SIAM J. CONTROL OPTIM.
Vol. 60, No. 5, pp. 2927–2946

STATE-SPACE REALIZATIONS OF PERIODIC CONVOLUTIONAL CODES*

E. FORNASINI†, D. NAPP‡, R. PEREIRA§, R. PINTO§, AND P. ROCHA¶

Abstract. Convolutional codes are discrete linear systems over a finite field and can be defined as $\mathbb{F}[d]$-modules, where $\mathbb{F}[d]$ is the ring of polynomials with coefficient in a finite field $\mathbb{F}$. In this paper we study the algebraic properties of periodic convolutional codes of period 2 and their representation by means of input-state-output representations. We show that they can be described as $\mathbb{F}[d^2]$-modules and present explicit representation of the set of equivalent encoders. We investigate their state-space representation and present two different but equivalent types of state-space realizations for these codes. These novel representations can be implemented by realizing two linear time-invariant systems separately and switching the input (or the output) that is entering (or leaving) the system. We investigate their minimality and provide necessary and also sufficient conditions in terms of the reachability and observability properties of the two linear systems involved. The ideas presented here can be easily generalized for codes with period larger than 2.

Key words. periodic systems, convolutional codes, realizations

MSC codes. 94B10, 93B20, 93C30

DOI. 10.1137/21M1452172

1. Introduction.

Convolutional codes form a powerful and widely used class of codes which are implemented in a variety of contexts, including wireless standards and satellite communications. As their encoders are linear time-invariant (LTI) systems over a finite field, a strong connection exists between the standard theory of discrete LTI over the real or complex field and the theory of convolutional codes, which uses finite fields [1, 2, 3]. This connection has led to many fundamental results in the state-space and trellis representations which are essential for the implementation and decoding of convolutional codes.

The codewords of a convolutional code are generated by a finite state LTI system (the encoder) that receives as input a streaming of data (the message) to be encoded, processes them, and eventually produces as output the to-be-sent codeword. In order to physically build a hardware implementation of an encoder (typically synthesized by means of shift registers), it is necessary to derive a state-space machine, which

*Received by the editors October 15, 2021; accepted for publication (in revised form) July 12, 2022; published electronically October 4, 2022. A preliminary draft of this work appeared in a conference proceedings as [34].

https://doi.org/10.1137/21M1452172

Funding: This work was supported by Portuguese funds through the Center for Research and Development in Mathematics and Applications (CIDMA) and the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia) within project UIDB/04106/2020. It was also partially supported by Base Funding (UIDB/00147/2020) and Programmatic Funding (UIDP/00147/2020) of the Systems and Technologies Center - SYSTEC - funded by national funds through the FCT/MCTES (PIDDAC). The work of the second author was partially supported by Spanish grants PID2019-108668GB-I00 of the Ministerio de Ciencia e Innovación of the Gobierno de España and VIGROB-287 of the Universitat d'Alacant.

†Department of Information Engineering, University of Padova, Padova, 35122, Italy (ettore.fornasini@unipd.it).

‡Department of Mathematics, University of Alicante, Alicante, 03690, Spain (diego.napp@ua.es).

§CIDMA, Department of Mathematics, University of Aveiro, Aveiro, 3810-193, Portugal (ricardopereira@ua.pt, raquel@ua.pt).

¶SYSTEC, Faculty of Engineering, University of Porto, Porto, 4200-465, Portugal (mprocha@fe.up.pt).

corresponds to viewing the encoder as a set of states with well-defined transitions among them. Moreover, this state machine is extremely important also in figuring out how to decode the data in order to reconstruct the original message; e.g., it helps to derive minimal trellis representations to implement the Viterbi algorithm [4, 5]. The problem of deriving state representations from an input-output map is the so-called *realization problem*, which has been thoroughly studied in the area of systems theory [6] and also in the context of convolutional codes [1, 7, 8, 9, 10, 11].

In this work we aim at investigating the realization problem of time-varying convolutional codes. Time-varying (in particular, periodic) convolutional codes are generated by processing the information through several different encoders, in contrast to standard LTI convolutional codes, which use one single encoder. This class of codes has attracted much attention after Costello conjectured in [12] (see also [13, 14]) that periodic convolutional codes can attain larger free distance, and therefore better error-correction capabilities, than their time-invariant counterparts. From the practical point of view this class of codes is also very important, as it is a capacity-approaching class of codes (as turbo codes and low-density parity-check codes) [15]. In the last decades researchers have investigated such codes developing their algebraic properties and building concrete optimal constructions; see [16, 17, 18, 19, 20]. However, the realization problem of these codes remains barely unexplored and only preliminary or partial results are known [21, 22, 23].

