathbb{Z}_{p^r}$ stems from applications in the communications area. The communications literature has dedicated considerable attention to error-correcting codes and sequences over $\mathbb{Z}_{p^r}$. This paper seeks to contribute to the fundamentals of a comprehensive theory of polynomial representations of systems over $\mathbb{Z}_{p^r}$. Applications are in the area of convolutional codes as well as minimal partial interpolation over $\mathbb{Z}_{p^r}$. In the latter area there are several open problems, see [10], [7]. This is relevant for Reed-Solomon codes over $\mathbb{Z}_{p^r}$, as well as for sequences over $\mathbb{Z}_{p^r}$. The present paper is a condensed version of [6]. For more details and proofs the reader is referred to [6].

II. Preliminary results on $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^r}[\xi]$

In this section we first give preliminaries on vectors and matrices over $\mathbb{Z}_{p^r}$ and close the section with preliminaries on polynomials and polynomial matrices with coefficients in $\mathbb{Z}_{p^r}$. We use the notation$[A]_p$ to denote A modulo p. To get around the difficulty of the presence of zero divisors in $\mathbb{Z}_{p^r}$, the 1996 paper [12] presents several fundamental results that culminate in a concept of "p-basis" and "p-dimension" for modules in $\mathbb{Z}_{p^r}^q$. Their exposition starts with the very useful concepts of "p-linear combination", "p-linear independence" and "p-generator sequence". We use these concepts in section IV, where they are connected to row reducedness.

Definition 2.1: [12] Let $v_1, \dots, v_k$ be vectors in $\mathbb{Z}_{p^r}^q$ and let $a_j \in \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$ for $j = 1, \dots, k$. Then the vector

$$\sum_{j=1}^{k} a_j v_j$$

is called a *p-linear combination* of $v_1, \dots, v_k$. The set of all p-linear combinations of $v_1, \dots, v_k$ is called the *p-span* of $\{v_1, \cdots, v_k\}$. $\diamond$

Definition 2.2: [12] An ordered sequence of vectors $(v_1, v_2, \cdots, v_k)$, with $v_i \in \mathbb{Z}_{p^r}^q$, is said to be a *$p$-generator sequence* if

1) for $1 \leq i \leq k-1$, the vector pv_i can be written as a p-linear combination of $v_{i+1}, \dots, v_k$ and
2) pv_k is the zero vector.

Theorem 2.3: [12, Thm 6.2] Let $(v_1, v_2, \cdots, v_k)$ be a p-generator sequence with $v_i \in \mathbb{Z}_{p^r}^q$ for $1 \leq i \leq k$. Then

$$p-\text{span } (v_1, v_2, \cdots, v_k) = \text{span } (v_1, v_2, \cdots, v_k).$$

In particular, $p-$span $(v_1, v_2, \cdots, v_k)$ is a submodule of $\mathbb{Z}_{p^r}^q$. $\diamond$

Definition 2.4: Let $v_1, \dots, v_k$ be vectors in $\mathbb{Z}_{p^r}^q$. Then they are said to be *p-linearly independent* if there does not exist a nontrivial p-linear combination of $v_1, \dots, v_k$ that equals zero. $\diamond$

In [12, Thm 6.11] it is proven that for any submodule M of $\mathbb{Z}_{p^r}^q$ there exists a p-linearly independent p-generator sequence $(v_1, v_2, \cdots, v_k)$ such that $M = p-$span $(v_1, v_2, \cdots, v_k)$. In fact, [12, p. 1846] gives a Gaussian elimination algorithm that takes as its input a set of arbitrary vectors in $\mathbb{Z}_{p^r}^q$. Denoting the span of these vectors by M, the algorithm then constructs a p-linearly independent p-generator sequence $(v_1, v_2, \cdots, v_k)$, such that $p-$span $(v_1, v_2, \cdots, v_k) = M$. Such a sequence has the property that each vector in M can be written *uniquely* as a p-linear combination of $v_1, \cdots, v_k$. Since the latter result is needed in the sequel, but not explicitly proven in [12], we present it in the following lemma.

