State representations of convolutional codes over a finite ring

D. Napp[a], R. Pinto[b], C. Rocha[*,c]

[a]*Departament of Mathematics, University of Alicante, Spain.*
[b]*Department of Mathematics, University of Aveiro, Portugal.*
[c]*Instituto Superior de Contabilidade e Administração de Coimbra, Instituto Politécnico de Coimbra, Portugal.*

Abstract

In this paper we study finite support convolutional codes over $\mathbb{Z}_{p^r}$ by means of an input-state-output representation. We show that the set of finite weight input-state-output trajectories associated to this type of representations has the structure of a $\mathbb{Z}_{p^r}$-submodule of $\mathbb{Z}_{p^r}^n$ and therefore is a (finite support) convolutional code. Fundamental system-theoretical properties such as observability, reachability or minimality, are investigated in this context.

Key words: Finite rings, Realization theory, Convolutional codes
2010MSC: 14G50, 93B15, 47A48, 94B10

1. Introduction

Convolutional codes are an important class of error correcting codes that are used to achieve reliable communications such as digital video transmission or satellite communications [14]. Since the sixties it has been widely known that convolutional codes and linear systems defined over a finite field are essentially the same objects [27, 34, 35]. In the last decades there has been a renew interest in this connection and many advances have been derived from using the system theoretical framework when dealing with convolutional codes, see [11, 12, 21, 23, 24, 28, 29, 30, 35, 36].

Most of the large body of literature on convolutional codes and on the relation of these codes with linear systems has been devoted to the *field* case. But sometimes it is too restrictive to consider fields and so, part of this theory has been extended to finite rings [8, 16, 18, 19, 20, 25, 33, 41]. This work continues this thread of research and we aim at studying convolutional codes over the ring $\mathbb{Z}_{p^r}$ (where p is a prime and r is an integer) from a system theoretical point of view. Our motivation for considering such a finite ring $\mathbb{Z}_{p^r}$ is due to the fact that this ring has a particular interest since in [26] Massey and Mittelholzer showed that convolutional codes over the ring $\mathbb{Z}_M$ are the most appropriate class of codes for phase modulation. As by the Chinese Remainder Theorem results on codes over $\mathbb{Z}_{p^r}$ can be easily extended to codes over $\mathbb{Z}_M$, most of the theory in the area has been developed considering the ring $\mathbb{Z}_{p^r}$. The algebraic structure of these codes was thoroughly investigated [7, 13, 20, 22, 33] and it was immediately apparent that these codes were more involved than the classical convolutional codes over finite fields. Indeed many important properties that hold

[*] Corresponding author

[1] This work is supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), references UIDB/04106/2020 and UIDP/04106/2020. Diego Napp is partially supported by Ministerio de Ciencia e Innovación via the grant with ref. PID2019-108668GB-I00.

in the field case, fail to be true in the ring case. We denote by $\mathbb{Z}_{p^r}[d]$ the ring of polynomials in the indeterminate d, with coefficients in $\mathbb{Z}_{p^r}$. Mathematically, a convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ of rate k/n can be defined as a free $\mathbb{Z}_{p^r}$-submodule of $\mathbb{Z}_{p^r}^n$ and as such can be described as

$$\mathcal{C} \quad = \quad \mathrm{Im}_{\mathbb{Z}_{p^r}[d]} G(d) = \{u(d)G(d) \,:\, u(d) \in \mathbb{Z}_{p^r}[d]^k\},$$

where $G(d) \in \mathbb{Z}_{p^r}[d]^{k \times n}$ is a full row rank matrix. Such $G(d)$ is called a generator matrix of $\mathcal{C}$. The degree or complexity of $\mathcal{C}$ is the maximum of the degrees of the full size minors of one and hence any generator matrix of $\mathcal{C}$.

State representations of convolutional codes over finite rings have been previously investigated in [4, 5, 17, 20], see also references therein. Here we propose to study finite support convolutional codes using the state framework proposed by J. Rosenthal et al., see [24, 28, 29, 36]. Within this approach the codewords are constituted by both the input and output of an associated linear system and therefore is different from the setting considering driving variable representations [9, 11], (K, L, M)-type representations [37], or other type of representations [3, 10, 16, 38]. In [6] the authors studied state representations of convolutional codes over the ring $R = \mathbb{F}_1 \times \mathbb{F}_2 \times \ldots \mathbb{F}_i \times \ldots \times \mathbb{F}_t$, where for $i = 1, 2, \ldots, t$, $\mathbb{F}_i$ is a finite field.

More concretely, in this work we consider the linear system given by the updating equations

$$\left\{ \begin{array}{rcl} x_{t+1} & = & x_t A + u_t B \\ y_t & = & x_t C + u_t D \end{array} \right. \tag{1}$$

where $A \in \mathbb{Z}_{p^r}^{\ell \times \ell}$, $B \in \mathbb{Z}_{p^r}^{k \times \ell}$, $C \in \mathbb{Z}_{p^r}^{\ell \times n-k}$ and $D \in \mathbb{Z}_{p^r}^{k \times n-k}$ and $x_0 = 0$. We will represent the system (1) by $\Sigma = (A, B, C, D)$ or shortly by Σ. Σ is said to have dimension ℓ and u_t represents the input, x_t the state vector and y_t the output, each at time t.

If we introduce a variable d, usually called the delay operator, to indicate the instant in which each input is introduced into the system, we can represent the input as a formal power sequence

$$u(d) = u_0 + u_1 d + \ldots. = \sum_{t \in \mathbb{N}_0} u_t d^t \in \mathbb{Z}_{p^r}^k[[d]],$$

and in a similar way,

$$y(d) = y_0 + y_1 d + \ldots. = \sum_{t \in \mathbb{N}_0} y_t d^t \in \mathbb{Z}_{p^r}^{n-k}[[d]] \quad \text{and} \quad x(d) = x_0 + x_1 d + \ldots. = \sum_{t \in \mathbb{N}_0} x_t d^t \in \mathbb{Z}_{p^r}^{\ell}[[d]].$$

We focus on the set of trajectories $(x(d),\, u(d),\, y(d)) \in \mathbb{Z}_{p^r}[[d]]^\ell \times \mathbb{Z}_{p^r}[[d]]^k \times \mathbb{Z}_{p^r}[[d]]^{n-k}$ of the system $\sum = (A,\, B,\, C,\, D)$ having finite support, i.e., when $x(d)$, $u(d)$ and $y(d)$ are polynomial vectors, see for instance [36]. We show that the set of such $(u(d), y(d))$ has the structure of a $\mathbb{Z}_{p^r}[d]$-submodule of $\mathbb{Z}_{p^r}[d]^n$ and therefore is a convolutional code. We investigate properties of these convolutional codes such as noncatastrophicity, freeness or complexity, in terms of the system-theoretical properties of the input-state-out representation (1). Finally we discuss the issue of minimal realizations. The main results of the paper are presented in Section 3 but previously we need to establish the necessary background on linear systems, polynomial and rational polynomial matrices over $\mathbb{Z}_{p^r}$. Some results in these preliminaries (Section 2) are new and others easy adaptations to the ring case of results derived for finite fields.