In this paper we shall concentrate our investigation on the class of periodic convolutional codes and focus on two main goals. In the first part of the paper we analyze the structural properties of these codes, and for the sake of simplicity we restrict ourselves to period $p = 2$. Periodic convolutional codes of period 2, also called 2-periodic convolutional codes, can be constructed based on two time-invariant convolutional codes. We show that if time-invariant convolutional codes are defined mathematically as $\mathbb{F}[d]$-modules, 2-periodic convolutional codes can be defined as $\mathbb{F}[d^2]$-modules whose generator matrices have entries in $\mathbb{F}[d]$.

In order to derive our results we will make extensive use of an associated LTI code, called lifted code, that is built by extending the coefficient of the information vectors and the codewords of the periodic code. This will provide a tool for investigating some properties of a periodic code $\mathcal{C}_p$; e.g., it allows us to characterize the set of equivalent encoders of $\mathcal{C}_p$. Moreover, as two full column rank generator matrices can produce a noninjective 2-periodic code, the injectivity of 2-periodic codes needs to be studied, and in section 3 conditions are provided for guaranteeing that two time-invariant encoders generate an injective 2-periodic convolutional code.

The second part of the paper is devoted to investigating state-space representations. The first observation is that one cannot expect, in general, to obtain a periodic input-state-output representation of a periodic convolutional code by means of the individual realizations of each of the associated time-invariant codes; see [22, 23]. To overcome this difficulty we introduce periodic encoding maps in such a way that their images are periodic convolutional codes. This will allow us to present two different ways of constructing state-space realizations that produce a 2-periodic convolutional code. The first one is carried out by realizing a transfer function defined in terms of the two LTI encoders of the associated time-invariant codes and switching periodically the outputs produced by the two resulting state-space machines. The second approach can be implemented in the same fashion but switching periodically the input (rather than the output) that enters in each state system. Both approaches provide effective procedures to implement 2-periodic convolutional codes. The algebraic properties of these realizations are then studied; in particular, we focus on the minimality of such

representations. Necessary and sufficient conditions in terms of the observability and reachability properties of an associated LTI system are presented. We also show that one can build a certain polynomial matrix to derive necessary and sufficient conditions for a realization to be minimal in terms of this matrix. These conditions can be efficiently checked, and we provide an example to illustrate this fact.

It is important to note that there exists a large body of literature on periodic LTI state-space systems [24, 25, 26, 27, 28, 29]. However, these systems are different from the ones considered in this paper. In the classical literature on periodic state-space systems, periodicity is present in the state updating equations, that is, the periodic system is described by $x_{t+1} = A(t)x_t + B(t)u_t$, $y_t = C(t)x_t + D(t)u_t$, where $A(t)$, $B(t)$, $C(t)$, and $D(t)$ are periodic. If this is the state description of a convolutional code, it is not obvious whether such periodic representations can be also described by periodic encoding maps and vice versa. Some partial results in this regard were presented in [23]. Also related is the thread of research in periodic behaviors [26, 30, 28, 31], where periodicity is defined in term of the trajectories of the system (behavior) following the ideas of Willems [32]. Within this behavioral framework the periodic convolutional codes considered in this paper are discrete finite support behaviors described by periodic image representations [33].

The remainder of the paper is organized as follows. In section 2, we collect some preliminaries on convolutional codes as well as periodic convolutional codes and study the algebraic properties of periodic convolutional codes. In particular, we introduce the lifted code and study injectivity and equivalent encoders for these codes. In section 3, we recall a simple state-space realization of LTI convolutional codes and introduce two novel state realizations to implement periodic convolutional codes. In section 4, we investigate minimality issues of the representations presented in section 3. Finally, in section 5 we draw some conclusions.

This paper extends [34], where some preliminary results were drawn concerning a state-space realization of periodic convolutional codes which is analogous to the first one presented here.

2. Preliminaries. In this section, we recall some facts about LTI convolutional codes and periodic convolutional codes.

We also introduce an LTI code associated to a periodic code, called the lifted code, which will play an important role in the remaining part of the paper.