Lemma 2.5: Let $(v_1, v_2, \cdots, v_k)$ be a p-linearly independent p-generator sequence with $v_i \in \mathbb{Z}_{p^r}^q$ for $1 \leq i \leq k$. Then any vector in $p-$span $(v_1, v_2, \cdots, v_k)$ can be written uniquely as a p-linear combination of $v_1, v_2, \dots, v_k$. $\diamond$

In [12] a *p-basis* for a submodule M of $\mathbb{Z}_{p^r}^q$ is defined as a p-linearly independent p-generator sequence, such that $p-$span $(v_1, v_2, \cdots, v_k) = M$. By Lemma 2.5, a p-basis consisting of k elements generates a module of cardinality p^k and therefore all p-bases of a given module M have the same number of elements. This justifies the following definition.

Definition 2.6: [12] Let M be a submodule of $\mathbb{Z}_{p^r}^q$ with a p-basis $(v_1, \dots, v_k)$. Then the *p-dimension* of M is defined as $p-\dim\,(M) = k$. $\diamond$

Lemma 2.7: Let $(v_1, v_2, \cdots, v_k)$ be a p-generator sequence with $v_i \in \mathbb{Z}_{p^r}^q$ for $1 \leq i \leq k$. Then $v_1, v_2, \cdots, v_k$ are p-linearly independent if and only if
$p-\dim\,(\text{span } (v_1, v_2, \cdots, v_k)) = k$ $\diamond$

Since the Gaussian elimination algorithm of [12, p. 1846]) can be used to determine the p-dimension of the span of an arbitrary set of vectors in $\mathbb{Z}_{p^r}^q$, the above lemma gives rise to an easy test for p-linear independence of a p-generator sequence. Note that the lemma does not hold if the p-generator sequence property is missing.

We next present several preliminaries on polynomials, polynomial vectors and polynomial matrices with coefficients in $\mathbb{Z}_{p^r}$, see for example the standard reference [9].

Definition 2.8: The *degree* of a nonzero polynomial $f(\xi) \in \mathbb{Z}_{p^r}[\xi]$, written as $f(\xi) = f_0 + f_1\xi + \ldots + f_n\xi^n$, is defined as

$$\deg\,(f(\xi)) = \max_{0 \leq i \leq n} \{i \mid f_i \neq 0\}.$$

The coefficient of the term $\xi^{\deg f(\xi)}$ in $f(\xi)$ (i.e., $f_{\deg f}$) is called the *leading coefficient* of $f(\xi)$. $\diamond$

Definition 2.9: The *row degree* of a nonzero polynomial vector $v(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$ is defined as

$$\text{rowdeg}\,(v(\xi)) = \max_{1 \leq i \leq q} \{\deg v_i(\xi)\}.$$

The vector of coefficients of the term $\xi^{\deg v(\xi)}$ in $v(\xi)$ is called the *leading row coefficient vector* of v and is denoted by v^{lrc}. $\diamond$

Definition 2.10: Let $A(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k\times q}[\xi]$. The *row degrees* of $A(\xi)$ are defined as the row degrees of its rows. The *leading row coefficient matrix* of $A(\xi)$ consists of the leading row coefficient vectors of its rows and is denoted by $A^{\rm lrc} \in \mathbb{Z}_{p^r}^{k\times q}$. ◇

Definition 2.11: A polynomial $f(\xi) \in \mathbb{Z}_{p^r}[\xi]$ is called a *unit polynomial* if there exists a polynomial $u(\xi) \in \mathbb{Z}_{p^r}[\xi]$ such that $u(\xi)f(\xi) \equiv 1$. ◇

Lemma 2.12: A polynomial $f(\xi) \in \mathbb{Z}_{p^r}[\xi]$, written as $f(\xi) = f_0 + f_1\xi + \ldots + f_n\xi^n$, is a unit polynomial iff

$$\max_{0\le i\le n} \{i \mid f_i \text{ is a unit in } \mathbb{Z}_{p^r}\} = 0.$$

The next lemma generalizes Lemma 2.12 to the matrix case.

Lemma 2.13: Let $U(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{q\times q}[\xi]$. The following statements are equivalent:

- $U(\xi)$ is unimodular
- $\det U(\xi)$ is a unit polynomial
- $[U(\xi)]_p$ is a unimodular matrix in $\mathbb{Z}_p^{q\times q}[\xi]$.