2. Linear systems and polynomial rational matrices over $\mathbb{Z}_{p^r}$

In this section, we present definitions and results that we will use throughout the paper regarding the theory of primeness of polynomial matrices over $\mathbb{Z}_{p^r}$, linear systems and rational matrices over $\mathbb{Z}_{p^r}$, including an algorithm to construct a state realization from a given rational matrix.

2.1. Primeness of polynomial matrices over $\mathbb{Z}_{p^r}$

When the coefficients of the polynomials are elements in a field, the notion of left primeness is well understood and fully characterized. For the case of multivariable polynomials matrices over a field three classes of left primeness were defined: minor prime, zero prime and weakly zero prime, see [32, 39, 40]. Similarly, when the coefficients of the polynomial in one variable belong to the ring $\mathbb{Z}_{p^r}$, one can distinguish two distinct notions of primeness, namely, zero prime and factor prime.

The trailing coefficient of a nonzero polynomial $q(d) \in \mathbb{Z}_{p^r}[d]$ is defined as the coefficient of the smallest power of d in $q(d)$. Consider the multiplicative closed subset of $\mathbb{Z}_{p^r}[d]$

$$S = \{q(d) \in \mathbb{Z}_{p^r}[d] \ : \ \text{the trailing coefficient of } q(d) \text{ is a unit}\}.$$

We denote by $\mathbb{Z}_{p^r}(d)$ the ring of rational functions over $\mathbb{Z}_{p^r}$ defined, see [13], as the localized ring

$$\mathbb{Z}_{p^r}(d) = S^{-1}\mathbb{Z}_{p^r}[d] = \left\{ \frac{p(d)}{q(d)} : p(d) \in \mathbb{Z}_{p^r}[d],\ q(d) \in S \right\}.$$

Since S has no zero divisors the localization $S^{-1}\mathbb{Z}_{p^r}[d]$ is the set of equivalent classes in the equivalence relation

$$\frac{p(d)}{q(d)} \sim \frac{p_1(d)}{q_1(d)} \text{ if and only if } p(d)q_1(d) = p_1(d)q(d).$$

Any element $a \in \mathbb{Z}_{p^r}$ has a p-adic expansion [2], i.e., it can be written uniquely as a linear combination of $1, p, p^2, \dots \dots, p^{r-1}$, with coefficients in $\mathcal{A}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$,

$$a = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1}p^{r-1},\ \ \alpha_i \in \mathcal{A}_p,\ \ i = 0, 1, \dots, r-1.$$

Note that all elements in $\mathcal{A}_p \backslash \{0\}$ are units. Given a matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{s\times t}$, denote by $[A(d)]_p$ or $\bar{A}(d)$ its (componentwise) projection over $\mathbb{Z}_p$.

Definition 2.1. *A polynomial matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{s\times t}$ is right factor-prime (rFP) if in all factorizations*

$$A(d) = \bar{A}(d)\Delta(d) \text{ with } \Delta(d) \in \mathbb{Z}_{p^r}[d]^{t\times t} \text{ and } \bar{A}(d) \in \mathbb{Z}_{p^r}[d]^{s\times t},$$

the right factor $\Delta(d)$ is unimodular, that is, it has a polynomial inverse or, equivalently, its determinant is a unit in $\mathbb{Z}_{p^r}$.

Definition 2.2. *A polynomial matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{s\times t}$, with $s > t$, is right zero-prime (rZP) if the ideal generated by all the t-th order minors of $A(d)$ is $\mathbb{Z}_{p^r}[d]$.*

Left factor-prime (rFP) and left zero-prime (rZP) matrices are defined in the same way, upon taking transposes. It can be shown that factor-primeness does not imply zero-primeness but the converse is true [31]. For the purpose of this paper we only need the characterization of zero prime polynomial matrices over $\mathbb{Z}_{p^r}$, see [31, Theorem 2.3].

Theorem 2.1. *Let $A(d) \in \mathbb{Z}_{p^r}[d]^{s\times t}$. The following are equivalent:*

1. *$A(d)$ is right zero-prime;*
2. *there exists a unimodular matrix $V(d) \in \mathbb{Z}_{p^r}[d]^{s\times s}$ such that $V(d)A(d) = \begin{bmatrix} I_t \\ 0 \end{bmatrix}$;*
3. *$A(d)$ admits a polynomial left inverse;*
4. *$\bar{A}(\alpha)$ has rank t, mod p, for all $\alpha \in \bar{\mathbb{Z}}_p$, where $\bar{\mathbb{Z}}_p$ denotes the algebraic closure of $\mathbb{Z}_p$;*
5. *$[A(d)]_p$ is right prime over $\mathbb{Z}_p$.*

We next present a new result in the context of $\mathbb{Z}_{p^r}$ that will be needed in Section 3.

Theorem 2.2. *Let $X(d) \in \mathbb{Z}_{p^r}[d]^{s\times t}$ be right zero-prime and $Y(d) \in \mathbb{Z}_{p^r}[d]^{(s-t)\times s}$ left zero-prime such that $Y(d)X(d) = 0$. The complementary full size minors* [2] *of $X(d)$ and $Y(d)$ are equal up to the multiplication by a unit of $\mathbb{Z}_{p^r}$.*

Proof: Write $X(d) = \begin{bmatrix} X_{L_{s-t}}(d) \\ X_{L_t}(d) \end{bmatrix}$ where $X_{L_{s-t}}(d)$ corresponds to the first $s-t$ rows of $X(d)$ and $X_{L_t}(d)$ to the last t rows and $Y(d) = \begin{bmatrix} Y_{C_{s-t}}(d) & Y_{C_t}(d) \end{bmatrix}$ where $Y_{C_{s-t}}(d)$ and $Y_{C_t}(d)$ are formed by the first $s-t$ and last t columns of $Y(d)$ respectively. Consider the two full size complementary minors of $X(d)$ and $Y(d)$: $\det(X_{L_t}(d))$ and $\det(Y_{C_{s-t}}(d))$ respectively.

As $X(d)$ is right zero-prime there exists, by Theorem 2.1, $\tilde{X}(d) \in \mathbb{Z}_{p^r}[d]^{t\times s}$ such that $\tilde{X}(d)X(d) = I_t$. As by assumption $Y(d)X(d) = 0$, we have that for some matrix $Z(d) \in \mathbb{Z}_{p^r}[d]^{t\times(s-t)}$ it holds that:

$$\begin{bmatrix} Y_{C_{s-t}}(d) & 0 \\ Z(d) & I_t \end{bmatrix} = \begin{bmatrix} Y(d) \\ \tilde{X}(d) \end{bmatrix} \begin{bmatrix} I_{s-t} & X_{L_{s-t}}(d) \\ 0 & X_{L_t}(d) \end{bmatrix}.$$

It follows that

$$\det(Y_{C_{s-t}}(d)) = r(d)\det(X_{L_t}(d)) \tag{2}$$

for some $r(d) \in \mathbb{Z}_{p^r}[d]$.