2.1. Time-invariant convolutional codes. Let $\mathbb{F}$ be a finite field, and let $\mathbb{F}[d]$ be the ring of polynomials with coefficient in $\mathbb{F}$. Denote also by $\mathbb{F}^n[d]$ and $\mathbb{F}^{n\times k}[d]$ the set of vectors of length n and the $n \times k$ matrices, respectively, with entries in $\mathbb{F}[d]$.

Convolutional encoders can be thought as black boxes where the information (or message) goes in, is transformed (encoded), and then is sent out as a codeword to be transmitted. If we introduce a variable d, usually called the delay operator, to indicate the instant in which each information arrives or each codeword is transmitted, then we can represent the message as a polynomial sequence

$$u(d) = u_0 + u_1 d + u_2 d^2 + \cdots \in \mathbb{F}^k[d]$$

and the codeword in a similar way:

$$v(d) = v_0 + v_1 d + v_2 d^2 + \cdots \in \mathbb{F}^n[d].$$

We introduce the notion of LTI convolutional code as follows [11, 35, 36, 37, 38].

DEFINITION 2.1. *A* time-invariant convolutional code $\mathcal{C}$ of rate k/n *is a submodule of* $\mathbb{F}^n[d]$ *of rank* k. *A full column rank matrix* $G(d) \in \mathbb{F}^{n\times k}[d]$ *such that*

$$\mathcal{C} = \{v(d) \in \mathbb{F}^n[d] \,:\, v(d) = G(d)u(d); u(d) \in \mathbb{F}^k[d]\} = \mathrm{Im}_{\mathbb{F}[d]}\, G(d)$$

is called an encoder *of* $\mathcal{C}$, $u(d)$ *is the* information vector, *and* $v(d)$ *is the* codeword.

The encoders of a code $\mathcal{C}$ are not unique; however, they only differ by right multiplication by unimodular matrices over $\mathbb{F}[d]$.

$G(d)$ is called *column reduced* if the sum of its column degrees attains the minimal possible value among all the encoders of the same code. If $G(d) \in \mathbb{F}^{n\times k}[d]$ has column degrees $\nu_1, \ldots, \nu_k$, it can be written as

$$G(d) = G_{\mathrm{hc}} \begin{bmatrix} d^{\nu_1} & & & \\ & d^{\nu_2} & & \\ & & \ddots & \\ & & & d^{\nu_k} \end{bmatrix} + G_{\mathrm{rem}}(d),$$

where the "remainder" $G_{\mathrm{rem}}(d)$ is a polynomial matrix such that the degree of column i is less than ν_i, $i = 1, \ldots, k$, and $G_{\mathrm{hc}} \in \mathbb{F}^{n\times k}$ is a matrix whose ith column contains the coefficients of d^{ν_i} in the ith column of $G(d)$. G_{hc} is called the *leading column coefficient matrix* and $G(d)$ is column reduced if and only if G_{hc} has full column rank. An encoder $G(d)$ is said to be *delay-free* if $G(0)$ has full column rank. See also [38, 39] for more details.

Note that the list of column degrees (also known as Forney indices) of a column reduced encoder is unique up to a permutation. We define the *degree* δ of a convolutional code as the sum of the column degrees of one, and hence any, column reduced encoder. A code $\mathcal{C}$ of rate k/n and degree δ is said to be an (n, k, δ) code.

The distance of a code is directly connected with its capacity of correcting errors introduced during transmission. Thus, one of the main objectives of coding theory is the construction of convolutional codes with a large free distance, which is defined as follows.

DEFINITION 2.2. *The* free distance *of a convolutional code* $\mathcal{C}$ *is given by*

$$d_{free}(\mathcal{C}) = \min\left\{\sum_{\ell=0}^{\infty} \mathrm{wt}(v_\ell) : v(d) \in \mathcal{C} \setminus \{0\}\right\},$$

where wt *denotes the* Hamming weight, *that is,* $\mathrm{wt}(v_\ell)$ *corresponds to the number of nonzero components of* v_ℓ, *and* v_ℓ *is the coefficient of* d^ℓ *in* $v(d)$.

2.2. Periodic convolutional codes. In this work we consider convolutional codes $\mathcal{C}$ with periodic encoding maps. Next we introduce the definition of such encoders (or encoding maps) together with the definition of the corresponding periodic (time-varying) convolutional codes; see [12, 14, 17].