III. p-Generator sequences in $\mathbb{Z}_{p^r}[\xi]$

In the previous section we recalled several notions from [12] for submodules consisting of *constant* vectors. In this section we extend these notions to submodules consisting of *polynomial* vectors. Although some of the definitions for the constant case carry over straightforwardly to the polynomial case, there are some major differences due to the existence of a degree concept for polynomial vectors. In this section we introduce the notion of "reduced p-basis" for modules in $\mathbb{Z}_{p^r}^q[\xi]$ and show how to construct such a basis. The results of this section form the main contributions of the paper as they play a crucial role in section IV where they are connected to row-reducedness and the predictable degree property for kernel representations of behaviors over $\mathbb{Z}_{p^r}$. The notions of p-linear combination, p-generator sequence and p-linear independence for vectors in $\mathbb{Z}_{p^r}^q$ (Definitions 2.1, 2.2 and 2.4) are straightforwardly extended to vectors in $\mathbb{Z}_{p^r}^q[\xi]$.

Definition 3.1: Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$ and let $a_j(\xi)$ be polynomials with coefficients in $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$. Then the vector

$$\sum_{j=1}^{k} a_j(\xi)v_j(\xi)$$

is called a *p-linear combination* of $v_1(\xi), \ldots, v_k(\xi)$. The set of all p-linear combinations of $v_1(\xi), \ldots, v_k(\xi)$ is called the *p-span* of $\{v_1(\xi), \cdots, v_k(\xi)\}$. ◇

Definition 3.2: An ordered sequence of vectors $(v_1(\xi), \cdots, v_k(\xi))$, with $v_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$, is said to be a *$p$-generator sequence* if

1) for $1 \le i \le k-1$, the vector $pv_i(\xi)$ can be written as a p-linear combination of $v_{i+1}(\xi), \ldots, v_k(\xi)$ and

2) $pv_k(\xi)$ equals the zero vector.

The following theorem is a generalization of Theorem 2.3.

Theorem 3.3: Let a p-generator sequence be given by $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ with $v_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$ for $1 \le i \le k$. Then

$$p\text{−span } (v_1(\xi), v_2(\xi), \cdots, v_k(\xi)) = \\ \text{span } (v_1(\xi), v_2(\xi), \cdots, v_k(\xi)).$$

In particular, p−span $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ is a submodule of $\mathbb{Z}_{p^r}^q[\xi]$. ◇

Definition 3.4: Let $v_1(\xi), \ldots, v_k(\xi)$ be vectors in $\mathbb{Z}_{p^r}^q[\xi]$. Then they are said to be *p-linearly independent* if there does not exist a nontrivial p-linear combination of $v_1(\xi), \ldots, v_k(\xi)$ that equals zero. ◇

The following lemma shows that p-linearly independent p-generator sequences in $\mathbb{Z}_{p^r}^q[\xi]$ have an important property in common with p-linearly independent p-generator sequences in $\mathbb{Z}_{p^r}^q$; it generalizes Lemma 2.5 to polynomial vectors.

Lemma 3.5: Let $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ be a p-linearly independent p-generator sequence in $\mathbb{Z}_{p^r}^q[\xi]$. Then every vector in p−span $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ can be written uniquely as a p-linear combination of $v_1(\xi), v_2(\xi), \ldots, v_k(\xi)$. ◇

It is not straightforward to define a concept of p-basis for polynomial vectors that mirrors the theory for constant vectors, as recounted in section II. This is due to the fact that a p-linear combination in $\mathbb{Z}_{p^r}^q[\xi]$ involves coefficients that are polynomials rather than constants. In the sequel we construct a concept of basis whereby the degrees of these polynomial coefficients are constrained. Recall from section II (Definition 2.9) that the leading row coefficient vector of a polynomial vector $v(\xi)$ in $\mathbb{Z}_{p^r}^q[\xi]$ is denoted by the vector $v^{\rm lrc} \in \mathbb{Z}_{p^r}^q$.

Definition 3.6: Let M be a submodule of $\mathbb{Z}_{p^r}^q[\xi]$, written as a p-span of a p-generator sequence $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$. Then $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ is called a *reduced p-basis* for M if the vectors $v_1^{\rm lrc}, v_2^{\rm lrc}, \ldots, v_k^{\rm lrc}$ are p-linearly independent in $\mathbb{Z}_{p^r}^q$. ◇

Lemma 3.7: Let M be a submodule of $\mathbb{Z}_{p^r}^q[\xi]$ with reduced p-basis $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$. Then $v_1(\xi), \cdots, v_k(\xi)$ are p-linearly independent in $\mathbb{Z}_{p^r}^q[\xi]$. ◇

A reduced p-basis exhibits predictable degree properties, as expressed by the following theorem.