On the other hand, as $Y(d)$ is a left zero-prime matrix, there exists, by Theorem 2.1, $\tilde{Y}(d) \in \mathbb{Z}_{p^r}[d]^{s\times(s-t)}$ such that $Y(d)\tilde{Y}(d) = I_{s-t}$. Taking into account that $Y(d)X(d) = 0$ we obtain

$$\begin{bmatrix} I_{s-t} & 0 \\ B(d) & X_{L_t}(d) \end{bmatrix} = \begin{bmatrix} Y_{C_{s-t}}(d) & Y_{C_t}(d) \\ 0 & I_t \end{bmatrix} \begin{bmatrix} \tilde{Y}(d) & X(d) \end{bmatrix},$$

for some matrix $B(d) \in \mathbb{Z}_{p^r}[d]^{t\times(s-t)}$. Thus $\det(X_{L_t}(d)) = s(d)\det(Y_{C_{s-t}}(d))$ for some $s(d) \in \mathbb{Z}_{p^r}[d]$ and according to (2),

$$\det(X_{L_t}(d)) = s(d)r(d)\det(X_{L_t}(d)),$$

that is, $r(d)$ and $s(d)$ are units of $\mathbb{Z}_{p^r}[d]$. We obtain this for any complementary full size order minors by permutation of rows/columns of $X(d)$ e $Y(d)$. □

2.2. Linear systems

We next present the property of reachability of linear systems over $\mathbb{Z}_{p^r}$ and its characterization.

Definition 2.3. *A system $\sum = (A,\, B,\, C,\, D)$ is said to be reachable if for every given state $x \in \mathbb{Z}_{p^r}^{\ell}$ of the system there exist a finite sequence of inputs $u_0,\, u_1 \ldots u_\theta \in \mathbb{Z}_{p^r}^{k}$, $\theta \in \mathbb{N}_0$, that drives the system from the initial state $x_0 = 0$ to $x_\theta = x$.*

Theorem 2.3. *Let $\sum = (A,\, B,\, C,\, D)$ be a linear system of dimension ℓ over $\mathbb{Z}_{p^r}$. The following statements are equivalent:*

1. *$\sum$ is reachable;*
2. *The rows of the matrix $\begin{bmatrix} B \\ BA \\ \vdots \\ BA^{\ell-1} \end{bmatrix}$ generate $\mathbb{Z}_{p^r}^{\ell}$ (over $\mathbb{Z}_{p^r}$);*

[2] Let $x(d)$ be the full t-size minor of the matrix $X(d)$ corresponding to the submatrix $X(d)$ formed by the rows with indices $i_1, i_2, \ldots, i_t$ and $y(d)$ the full $(s-t)$-size minor of the matrix $Y(d)$ corresponding to the submatrix of $Y(d)$ formed by the columns with indices $j_1, j_2, \ldots, j_{s-t}$. We say that $x(d)$ and $y(d)$ are *complementary minors* if $\{i_1, i_2, \ldots, i_t\} \cap \{j_1, j_2, \ldots, j_{s-t}\} = \emptyset$ (note that $\{i_1, i_2, \ldots, i_t\} \cup \{j_1, j_2, \ldots, j_{s-t}\} = \{1, 2, \ldots, s\}$).

3. *The ideal generated by the minors of order ℓ of the matrix* $\begin{bmatrix} I_\ell d - A \\ -B \end{bmatrix}$ *is* $\mathbb{Z}_{p^r}$*;*
4. *The matrix* $\begin{bmatrix} I_\ell d - A \\ -B \end{bmatrix}$ *is right-zero prime.*

The equivalence of the first three statements was proven in [1] and the last statement, commonly known by the *PBH test* (Popov-Belevitch-Hautus [15]) was recently shown in [31].

Given a sequence of inputs $u(d)$ and the corresponding sequence of states $x(d)$, the system $\sum = (A,\, B,\, C,\, D)$ generates the output sequence $y(d)$. The triple $(x(d),\, u(d),\, y(d)) \in \mathbb{Z}_{p^r}[[d]]^l \times \mathbb{Z}_{p^r}[[d]]^k \times \mathbb{Z}_{p^r}[[d]]^{(n-k)}$ is called a trajectory of the system. From the first equation of (1) it follows that

$$\sum_{t\in\mathbb{N}_0} x_{t+1}d^t = \sum_{t\in\mathbb{N}_0} x_t d^t A + \sum_{t\in\mathbb{N}_0} u_t d^t B$$

and, as we have that $x_0 = 0$ then

$$x(d)d^{-1} = x(d)A + u(d)B,$$

which is equivalent to

$$x(d) = u(d)Bd(I_\ell - Ad)^{-1}.$$

From the second equation of (1) we obtain the input-output relation

$$y(d) = u(d)\left[Bd\,(I_\ell - Ad)^{-1}\,C + D\right].$$

The rational matrix $T(d) = D + \left[Bd\,(I_\ell - Ad)^{-1}\,C\right]$ is called the transfer matrix of the system $\sum = (A,\, B,\, C,\, D)$ and we say that $\sum = (A,\, B,\, C,\, D)$ is a realization of $T(d)$. A rational matrix that admits a realization is said to be realizable. Observe that a realizable rational matrix admits several realizations.

2.3. Rational matrices over $\mathbb{Z}_{p^r}$

Next, we study rational matrices over $\mathbb{Z}_{p^r}$ and address the realization problem of these matrices. We consider left matrix fraction description of a rational matrix and introduce the novel notion of irreducible left matrix fraction description. We also give an algorithm that provides a realization of a realizable rational matrix.

As explained above rational functions can be represented by the quotient of two polynomials $\dfrac{p(d)}{q(d)}$, where $p(d),\, q(d) \in \mathbb{Z}_{p^r}[d]$ and the coefficient of the smallest power of d in $q(d)$ is a unit of $\mathbb{Z}_{p^r}$. Analogously, a rational matrix $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ can be described as the "quotient" of two polynomial matrices. Let $N(d) \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}$ and $J(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ be an invertible matrix such that the coefficient of the smallest degree of $\det(J(d)) \in \mathbb{Z}_{p^r}[d]$ is a unit of $\mathbb{Z}_{p^r}$. We say that $J^{-1}(d)N(d)$ is a *left matrix fractional representation* (ℓMFD) of $T(d)$, if $T(d) = J^{-1}(d)N(d)$.

Obviously $T(d) = \begin{bmatrix} \dfrac{p_{ij}(d)}{q_{ij}(d)} \end{bmatrix} \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ always admit a ℓMFD. Indeed, consider $q(d) = \prod_{\substack{i=1,\dots,k \\ j=1,\dots,n-k}} q_{ij}(d)$ and $T(d) = J^{-1}(d)N(d)$, for

$$J(d) = \begin{bmatrix} q(d) & & \\ & \ddots & \\ & & q(d) \end{bmatrix} \in \mathbb{Z}_{p^r}[d]^{k\times k} \quad \text{and} \quad N(d) = \begin{bmatrix} \dfrac{p_{ij}(d)q(d)}{q_{ij}(d)} \end{bmatrix} \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}.$$

We say that a ℓMFD $J^{-1}(d)N(d)$ of $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ is *irreducible* if the polynomial matrix $\begin{bmatrix} J(d) & N(d) \end{bmatrix}$ is left factor prime. There exist rational matrices that admit an irreducible ℓMFD $J^{-1}(d)N(d)$ such that $\begin{bmatrix} J(d) & N(d) \end{bmatrix}$ is left zero-prime. In this case, all irreducible ℓMFD have the same properties, as we show in the following theorem.