DEFINITION 2.3. *Given* r *full column rank polynomial matrices* $G^0(d), G^1(d), \ldots, G^{r-1}(d) \in \mathbb{F}^{n\times k}[d]$, *the* periodic encoding map *induced by* $G^0(d), G^1(d), \ldots, G^{r-1}(d)$ *is defined as*

$$\begin{array}{rccc} \Phi_{(G^0,G^1,\ldots,G^{r-1})}: & \mathbb{F}^k[d] & \to & \mathbb{F}^n[d], \\ & u(d) & \mapsto & v(d) \end{array}$$

with $v(d) = \sum_{i=0}^{+\infty} v_i d^i$ *and* $v_{r\ell+t} = (G^t(d)u(d))_{r\ell+t}$, $t = 0, 1, \ldots, r-1$, $\ell \in \mathbb{N}_0$, *and where* $(G^t(d)u(d))_{r\ell+t}$ *represents the* $(r\ell + t)$*-coefficient of the polynomial* $G^t(d)u(d)$.

The corresponding periodic convolutional code $\mathcal{C}_p$ *is*

$$\mathcal{C}_p = \{v(d) \in \mathbb{F}^n[d] : \exists\, u(d) \in \mathbb{F}^k[d] \text{ s.t. (2.1) holds}\} = \mathrm{Im}_{\mathbb{F}[d]}\, \Phi_{(G^0,G^1,\ldots,G^{r-1})},$$

$$v(d) = \Phi_{(G^0,G^1,\ldots,G^{r-1})}(u(d)). \tag{2.1}$$

Such code will be called an r-periodic convolutional code *of rate* k/n.

Note that such periodic codes are not necessarily $\mathbb{F}[d]$-submodules of $\mathbb{F}^n[d]$.

Example 2.1. Consider the encoding map $\Phi_{(G^0,G^1)} : \mathbb{F}[d] \to \mathbb{F}^3[d]$ such that $G^0(d) = \begin{bmatrix} d \\ 1 \\ d \end{bmatrix}$ and $G^1(d) = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$. Consider also the information word $u(d) = 1$. The corresponding codeword $v(d)$ is given by $v(d) = v_0 + v_1 d + \cdots + v_k d^k$, where

$$v_0 = \left(G^0(d)u(d)\right)_0 = \left(\begin{bmatrix} d \\ 1 \\ d \end{bmatrix}\right)_0 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \ ;$$

$$v_1 = \left(G^1(d)u(d)\right)_1 = \left(\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}\right)_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \ ; \ v_j = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \ j \geq 1.$$

So $v(d) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is a codeword of the code.

Consider now the word $dv(d)$, and investigate whether or not this is a codeword. $dv(d) = \begin{bmatrix} 0 \\ d \\ 0 \end{bmatrix}$ is a codeword if and only if there exists an information word $a(d)$ such that $\Phi_{(G^0,G^1)}(a(d)) = \begin{bmatrix} 0 \\ d \\ 0 \end{bmatrix}$. Let us now compute $\Phi_{(G^0,G^1)}(a(d)) =: w(d)$. We then have that

$$(w(d))_0 = \left(G^0(d)a(d)\right)_0 = \left(\begin{bmatrix} d \\ 1 \\ d \end{bmatrix} a(d)\right)_0 = \left(\begin{bmatrix} 0 \\ a(d) \\ 0 \end{bmatrix}\right)_0.$$

But this implies that $(a(d))_0 = 0$ since $(dv(d))_0 = 0$.

Now

$$(w(d))_1 = \left(G^1(d)a(d)\right)_1 = \left(\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} a(d)\right)_1 = \left(\begin{bmatrix} 0 \\ a(d) \\ a(d) \end{bmatrix}\right)_1,$$

which implies that

$$\left(\begin{bmatrix} 0 \\ a(d) \\ a(d) \end{bmatrix}\right)_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix},$$

since $(dv(d))_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$. Thus on the one hand $(a(d))_1 = 1$ and on the other hand $(a(d))_1 = 0$, which is impossible. So, we can conclude that although $v(d)$ is a codeword, $dv(d)$ is not, meaning that the periodic code $\mathrm{Im}(\Phi_{(G^0,G^1)})$ is not an $\mathbb{F}[d]$-submodule of $\mathbb{F}^3[d]$.