Theorem 3.8: Let $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ be a reduced p-basis for a module M in $\mathbb{Z}_{p^r}^q[\xi]$. Let $v(\xi) \in M$. Denote rowdeg $v(\xi)$ by d and rowdeg $v_i(\xi)$ by d_i for $i = 1, \ldots, k$. Then $v(\xi)$ can be written uniquely as a p-linear combination

$$v(\xi) = a_1(\xi)v_1(\xi) + \cdots + a_k(\xi)v_k(\xi), \tag{1}$$

where $a_i(\xi)$ is a polynomial of degree $\le d - d_i$ with coefficients in $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$. ◇

Lemma 3.9: Let $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ be a p-generator sequence in $\mathbb{Z}_{p^r}^q[\xi]$ with $k \ge 2$. Assume that $v_2^{\rm lrc}, v_3^{\rm lrc}, \ldots, v_k^{\rm lrc}$ are p-linearly independent in $\mathbb{Z}_{p^r}^q$. Then $(v_1^{\rm lrc}, v_2^{\rm lrc}, \ldots, v_k^{\rm lrc})$ is a p-generator sequence in $\mathbb{Z}_{p^r}^q$. ◇

From Lemmas 2.7, 3.9 we immediately get:

Theorem 3.10: Let M be a submodule of $\mathbb{Z}_{p^r}^q[\xi]$, written as a p-span of a p-generator sequence $(v_1(\xi), v_2(\xi), \ldots, v_k(\xi))$. Then $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ is a reduced p-basis for M if and only if the following two conditions hold:

1) $(v_1^{\rm lrc}, v_2^{\rm lrc}, \ldots, v_k^{\rm lrc})$ is a p-generator sequence in $\mathbb{Z}_{p^r}^q$.
2) $p-\dim$ (span $(v_1^{\rm lrc}, v_2^{\rm lrc}, \ldots, v_k^{\rm lrc}) = k$.

The p-dimension of the span of a p-generator sequence in $\mathbb{Z}_{p^r}^q$ can easily be calculated by the Gaussian elimination algorithm of [12, p. 1846]), which brings the vectors in the sequence into row echelon form. By the above theorem, applying this algorithm to a p-generator sequence $(v_1^{\rm lrc}, v_2^{\rm lrc}, \ldots, v_k^{\rm lrc})$ then provides a practical method to establish whether a p-generator sequence $(v_1(\xi), v_2(\xi), \cdots, v_k(\xi))$ is a reduced p-basis in $\mathbb{Z}_{p^r}^q[\xi]$.

We next show that every submodule M of $\mathbb{Z}_{p^r}^q[\xi]$ has a reduced p-basis. Below we give an algorithm that takes as its input an arbitrary set of vectors in $\mathbb{Z}_{p^r}^q[\xi]$ that span M and produces a reduced p-basis for M as its output.

For $r = 1$, i.e., the field case $\mathbb{Z}_p^q[\xi]$, the algorithm boils down to classical row reduction operations, as found in [13], [17], [2], [4].

Algorithm 3.11:
Input data: module $M :=$ span $(w_1(\xi), \ldots, w_g(\xi))$ with $w_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$.
Initialization: define p-generator sequence

$$V \leftarrow (p^j w_1(\xi), \ldots, p^j w_g(\xi))_{j=0\ldots p-1}. \tag{2}$$

Step 1: Re-order V according to non-increasing row degree such that

$$V \leftarrow (v_1(\xi), \ldots, v_k(\xi), 0, \ldots, 0),$$

making sure that vectors of equal row degree are not swapped. Denoting $d_i :=$ rowdeg $v_i(\xi)$ for $1 \leq i \leq k$, we then have $d_i \geq d_j$ for $i < j$.
Step 2: Remove zero vectors, resulting in

$$V \leftarrow (v_1(\xi), \ldots, v_k(\xi)).$$

Step 3: Determine smallest ℓ such that

1) $(v_{\ell+1}^{\rm lrc}, \ldots, v_k^{\rm lrc})$ is a p-generator sequence in $\mathbb{Z}_{p^r}^q$ and
2) $p-\dim$ (span $(v_{\ell+1}^{\rm lrc}, \ldots, v_k^{\rm lrc})) = k - \ell$.