Theorem 2.4. *Let $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ and $J_1^{-1}(d)N_1(d)$ e $J_2^{-1}(d)N_2(d)$ be two irreducible ℓMFD of $T(d)$. If $\begin{bmatrix} J_1(d) & N_1(d) \end{bmatrix}$ is left zero-prime then $\begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix}$ is left zero prime. Moreover,*

$$\begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix} = U(d) \begin{bmatrix} J_1(d) & N_1(d) \end{bmatrix}$$

for some unimodular matrix $U(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$.

Proof: As $T(d) = J_1^{-1}(d)N_1(d) = J_2^{-1}(d)N_2(d)$ then

$$J_1^{-1}(d) \begin{bmatrix} J_1(d) & N_1(d) \end{bmatrix} = J_2^{-1}(d) \begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix}$$

and therefore

$$J_2(d)J_1^{-1}(d) \begin{bmatrix} J_1(d) & N_1(d) \end{bmatrix} = \begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix}. \quad (3)$$

Thus, $\begin{bmatrix} J_1(d) & N_1(d) \end{bmatrix}$ is left zero prime and $\begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix}$ is a polynomial matrix and so according to Theorem 2.1 the matrix $J_2(d)J_1^{-1}(d)$ is also polynomial. On the other hand $\begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix}$ is left factor-prime, since $J_2^{-1}(d)N_2(d)$ is irreducible. By (3) it follows that $J_2(d)J_1^{-1}(d)$ is unimodular and then $\begin{bmatrix} J_2(d) & N_2(d) \end{bmatrix}$ is left zero-prime. □

However, not all rational matrices admit this type of representation as we illustrate in the next example.

Example 2.1. *The fractional representation $t(d) = \dfrac{1+4d}{1+d} \in \mathbb{Z}_9(d)$ is irreducible as the matrix $\begin{bmatrix} 1+d & 1+4d \end{bmatrix}$ is left factor-prime. However, it is not left zero-prime because $[1+d \;\; 1+4d]_3 = (1+d)[1 \;\; 1] \mod 3$ and therefore by Theorem 2.4, $t(d)$ does not admit a fractional representation $\dfrac{p(d)}{q(d)}$, where $\begin{bmatrix} p(d) & q(d) \end{bmatrix}$ is a left zero-prime matrix.*

As defined in the last section, a realizable matrix is a rational matrix that is the transfer matrix of a linear system. Thus, these matrices establish a causal relation between inputs and outputs. The next result characterizes the rational functions that are realizable by means of ℓMFD.

Proposition 2.1. *[13] Let $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ and $J^{-1}(d)N(d)$ a ℓMFD of $T(d)$. The matrix $T(d)$ is realizable if and only if $J(0)$ is invertible.*

Next we present an algorithm that gives the realization of a realizable matrix $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ that admits a ℓMFD $J^{-1}(d)N(d)$ where $J(0)$ is invertible. Similar algorithms in the context of finite fields were first presented in [9] and later on in [11]. The proof that the algorithm actually provides a realization of $T(d)$ is very analogous to the one given for fields and therefore we omit its proof.

Algorithm 1
Input data: $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$.

Step 1: Consider $J(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ and $N(d) \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}$ such that $T(d) = J^{-1}(d)N(d)$ where $J(0)$ is invertible.

Step 2: Rewrite $T(d)$ of the form

$$T(d) = J^{-1}(0)N(0) + J^{-1}(d)\hat{N}(d),$$

with $\hat{N}(d) = N(d) - J(d)J^{-1}(0)N(0)$.

Step 3: Define $D = J^{-1}(0)N(0)$.

Step 4: Denote by ν_1, ν_2, … ν_k the degrees of the rows 1, 2, …, k of the matrix $\left[\begin{array}{cc} J(d) & \hat{N}(d) \end{array}\right]$. Consider that for $i = 1, 2, \ldots, k$, $\nu_i > 0$ and $\ell = \sum_{i=1}^{k} \nu_i$. For $i = 1, 2, \ldots, k$ consider the nilpotent Jordan block $\nu_i \times \nu_i$:

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

Step 5: Define the matrix

$$\tilde{A} = \mathrm{diag}\{A_1, A_2, \ldots, A_k\}. \qquad (4)$$

Step 6: Define the matrix

$$\tilde{B} = \begin{bmatrix} e_1 \\ e_{\nu_1+1} \\ e_{\nu_1+\nu_2+1} \\ \vdots \\ \vdots \\ e_{\nu_1+\nu_2+\cdots+\nu_{k-1}+1} \end{bmatrix}, \qquad (5)$$

where e_i, $i = 1, \ldots, \nu_1 + \nu_2 + \cdots + \nu_{k-1} + 1$ is the $i - th$ canonical vector of $\mathbb{Z}_{p^r}^{\ell}$.

Step 7: Define the matrix $C \in \mathbb{Z}_{p^r}^{\ell \times m}$ where $m = \nu_1 + \nu_2 + \cdots + \nu_k$ such that $\hat{N}(d) = \Psi(d)C$ and

$$\Psi(d) \;=\; \begin{bmatrix} d & \cdots & d^{\nu_1} & & & & & & \\ & & & d & \cdots & d^{\nu_2} & & & \\ & & & & & & \ddots & & \\ & & & & & & d & \cdots & d^{\nu_k} \end{bmatrix}.$$

Step 8: Define the matrix

$$B = J^{-1}(0)\tilde{B}.$$

Step 9: Define the matrix

$$A = \tilde{A} + \bar{A}\tilde{B},$$

where $\bar{A} \in \mathbb{Z}_{p^r}^{\ell \times k}$ with $\ell = \nu_1 + \nu_2, \cdots + \nu_k$ is such that $J(d) = (I_k - \Psi(d)\bar{A})J(0)$.

Output: $\sum = (A, B, C, D)$.

Remark 2.1. *In case $\nu_i = 0$ for some i, the procedure is the same as above, however the i-th row in $\tilde{B}$ and in $\Psi(d)$ has to be zero, and the i-th diagonal block A_i is empty.*

Lemma 2.1. *The matrix $\begin{bmatrix} I_s d - \tilde{A} \\ -\tilde{B} \end{bmatrix}$, where $\tilde{A}$ and $\tilde{B}$ are the matrices defined in (4) and (5) and $s = \nu_1 + \nu_2 + \ldots + \nu_k$, is left zero-prime over $\mathbb{Z}_{p^r}[d]$.*

Proof: For all $d \in \mathbb{Z}_{p^r} \backslash \{0\}$, $\begin{bmatrix} I_s d - \tilde{A} \\ -\tilde{B} \end{bmatrix}$ has full column rank with rank equal to $s = \nu_1 + \nu_2 + \ldots + \nu_k$ where ν_i, $i = 1, \ldots, k$ is defined in Step 4 of the algorithm. We observe that the same holds for $d = 0$, as $\begin{bmatrix} -\tilde{A} \\ -\tilde{B} \end{bmatrix}$ is full column rank. □

Although the next result follows the same reasoning of the counterpart result for finite fields, we opt to present its short proof as it is new in this context.