(to check the latter condition use the Gaussian elimination algorithm of [12, p. 1846]).
Step 4: For $i = 1, \ldots, k - \ell$ let $\alpha_i \in \mathbb{Z}_{p^r}$ be such that

$$v_\ell^{\rm lrc} + \alpha_1 v_{\ell+1}^{\rm lrc} + \alpha_2 v_{\ell+2}^{\rm lrc} + \ldots + \alpha_{k-\ell} v_k^{\rm lrc} = 0. \tag{3}$$

Replace $v_\ell(\xi)$ by

$$\begin{aligned} &v_\ell(\xi) + \alpha_1 \xi^{d_\ell - d_{\ell+1}} v_{\ell+1}(\xi) + \\ &\alpha_2 \xi^{d_\ell - d_{\ell+2}} v_{\ell+2}(\xi) + \cdots + \alpha_{k-\ell} \xi^{d_\ell - d_k} v_k(\xi). \end{aligned} \tag{4}$$

Go to Step 1.
The algorithm stops when $\ell = 0$ at Step 3.
Output data: $(v_1(\xi), \ldots, v_k(\xi))$.

Theorem 3.12: Let a module M be given as $M =$ span $(w_1(\xi), \ldots, w_g(\xi))$ with $w_i(\xi) \in \mathbb{Z}_{p^r}^q[\xi]$. Then Algorithm 3.11 produces a reduced p-basis $(v_1(\xi), \ldots, v_k(\xi))$ for M. ◇

A reduced p-basis of a module M gives rise to several invariants of M, as shown by the following theorem.

Theorem 3.13: Let $(v_1(\xi), \ldots, v_k(\xi))$ and $(\tilde{v}_1(\xi), \ldots, \tilde{v}_{\tilde{k}}(\xi))$ be two reduced p-bases with

$$p-\text{span } (\tilde{v}_1(\xi), \ldots, \tilde{v}_{\tilde{k}}(\xi)) = p-\text{span } (v_1(\xi), \ldots, v_k(\xi)).$$

Then $\tilde{k} = k$. Furthermore, denoting rowdeg $v_i(\xi)$ by d_i and rowdeg $\tilde{v}_i(\xi)$ by $\tilde{d}_i$ we have that $\tilde{d}_i = d_i$ for $i = 1, \ldots, k$. ◇

Because of the above theorem the next notion is well-defined.

Definition 3.14: Let M be a submodule of $\mathbb{Z}_{p^r}^q[\xi]$. Let $(v_1(\xi), \ldots, v_k(\xi))$ be a reduced p-basis of M. Denote rowdeg $v_i(\xi)$ by d_i for $i = 1, \ldots, k$. Then the *p-dimension* of M is defined as $p-\dim\ (M) = k$. The *p-degrees* of M are defined as $d_1, \ldots, d_k$. ◇

Note that it follows from the construction in Algorithm 3.11 that for any set of vectors $\{w_1(\xi), \ldots, w_g(\xi)\}$ in $\mathbb{Z}_{p^r}^q[\xi]$ we have $p-\dim$ (span $(w_1, \ldots, w_g)) \leq gr$.

IV. Parametrization of all annihilators

In this section we set out to develop a kernel representation that has the predictable-degree property.

Example 4.1: In $\mathbb{Z}_{27}$: consider the behavior

$$\mathcal{B} = \text{span } \left\{ \left(\begin{bmatrix} 9 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots \right) \right. .$$

A kernel representation for $\mathcal{B}$ is given by $A(\sigma)\boldsymbol{w} = 0$, where

$$A(\xi) = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \end{bmatrix}. \tag{5}$$

$A(\xi)$ does not have the predictable-degree property since

$$[9\ \xi]\, A(\xi) = [\xi\ 0]\,.$$

In the above example it is not possible to apply the usual row reduction operations that are familiar from the field setting. This is due to the fact that 9 is a zero divisor in $\mathbb{Z}_{27}$. So how to go about deriving an equivalent kernel representation that possesses the predictable-degree property? In this section we put the results of the previous section to work. We first define the concepts of "p-predictable degree property" and "p-row reduced" that turn out to be appropriate for our ring setting.

Definition 4.2: Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k\times q}[\xi]$ with row degrees $d_1, \ldots, d_k$. Let $a(\xi) = \left[\ a_1(\xi) \quad \cdots \quad a_k(\xi)\ \right]$ be a nonzero polynomial vector with coefficients in $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$. Then $R(\xi)$ is said to have the *p-predictable-degree property* if the row degree of $a(\xi)R(\xi)$ equals

$$\max_{1\leq i\leq k}\ (d_i + \deg a_i).$$

Definition 4.3: Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k\times q}[\xi]$. Then $R(\xi)$ is *p-row-reduced* if the rows of its leading row coefficient matrix are p-linearly independent in $\mathbb{Z}_{p^r}^q$. ◇

Example 4.4: In $\mathbb{Z}_{27}$: consider again the behavior $\mathcal{B}$ of Example 4.1, given by $A(\sigma)\boldsymbol{w} = 0$ with $A(\xi)$ defined in (5).

A kernel representation for $\mathcal{B}$ whose rows constitute a p-linearly independent p-generator sequence is immediately found. It is given by $\tilde{R}(\sigma)\boldsymbol{w} = 0$, where

$$\tilde{R}(\xi) = \begin{bmatrix} A(\xi) \\ pA(\xi) \\ \vdots \\ p^{r-1}A(\xi) \end{bmatrix} = \begin{bmatrix} 0 & \xi^2 \\ 1 & 18\xi \\ 0 & 3\xi^2 \\ 3 & 0 \\ 0 & 9\xi^2 \\ 9 & 0 \end{bmatrix}. \qquad (6)$$

Such representation is in adapted form as defined in [1]. Its leading row coefficient matrix equals

$$\tilde{R}^{\mathrm{lrc}} = \begin{bmatrix} 0 & 0 & 0 & 3 & 0 & 9 \\ 1 & 18 & 3 & 0 & 9 & 0 \end{bmatrix}^{\mathrm{T}}$$

It is not difficult to see that the matrix $\tilde{R}(\xi)$ is not p-row-reduced. An alternative kernel representation for $\mathcal{B}$ is given by $R(\sigma)\boldsymbol{w} = 0$, where

$$R(\xi) = \begin{bmatrix} 0 & 0 & 14 & \xi & 3 & 9 \\ \xi^2 & 3\xi^2 & 9\xi & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$$

Its leading row coefficient matrix equals

$$R^{\mathrm{lrc}} = \begin{bmatrix} 0 & 0 & 0 & 1 & 3 & 9 \\ 1 & 3 & 9 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$$

It is not difficult to see that the rows of R^{lrc} are 3-linearly independent, so that the matrix $R(\xi)$ is p-row-reduced. $\diamond$

We now present the first main result of this section which connects the p-predictable degree property with p-row-reducedness.

Theorem 4.5: Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k\times q}[\xi]$. Then $R(\xi)$ has the p-predictable degree property if and only if it is p-row-reduced. $\diamond$

Example 4.6: In $\mathbb{Z}_{27}$: consider again the behavior $\mathcal{B}$ of Example 4.4 with the adapted representation $\tilde{R}(\sigma)\boldsymbol{w} = 0$, where $\tilde{R}(\xi)$ is given by (6). The matrix $\tilde{R}(\xi)$ does not have the p-predictable degree property, since

$$\begin{bmatrix} 0 & \xi & 0 & 0 & 0 & 1 \end{bmatrix} \tilde{R}(\xi) = \begin{bmatrix} \xi & 0 \end{bmatrix}.$$

Indeed the matrix $\tilde{R}(\xi)$ is not p-row reduced. $\diamond$

It can be shown that the behavior of the above example does not allow for a p-row reduced kernel representation in adapted form. Because of this, we step away from the adapted form and introduce a less restrictive type of kernel representation which we call the "composed form", defined below. Later in this section we put Algorithm 3.11 to work to show that any behavior that can be represented by a kernel representation, admits a p-row reduced kernel representation in composed form. Below we see that the composed form is essential for our main parametrization result.

Definition 4.7: Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k\times q}[\xi]$. Then $R(\xi)$ is defined to be in *composed form* if there exists a row permutation matrix P such that the rows of $PR(\xi)$ are a p-generator sequence (Definition 3.2) in $\mathbb{Z}_{p^r}^{q}[\xi]$. $\diamond$

As remarked in [12], the concept of "p-generator sequence" coincides with the concept of "generating system along a composition chain" in commutative ring theory, see [8]. This explains our terminology "composed form".