Theorem 2.5. *Let $T(d) = J(d)^{-1}N(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ with $J(0)$ invertible and $N(d) \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}$. Every realization of $T(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ by means of the algorithm given above is reachable.*

Proof: Let $\sum = (A,\, B,\, C,\, D)$ be a realization given by Algorithm 1, $T(d) = D + Bd(I - Ad)^{-1}C$. As $A = \tilde{A} + \bar{A}\tilde{B}$ and $B = J^{-1}(0)\tilde{B}$ it follows that $I_s d - A = I_s d - \tilde{A} - \bar{A}\tilde{B}$ where $s = \nu_1 + \nu_2 + \ldots + \nu_k$. Further,

$$\begin{bmatrix} I_s d - A \\ -B \end{bmatrix} = \begin{bmatrix} I_s & \bar{A} \\ 0 & J^{-1}(0) \end{bmatrix} \begin{bmatrix} I_s d - \tilde{A} \\ -\tilde{B} \end{bmatrix}.$$

Now observe that $\begin{bmatrix} I_s & \bar{A} \\ 0 & J^{-1}(0) \end{bmatrix}_p$ is invertible over $\mathbb{Z}_p$, i.e., $\begin{bmatrix} I_s & \bar{A} \\ 0 & J^{-1}(0) \end{bmatrix}$ is invertible over $\mathbb{Z}_{p^r}$. By Lemma 2.1, $\begin{bmatrix} I_s d - \tilde{A} \\ -\tilde{B} \end{bmatrix}$ is right zero-prime . This implies that $\begin{bmatrix} I_s d - A \\ -B \end{bmatrix}$is right zero-prime and therefore $(A,\, B,\, C,\, D)$ is a reachable realization of $T(d)$ according to Lemma 2.3. □

3. State representations of finite support convolutional codes over $\mathbb{Z}_{p^r}$

We consider convolutional codes described by the input-state-output representations as in (1) where the codewords are the finite-support input-output trajectories $v(d) = \begin{bmatrix} u(d) & y(d) \end{bmatrix}$ of the system. Moreover, for a finite-support input-output trajectory to be a codeword it is required that the corresponding state sequence has also finite support in order to avoid having the corresponding state vector infinitely excited. This leads to the following definition.

Definition 3.1. *[36, Definition 2.3] A trajectory $(x(d),\, u(d),\, y(d)) \in \mathbb{Z}_{p^r}[[d]]^{\ell} \times \mathbb{Z}_{p^r}[[d]]^{k} \times \mathbb{Z}_{p^r}[[d]]^{n-k}$ of a system $\sum = (A,\, B,\, C,\, D)$ is a finite-weight codeword if $x(d)$, $u(d)$ e $y(d)$ are polynomial vectors. Under these conditions the pair $(u(d),\, y(d))$ is called finite-weight input-output trajectory and $(x(d),\, u(d),\, y(d))$ a finite-weight trajectory.*

As explained above, one can use the linear system (1) description

$$\left\{ \begin{array}{rcl} x(d) & = & x(d)Ad + u(d)Bd \\ y(d) & = & x(d)C + u(d)D \end{array} \right.$$

or equivalently

$$\left\{ \begin{array}{lcl} (I_\ell - Ad)x(d) - u(d)Bd & = & 0 \\ y(d) - x(d)C - u(d)D & = & 0 \end{array} \right. . \tag{6}$$

In this way we obtain the matrix

$$X(d) = \left[\begin{array}{cc} I_\ell - Ad & -C \\ -Bd & -D \\ 0 & I_{n-k} \end{array} \right] \tag{7}$$

and $[x(d)\ u(d)\ y(d)]$ is a trajectory of the system if and only if $\left[\begin{array}{ccc} x(d) & u(d) & y(d) \end{array} \right] X(d) = 0$. That is, the set of trajectories of $(A,\ B,\ C,\ D)$ coincides with the kernel of $X(d)$.

Before showing that the set of input-output finite-weight trajectory of a linear system is a convolutional code over $\mathbb{Z}_{p^r}$ we need the following lemma.

Lemma 3.1. *Let* $\sum$=$(A,\ B,\ C,\ D)$ *be a reachable system. The matrix* $X(d) = \left[\begin{array}{cc} I_\ell - Ad & -C \\ -Bd & -D \\ 0 & I_{n-k} \end{array} \right]$ *defined in (7) is right zero-prime .*

Proof: It is easy to check that if $\left[\begin{array}{c} I_\ell d - A \\ -B \end{array} \right]$ is right zero prime then $\left[\begin{array}{c} I_\ell - Ad \\ -Bd \end{array} \right]$ is right zero prime. Thus, since Σ is reachable, the matrix $\left[\begin{array}{c} I_\ell - Ad \\ -Bd \end{array} \right]$ is right zero-prime and so admits a polynomial left inverse. Let $\left[\begin{array}{cc} U(d) & V(d) \end{array} \right]$ be such inverse. Then, the matrix $\left[\begin{array}{ccc} U(d) & V(d) & U(d)C + V(d)D \\ 0 & 0 & I_{n-k} \end{array} \right]$, is the polynomial left inverse matrix of $X(d)$ and therefore $X(d)$ is right zero-prime . □

Theorem 3.1. *The set of finite-weight input-output trajectories of a reachable linear system* $\sum = (A,\ B,\ C,\ D)$ *is a free convolutional code over* $\mathbb{Z}_{p^r}$ *of rate* k/n.

Proof: By Lemma 3.1 the matrix $X(d) = \left[\begin{array}{cc} I_\ell - Ad & -C \\ -Bd & -D \\ 0 & I_{n-k} \end{array} \right]$ is right zero-prime . Further by Theorem 2.1 $X(d)$ admits a unimodular extension, that is, there exists a matrix $Y(d) \in \mathbb{Z}_{p^r}[d]^{(\ell+n)\times k}$ such that $\left[\begin{array}{cc} X(d) & Y(d) \end{array} \right]$ is unimodular. Let $U(d) = \left[\begin{array}{cc} L_0(d) & G_0(d) \\ L(d) & G(d) \end{array} \right]$ be an inverse of $\left[\begin{array}{cc} X(d) & Y(d) \end{array} \right]$ where $L_0(d) \in \mathbb{Z}_{p^r}[d]^{(\ell+n-k)\times \ell}$, $G_0(d) \in \mathbb{Z}_{p^r}[d]^{(\ell+n-k)\times n}$, $L(d) \in \mathbb{Z}_{p^r}[d]^{k\times \ell}$ and $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$. Then, we have that

$$U(d) \left[\begin{array}{cc} X(d) & Y(d) \end{array} \right] = I_{\ell+n} \tag{8}$$

$$\left[\begin{array}{cc} X(d) & Y(d) \end{array} \right] U(d) = I_{\ell+n}. \tag{9}$$

Further, $\mathrm{Im}_{\mathbb{Z}_{p^r}[[d]]} \left[\begin{array}{cc} L(d) & G(d) \end{array} \right]$ coincides with the kernel of $X(d)$. According to (8) we have that $\left[\begin{array}{cc} L(d) & G(d) \end{array} \right] X(d) = 0$, i.e.,

$$\mathrm{Im}_{\mathbb{Z}_{p^r}[[d]]} \left[\begin{array}{cc} L(d) & G(d) \end{array} \right] \subseteq \ker_{\mathbb{Z}_{p^r}[[d]]}(X(d)).$$