It can be shown that the adapted form in [1] is a special case of the composed form. In other words, the composed form provides a less restrictive type of kernel representation that turns out to be suitable for row-reducedness issues.

In defining the p-predictable degree property (Definition 4.2), a crucial feature is that coefficients are restricted to the subset $\{0, 1, \ldots, p-1\}$ of $\mathbb{Z}_{p^r}$. When coupled with the composed form, this restriction does not weaken the usefulness of the concept, as compared to the field case. This is due to a special property of the composed form, that follows immediately from Theorem 3.3: for any matrix $R(\xi)$ in composed form and $F(\xi)$ in $\mathbb{Z}_{p^r}^{k}[\xi]$, the vector $F(\xi)R(\xi)$ can be rewritten as $\bar{F}(\xi)R(\xi)$, where $\bar{F}(\xi)$ is a vector in $\mathbb{Z}_{p^r}^{k}[\xi]$ with coefficients restricted to the subset $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$.

We now present the second main result of this section which demonstrates that the combination of the p-predictable degree property and the composed form is powerful enough to yield a parametrization result for annihilators of $\mathcal{B}$ that is the ring counterpart of the field case.

Theorem 4.8: Let $\mathcal{B}$ be a behavior given by $R(\sigma)\boldsymbol{w} = 0$ where $R(\xi) \in \mathbb{Z}_{p^r}^{k\times q}[\xi]$ is in composed form and has the p-predictable-degree property. Denote the row degrees of $R(\xi)$ by $d_1, \ldots, d_k$. Let $V(\xi)$ be a polynomial vector in $\mathbb{Z}_{p^r}^{q}[\xi]$ of row degree d. Then $V(\xi)$ is an annihilator of $\mathcal{B}$ if and only if there exists a unique vector $Q(\xi) = \begin{bmatrix} q_1(\xi) & \cdots & q_k(\xi) \end{bmatrix}$ in $\mathbb{Z}_{p^r}^{k}[\xi]$ such that

1) $V(\xi) = Q(\xi)R(\xi)$
2) $\deg q_i(\xi) \leq d - d_i \quad$ for $i = 1, \ldots, k$
3) the coefficients of $q_i(\xi)$ belong to $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$ for $i = 1, \ldots, k$.

As in the field case, the strength of the above theorem is in the "only if"-part: condition 2 yields an explicit parametrization of annihilators of a pre-specified row degree, where the bound on the number of coefficients can be calculated a priori.

Theorems 3.10 and 4.5 immediately lead to the following theorem which gives an easy test for establishing whether a kernel representation in composed form is p-row reduced. Again the Gaussian elimination procedure of [12, p. 1846]) can be used to check the second condition in the theorem.

Theorem 4.9: Let $R(\xi)$ be a matrix in $\mathbb{Z}_{p^r}^{k\times q}[\xi]$ in composed form. Let P be a row permutation matrix such that the rows of $PR(\xi)$ are a p-generator sequence in $\mathbb{Z}_{p^r}^{q}[\xi]$. Denote the rows of PR^{lrc} by $w_1, \ldots, w_k$. Then $R(\xi)$ has the p-predictable degree property if and only if the following two conditions hold:

1) $(w_1, \ldots, w_k)$ is a p-generator sequence in $\mathbb{Z}_{p^r}^{q}$.
2) $p-\dim\,(\mathrm{span}\,(w_1, \ldots, w_k)) = k$.

Note that for the case $r = 1$, i.e., for behaviors over the field $\mathbb{Z}_p$, the above theorem yields the classical row reducedness test which amounts to R^{lrc} having full row rank.

In the next theorem we present the third main result of this section in showing that any behavior that can be represented by a kernel representation, admits a p-row-reduced kernel representation in composed form. The proof is constructive and based on Algorithm 3.11.

Theorem 4.10: Let $\mathcal{B}$ be a behavior over $\mathbb{Z}_{p^r}$. Then there exists a kernel representation $R(\sigma)\boldsymbol{w} = 0$ of $\mathcal{B}$, such that $R(\xi)$ is in composed p-row reduced form. $\diamond$

Example 4.11: In $\mathbb{Z}_{27}$: consider again the behavior $\mathcal{B}$ of Example 4.1.