For the converse consider a vector of $\ker_{\mathbb{Z}_{p^r}[[d]]}(X(d))$, that is a vector $s(d) \in \mathbb{Z}_{p^r}[[d]]^{\ell+n}$ such that

$s(d)X(d) = 0$. By (9) we have that

$$s(d)I_{\ell+n} = s(d)\left[\begin{array}{cc} X(d) & Y(d) \end{array}\right]U(d) = \left[\begin{array}{cc} 0 & s(d)Y(d) \end{array}\right]\left[\begin{array}{cc} L_0(d) & G_0(d) \\ L(d) & G(d) \end{array}\right].$$

Then, $s(d) = t(d)\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ with $t(d) = s(d)Y(d) \in \mathbb{Z}_{p^r}[[d]]^k$ and then $s(d) \in \mathrm{Im}_{\mathbb{Z}_{p^r}[[d]]}\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$. Therefore $\mathrm{Im}_{\mathbb{Z}_{p^r}[[d]]}\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] = \ker_{\mathbb{Z}_{p^r}[[d]]}(X(d))$.

As $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ is formed by rows of the unimodular matrix $U(d)$, then $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ is left zero-prime. Thus, by Theorem 2.1, the set of finite-weight trajectories of the system $\sum = (A,\, B,\, C,\, D)$, $\ker_{\mathbb{Z}_{p^r}[[d]]} X(d) \cap \mathbb{Z}_{p^r}[d]^{\ell+n}$ is given by

$$\begin{aligned} \mathrm{Im}_{\mathbb{Z}_{p^r}[[d]]}\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] \cap \mathbb{Z}_{p^r}[d]^{\ell+n} &= \mathrm{Im}_{\mathbb{Z}_{p^r}(d)}\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] \cap \mathbb{Z}_{p^r}[d]^{\ell+n} \\ &= \mathrm{Im}_{\mathbb{Z}_{p^r}[d]}\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]. \end{aligned}$$

In this way, for every finite-weight trajectory of $\sum = (A,\, B,\, C,\, D)$, $(x(d),\, u(d),\, y(d))$ where $x(d) \in \mathbb{Z}_{p^r}[d]^\ell$, $u(d) \in \mathbb{Z}_{p^r}[d]^k$ and $y(d) \in \mathbb{Z}_{p^r}[d]^{(n-k)}$ there exists an $r(d) \in \mathbb{Z}_{p^r}[d]^k$ such that

$$(x(d),\, u(d),\, y(d)) = r(d)\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$$

and therefore $(u(d),\, y(d)) = r(d)G(d)$. Then, $\mathrm{Im}_{\mathbb{Z}_{p^r}[d]}G(d)$ coincides with the set of finite-weight input-output trajectories of $\sum = (A,\, B,\, C,\, D)$ and $G(d)$ is a generator matrix of this set. It remains to show that $G(d)$ is full row rank. For the left zero-prime matrix $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ of size $k \times (\ell + n)$ and the right zero-prime matrix $X(d)$ of size $(\ell + n) \times (\ell + n - k)$ we have that $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]X(d) = 0$. Let $\tilde{G}(d)$ be the matrix that is obtained from $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ deleting the first ℓ and last $n - k$ columns. From Theorem 2.2 we have that

$$\det(\tilde{G}(d)) = \alpha \det\left(\left[\begin{array}{cc} I_\ell - Ad & -C \\ 0 & I_{n-k} \end{array}\right]\right),$$

with α a unit of $\mathbb{Z}_{p^r}$. Finally, since $\det\left(\left[\begin{array}{cc} I_\ell - Ad & -C \\ 0 & I_{n-k} \end{array}\right]_p\right) \neq 0$ then $\det([\tilde{G}(d)]_p) \neq 0$ and therefore $\mathrm{rank}(G(d)) = k$. □

We denote by $\mathcal{C}(A,\, B,\, C,\, D)$ the convolutional code constituted by the finite-weight input-output trajectories of a reachable system $\sum = (A,\, B,\, C,\, D)$. We denote $\sum$ an input-state-output representation of $\mathcal{C} = \mathcal{C}(A,\, B,\, C,\, D)$.

Theorem 3.2. *Let $\mathcal{C}$ be a convolutional code with complexity δ with input-state-output representation $\sum = (A,\, B,\, C,\, D)$ that is reachable and with dimension ℓ. Then, $\ell \geq \delta$.*

Proof: Take the right zero-prime matrix $X(d) = \left[\begin{array}{cc} I_\ell - Ad & -C \\ -Bd & -D \\ 0 & I_{n-k} \end{array}\right]$ and the matrices $L(d) \in \mathbb{Z}_{p^r}[d]^{k\times\ell}$ and $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ such that

$$\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]X(d) = 0,$$

with $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ a left zero-prime matrix and $G(d)$ a generator matrix of $\mathcal{C}$, as shown in the proof of Theorem 3.1. Note that the full size minors of $X(d)$ have degree less than or equal to ℓ since the first ℓ columns of $X(d)$ have degree less than or equal to 1 and the remaining have degree zero. As

$\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] X(d) = 0$ then $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ is left zero-prime and $X(d)$ is right zero-prime and, by Theorem 2.2, the full size minors of $G(d)$ coincide with the full size minors of $X(d)$ up to the multiplication of a unit in $\mathbb{Z}_{p^r}$. Thus, the complexity of $G(d)$ is less than or equal to ℓ. □

A catastrophic generator matrix $G(d)$ is a generator matrix for which there exists a sequence $u(d) \in \mathbb{F}(d)^k$ of infinite support such that $w(d) = u(d)G(d) \in \mathbb{F}(d)^n$ has finite support, i.e., it is polynomial. It was shown in [31] that $G(d)$ is noncatastrophic if and only if $G(d)$ is left zero-prime. Moreover, equivalent generator matrices are full row rank matrices that are generator matrices of the same code. Then, two equivalent generator matrices, $G_1(d), G_2(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$, are such that $G_2(d) = U(d)G_1(d)$, for some unimodular matrix $U(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$. Thus, it follows that if a convolutional code admits a left zero-prime generator matrix then all its generator matrices are also left zero-prime. We call such codes *noncatastrophic* codes. Next we present a characterization of the state reachable representations of noncatastrophic codes.