The initialization step of Algorithm 3.11 essentially considers the adapted form (6), given by

$$\begin{bmatrix} 0 & 1 & 0 & 3 & 0 & 9 \\ \xi^2 & 18\xi & 3\xi^2 & 0 & 9\xi^2 & 0 \end{bmatrix}^{\mathrm{T}}.$$

Performing the row permutations of Step 1 of Algorithm 3.11 gives

$$\begin{bmatrix} 0 & \xi^2 \\ 0 & 3\xi^2 \\ 0 & 9\xi^2 \\ 1 & 18\xi \\ 3 & 0 \\ 9 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 0 & 3 \\ 0 & 9 \\ 0 & 18 \\ 3 & 0 \\ 9 & 0 \end{bmatrix}. \tag{7}$$

where the second matrix is the leading row coefficient matrix. We now demonstrate how Step 3 in the algorithm is performed using Gaussian elimination. Clearly, the last 3 rows of the leading row coefficient matrix in (7) are a p-linearly independent p-generator sequence. Let us now denote the p-generator sequence consisting of the last 4 rows of the leading row coefficient matrix in (7) by V. Thus

$$V = ([0\ 9], [0\ 18], [3\ 0], [9\ 0]).$$

Applying the Gaussian elimination algorithm of [12, p. 1846]) to V, it follows that $([0\ 9], [3\ 0], [9\ 0])$ is a p-basis in row echelon form for $p-\mathrm{span}\ (V)$. Thus

$$p-\dim\ (p-\mathrm{span}\ (V)) = 3,$$

so that the vectors in V are not p-linearly independent. Indeed, $[0\ 9] + [0\ 18]$ is a nontrivial p-linear combination that equals zero. Step 4 yields premultiplication by the unimodular matrix $U(\xi)$ that is obtained by changing the zero at the $(3, 4)$ spot in the 6×6 unit matrix into a ξ. Note that, by Lemma 2.13, the matrix $U(\xi)$ is indeed unimodular. Premultiplication by $U(\xi)$ yields

$$R(\xi) = \begin{bmatrix} 0 & 0 & \xi & 1 & 3 & 9 \\ \xi^2 & 3\xi^2 & 0 & 18\xi & 0 & 0 \end{bmatrix}^{\mathrm{T}}.$$

Going back to Step 1, no further row permutations are needed—the matrix $R(\xi)$ is in composed form and p-row-reduced, as desired. $\diamond$

V. Conclusions

In this paper we addressed and solved the open problem, posed in [1], of deriving a theory of row-reduced kernel representations for systems over $\mathbb{Z}_{p^r}$. We showed the importance of this problem in terms of parametrization of annihilators. We found that we had to step away from the adapted form, as found in the literature, and resort to a less restricted form, which we introduced as the "composed form". Our approach has been to extend the concepts and results of [12] to a polynomial context and apply these to the submodule $\mathcal{B}^{\perp}$ of annihilators of $\mathcal{B}$.

Because of this general approach, our results are also applicable to image representations of behaviors over $\mathbb{Z}_{p^r}$. It is a subject of future investigation to develop this further. In particular, the role of the p-degrees of $\mathcal{B}^{\perp}$ in relation to the minimal state space dimension in an input/state/output realization deserves attention.

One of our main results extends the classical leading row coefficient rank test that determines row reducedness in the field case. We derived that row reducedness of a polynomial matrix over $\mathbb{Z}_{p^r}$ involves the composed form as well as a leading row coefficient rank test. The latter is performed via Gaussian elimination.

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 [3], [10]. Generalizations to finite commutative rings (see [9]) and finite abelian groups (as in [12, Sect. IX-C] and [1]) are then also possible.

References

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

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

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

[4] T. Kailath. *Linear Systems*. Prentice Hall, Englewood Cliffs, N.J, 1980.

[5] M. Kuijper, R. Pinto, and J. W. Polderman. Kernel representations for behaviors over finite rings. In *Proceedings of the 17th International Symposium on the Mathematical Theory of Networks and Systems (MTNS)*, pages 2494–2503, Kyoto, Japan, July 2006.

[6] M. Kuijper, R. Pinto, and J.W. Polderman. The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications*, 425(2-3):776–796, 2007.

[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] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1986.

[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] 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.

[13] J.H.M. Wedderburn. *Lectures on matrices*. Dover Phoenix, 1934.

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

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

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

[17] W.A. Wolovich. *Linear multivariable systems*. Springer, New York NY, USA, 1974.