Theorem 3.3. *Let $\sum = (A,\, B,\, C,\, D)$ be a reachable system of dimension ℓ. The convolutional code $\mathcal{C}(A,\, B,\, C,\, D)$ is noncatastrophic if and only if $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right]$ is left zero-prime.*

Proof: As $\sum$ is reachable the matrix $X(d) = \left[\begin{array}{cc} I_\ell - Ad & -C \\ -Bd & -D \\ 0 & I_{n-k} \end{array}\right]$ is right zero-prime and there exist matrices $L(d) \in \mathbb{Z}_{p^r}[d]^{k\times \ell}$ and $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ such that $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] X(d) = 0$, where $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ is left zero-prime and $G(d)$ is a generator matrix of $\mathcal{C}(A,\, B,\, C,\, D)$. Suppose that $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right]$ is left zero-prime. If $\mathcal{C}(A,\, B,\, C,\, D)$ is catastrophic $G(d)$ is not left zero-prime or equivalently, there exists $u(d) \in \mathbb{Z}_{p^r}(d)$ not polynomial such that $u(d)G(d)$ is polynomial. From $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] X(d) = 0$ it follows that

$$u(d)\left[\begin{array}{cc} L(d) & G(d) \end{array}\right] X(d) = 0.$$

Further,

$$u(d)L(d)\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right] = -u(d)G(d)\left[\begin{array}{cc} -Bd & D \\ 0 & I_{n-k} \end{array}\right].$$

Since $-u(d)G(d)\left[\begin{array}{cc} -Bd & D \\ 0 & I_{n-k} \end{array}\right]$ is polynomial and $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right]$ is a left zero-prime matrix we conclude that $u(d)L(d)$ is polynomial and therefore $u(d)\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ is also polynomial which contradicts that $\left[\begin{array}{cc} L(d) & G(d) \end{array}\right]$ is left zero-prime and $u(d) \in \mathbb{Z}_{p^r}(d)$ is not a polynomial. Thus, $\mathcal{C}(A,\, B,\, C,\, D)$ is noncatastrophic.

For the converse suppose that $\left[\begin{array}{cc} I - Ad & -C \end{array}\right]$ is not a left zero-prime matrix. Then, by Theorem 2.2, the minors of order ℓ of $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right]$ admit a common factor, say $q(d)$, that is not a unit in $\mathbb{Z}_{p^r}[d]$. Then, $q(d)$ is also a common factor of the minors of order $n-k+\ell$ of $X(d)$ with respect to the matrices that admit $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right]$ as submatrices. Consequently, according to Theorem 2.2 $q(d)$ is a common factor of the minors of order k of $G(d)$. Thus, $G(d)$ is not a left zero-prime matrix and therefore $\mathcal{C}(A,\, B,\, C,\, D)$ is catastrophic. Thus, we conclude that if $\mathcal{C}(A,\, B,\, C,\, D)$ is noncatastrophic then $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array}\right]$ is left zero-prime. □

From this theorem it follows that if $\sum = (A,\, B,\, C,\, D)$ is a reachable state representation of a noncatastrophic convolutional code $\mathcal{C}$ then the codewords of $\mathcal{C}$ are the polynomial input-output trajectories of Σ. Next, we show how to obtain an ISO representation of a noncatastrophic convolutional code.

Consider $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ a generator matriz of a noncatastrophic convolutional code $\mathcal{C}$. As $G(d)$ is left zero-prime, $G(d)$ admits a polynomial right inverse and therefore $G(0)$ has full row rank. Write

$$G(d) = \left[\begin{array}{cc} J(d) & N(d) \end{array} \right],$$

where $J(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$, $N(d) \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}$ and $J(0)$ is an invertible matrix. Observe that by a permutation of columns of $G(d)$ it is always possible obtain a matrix with these conditions.

Theorem 3.4. *Let $\mathcal{C}$ be a noncatastrophic convolutional code and $G(d)$ a generator matrix of $\mathcal{C}$ such that*

$$G(d) = \left[\begin{array}{cc} J(d) & N(d) \end{array} \right],$$

where $J(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$, $N(d) \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}$ and $J(0)$ an invertible matrix. Consider $T(d) = J^{-1}(d)N(d)$ and $\sum = (A,\, B,\, C,\, D)$ a realization of $T(d)$. If $\sum$ is a reachable realization of $T(d)$ such that $\left[\begin{array}{cc} I_\ell - Ad & -C \end{array} \right]$ is a left zero-prime matrix then $\sum$ is an ISO representation of $\mathcal{C}$.

Proof: Note that if $(u(d), y(d))$ is an finite-weight input-output trajectory of $\sum$ then $y(d) = u(d)T(d)$. Thus, $y(d) = u(d)J^{-1}(d)N(d)$. Considering $v(d) = u(d)J^{-1}(d)$ we obtain that

$$\left[\begin{array}{cc} u(d) & y(d) \end{array} \right] = v(d) \left[\begin{array}{cc} J(d) & N(d) \end{array} \right] = v(d)G(d),$$

for some $v(d) \in \mathbb{Z}_{p^r}[[d]]^k$. Since $G(d)$ is left zero-prime it follows that $v(d) \in \mathbb{Z}_{p^r}[d]^k$. In this way we conclude that the input-output polynomial trajectories of $\sum$ are codewords of $\mathcal{C}$. We now check that $\sum$ is an ISO representation of $G(d)$, that is, the input-output trajectories of $\sum$ that are polynomials coincide with the finite-weight input-output trajectories of $\sum$. To this end we consider $(u(d), y(d))$ a polynomial input-output trajectory of $\sum$ and $x(d) \in \mathbb{Z}_{p^r}[[d]]^\ell$ the corresponding state. It follows that

$$\left[\begin{array}{ccc} x(d) & u(d) & y(d) \end{array} \right] \left[\begin{array}{cc} I_\ell - Ad & -C \\ -Bd & -D \\ 0 & I_{n-k} \end{array} \right] = 0$$

is equivalent to

$$x(d) \left[\begin{array}{cc} I_\ell - Ad & -C \end{array} \right] = - \left[\begin{array}{cc} u(d) & y(d) \end{array} \right] \left[\begin{array}{cc} -Bd & D \\ 0 & I_{n-k} \end{array} \right].$$

Hence, since $\left[\begin{array}{cc} u(d) & y(d) \end{array} \right]$ is polynomial it follows that $- \left[\begin{array}{cc} u(d) & y(d) \end{array} \right] \left[\begin{array}{cc} -Bd & D \\ 0 & I_{n-k} \end{array} \right]$ is also polynomial. Then we conclude that $x(d)$ is polynomial because $[I_\ell - Ad \quad - C]$ is left zero prime. Therefore $\sum$ is an ISO representation of $G(d)$. □

Thus, to obtain an ISO representation of a noncatastrophic convolutional code we consider $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ one of its generator matrices. Suppose, without loss of generality, that $G(d) = \left[\begin{array}{cc} J(d) & N(d) \end{array} \right]$ with $J(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$, $N(d) \in \mathbb{Z}_{p^r}(d)^{k\times(n-k)}$ and $J(0)$ an invertible matrix. Let $T(d) = J^{-1}(d)N(d)$ and $\sum = (A,\, B,\, C,\, D)$ a realization of $T(d)$ of dimension ℓ derived from Algorithm 1. $\sum$ is an ISO representation of $\sum$.

Now consider a particular class of noncatastrophic codes: the convolutional codes that admit a generator matrix $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ left zero-prime such that the constant matrix formed by the coefficients of degree equal to the maximum degree of the entries in each row, $[G(d)]_{hc}$, is full row rank. If $\mathcal{C}$ is a convolutional code that admits such generator matrix $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ and Σ is an ISO representation of $\mathcal{C}$ obtained by the methodology described above, then, Σ is an ISO representation of $\mathcal{C}$ of minimal dimension. Indeed, if $[G(d)]_{hc}$ is full row rank then $G(d)$ has complexity equal to the sum of the row degrees of $G(d)$, that is, has complexity equal to the dimension of the system. It follows from Theorem 3.2 that $\sum = (A,\ B,\ C,\ D)$ is a state representation of minimal dimension of the code.

4. Conclusions

A vast number of results of convolutional encoders have been extended from the context of finite fields to the finite ring case. In this work we have extended many fundamental results of input-state-output representations of finite support convolutional codes to the context of the finite ring $\mathbb{Z}_{p^r}$. Notions such as noncatastrophicity, reachability or minimality have been investigated in the work.

References

[1] W. Brewer. *Linear Systems over commutative rings.* Dover Publications Inc., New York, 1986.

[2] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, 6(1):21–35, 1995.

[3] M. Carriegos and M.T. Trobajo. Linear systems over hermite rings. some pole-placement results. *Authorea*, September 11, 2020.

[4] N. DeCastro-García. Feedback equivalence of convolutional codes over finite rings. *Open Mathematics*, 15(1):1495 – 1508, 2017.

[5] N. DeCastro-García and M.I. García-Planas. Concatenated linear systems over rings and their application to construction of concatenated families of convolutional codes. *Linear Algebra and its Applications*, 542:624 – 647, 2018.

[6] N. DeCastro-García, M. V. Carriegos, and A.L. Muñoz Castañeda. A characterization of von Neumann rings in terms of linear systems. *Linear Algebra and its Applications*, 494:236–244, 2016.

[7] F. Fagnani and S. Zampieri. System-theoretic properties of convolutional codes over rings. *IEEE Trans. Inform. Theory*, 47(6):2256–2274, 2001.

[8] F. Fagnani and S. Zampieri. Minimal and systematic convolutional codes over finite Abelian groups. *Linear Algebra and its Applications*, 378:31–59, 2004.

[9] E. Fornasini and R. Pinto. Matrix fraction descriptions in convolutional coding. *Linear Algebra and its Applications*, 392:119 – 158, 2004.

[10] E. Fornasini and M.E. Valcher. Multidimensional systems with finite support behaviors: signal structure, generation and detection. *SIAM Journal on Control and Optimization*, 36(2):760–779, 1998.

[11] H. Gluesing-Luerssen and G. Schneider. State space realizations and monomial equivalence for convolutional codes. *Linear Algebra and its Applications*, 425(2):518 – 533, 2007.

[12] Napp D. Herranz, V. and C. Perea. 1/n turbo codes from linear system point of view. *RACSAM*, 114(118), 2020.

[13] R. Johannesson, Z.X. Wan, and E. Wittenmark. Some structural properties of convolutional codes over rings. *IEEE Trans. Inform. Theory*, 44(2):839–845, 1998.

[14] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding.* IEEE Press, New York, 2015.

[15] T. Kailath. *Linear systems.* Prentice Hall information and system sciences series. Prentice-Hall, Englewood Cliffs, 1980.

[16] M. Kuijper and R. Pinto. Minimal trellis construction for finite support convolutional ring codes. *Lecture Notes in Computer Science*, 5228:95–106, 2008.

[17] M. Kuijper and R. Pinto. On minimality of convolutional ring encoders. *IEEE Trans. Automat. Contr.*, 55)(11):4890 –4897, 2009.

[18] M. Kuijper and R. Pinto. An iterative algorithm for parametrization of shortest length linear shift registers over finite chain rings. *Designs, Codes and Cryptography*, 83(2):283–305, May 2017.

[19] M. Kuijper and R. Pinto. Minimal trellis construction for finite support convolutional ring codes. *In A. Barbero, editor, Coding Theory and Applications (ICMCTA), LN in Computer Science*, 5228:95–106, Springer, 2008.

[20] 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.

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

[22] M. Kuijper and K. Schindelar. Minimal Gröbner bases and the predictable leading monomial property. *Linear Algebra and its Applications*, 434(1):104 – 116, 2011.

[23] M. Kuijper, M. van Dijk, H. Hollmann, and A J. Oostveen. A unifying system-theoretic framework for errors-and-erasures Reed-Solomon decoding. In S. Boztas and I.E. Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, LN in Computer Science 2227, pages 343–352. Springer, 2001.

[24] J. Lieb and J. Rosenthal. Erasure decoding of convolutional codes using first order representations. *Arxiv*, https://arxiv.org/abs/2008.09013, 2020.

[25] A. Alahmadi M. Shi and P. Solé. *Codes and Rings.* Elsevier, Academic Press, 2017.

[26] J. L. Massey and T. Mittelholzer. Convolutional codes over rings. *In Proc. 4th Joint Swedish-Soviet Int. Workshop Information Theory*, pages 14–18, 1989.

[27] J. L. Massey and M. K. Sain. Codes, automata, and continuous systems: Explicit interconnections. In *IEEE Transactions on Automatic Control*, volume 12, pages 644–650, 1967.

[28] A. L. Muñoz Castañeda, J. M. Muñoz-Porras, and F. J. Plaza-Martín. Rosenthal's decoding algorithm for certain 1-dimensional convolutional codes. *IEEE Transactions on Information Theory*, 65(12):7736–7741, 2019.

[29] D. Napp, C. Perea, and R. Pinto. Input-state-output representations and constructions of finite support 2D convolutional codes. *Advances in Mathematics of Communications*, 4(4):533–545, 2010.

[30] D. Napp, R. Pereira, R. Pinto, and P. Rocha. Periodic state-space representations of periodic convolutional codes. *Cryptography and Communications*, 11(4):585–595, 2019.

[31] D. Napp, R. Pinto, and C. Rocha. Noncatastrophic convolutional codes over a finite ring. *Journal of Algebra and Its Applications*, 0(0):2350029, 2021.

[32] D. Napp and P. Rocha. Autonomous multidimensional systems and their implementation by behavioral control. *Systems & Control Letters*, 59(3–4):203–208, 2010.

[33] J. Rosenthal. An optimal control theory for systems defined over finite rings. In V. D. Blondel, E. D. Sontag, M. Vidyasagar, and J. C. Willems, editors, *Open Problems in Mathematical Systems and Control Theory*, chapter 38, pages 193–201. Springer-Verlag, London, Berlin, New York, 1998.

[34] J. Rosenthal. Connections between linear systems and convolutional codes. In Brian Marcus and Joachim Rosenthal, editors, *Codes, Systems and Graphical Models*, volume 123 of *The IMA Volumes in Mathematics and its Applications*, pages 39–66. Springer-Verlag, New York, 2001.

[35] J. Rosenthal and X. Wang. Output feedback pole placement with dynamic compensators. *IEEE Transactions on Information Theory*, AC-41(6):830–843, 1996.

[36] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inf. Th*, 45(6):1833–1844, 1999.

[37] M. V. Carriegos, N. DeCastro-García, and A.L. Muñoz Castañeda. Linear representations of convolutional codes over rings. *preprint in arXiv: 1609.05043v1*, 1-17, 2016.

[38] M. V. Carriegos and A.L. Muñoz Castañeda. On the k-theory of feedback actions on linear systems. *Linear Algebra and its Applications*, 440:233 – 242, 2014.

[39] J. Wood. A formal theory of matrix primeness. *Mathematics of Control, Signals and Systems*, 11(1):40–78, 1998.

[40] E. Zerz. Primeness of multivariate polynomial matrices. *Systems Control Lett.*, 29(3):139–145, 1996.

[41] E. Zerz. On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings. *Asian Journal of Control*, 12(2):119–126, 2010.