Two sequences of polynomial matrices $G^0(d), \ldots, G^{r-1}(d)$ and $\widetilde{G}^0(d), \ldots, \widetilde{G}^{r-1}(d)$ are said to be *equivalent* if the corresponding periodic encoding maps have the same image (i.e., if the corresponding periodic convolutional codes coincide).

For simplicity we will assume $r = 2$ and denote $G^0(d) = G(d)$ and $G^1(d) = J(d)$.

Let

$$G(d) = \sum_{i=0}^{s} G_i d^i \quad \text{and} \quad J(d) = \sum_{i=0}^{s} J_i d^i$$

be two full column rank matrices with $G_i, J_i \in \mathbb{F}^{n\times k}$, $i = 0, 1, \ldots, s$, and introduce the following matrices:

$$R(d) = \sum_{i=0}^{s} R_i d^i \quad \text{and} \quad S(d) = \sum_{i=0}^{s} S_i d^i, \tag{2.2}$$

where $R_i = G_i$ and $S_i = J_i$, if $i = 2j$, and $R_i = J_i$ and $S_i = G_i$, if $i = 2j+1$, for $j \in \mathbb{N}$. Moreover, given $u(d) = \sum_{i\in\mathbb{N}} u_i d^i \in \mathbb{F}^k[d]$ define $p_0(d^2) \in \mathbb{F}^k[d^2]$ and $p_1(d^2) \in \mathbb{F}^k[d^2]$ as follows:

$$p_0(d^2) = \sum_{j\in\mathbb{N}} u_{2j} d^{2j} \text{ and } p_1(d^2) = \sum_{j\in\mathbb{N}} u_{2j+1} d^{2j}. \tag{2.3}$$

Clearly we have

$$\Phi_{(G,J)}(u(d)) = \left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right] \left[\begin{array}{c} p_0(d^2) \\ p_1(d^2) \end{array}\right],$$

which implies that $\mathcal{C}_p = \Phi_{(G^0,G^1)}$ is an $\mathbb{F}[d^2]$-module in $\mathbb{F}^n[d]$. So, a 2-periodic convolutional code of rate k/n is an $\mathbb{F}[d^2]$-module which admits a representation of the type $\left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right]$, with $R(d), S(d) \in \mathbb{F}^{n\times k}[d]$, i.e, $\mathcal{C}_p = \mathrm{Im}_{\mathbb{F}[d^2]} \left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right]$. We call a representation of this type an $\mathbb{F}[d^2]$-*generator* of the code $\mathcal{C}_p$.

The next result, whose simple proof we omit, characterizes all $\mathbb{F}[d^2]$-generators of a code $\mathcal{C}_p$.

LEMMA 2.1. *Let $R(d), S(d) \in \mathbb{F}^{n\times k}[d]$ such that $\mathcal{C}_p = \mathrm{Im}_{\mathbb{F}[d^2]} \left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right]$. If $\left[\begin{array}{c|c} R'(d) & dS'(d) \end{array}\right]$, with $R'(d), S'(d) \in \mathbb{F}^{n\times k}[d]$, is another $\mathbb{F}[d^2]$-generator of $\mathcal{C}_p$, it follows that*

$$\left[\begin{array}{c|c} R'(d) & dS'(d) \end{array}\right] = \left[\begin{array}{c|c} R(d) & dS(d) \end{array}\right] \left[\begin{array}{cc} U_{11}(d^2) & 0 \\ U_{21}(d^2) & U_{22}(d^2) \end{array}\right],$$

where $U_{11}(d^2), U_{21}(d^2), U_{22}(d^2) \in \mathbb{F}^{k\times k}[d^2]$ and $U_{11}(d^2), U_{22}(d^2)$ are unimodular, i.e., $\det U_{11}(d^2)$, $\det U_{22}(d^2) \in \mathbb{F}\backslash\{0\}$.

2.3. Lifted code. Consider the linear map

$$\mathcal{L} : \mathbb{F}^n[d] \to \mathbb{F}^{2n}[d]$$

defined by

$$\mathcal{L}(v(d)) = v^L(d), \text{ where } (v^L(d))_\ell = \left(\begin{bmatrix} I_n \\ d^{-1} I_n \end{bmatrix} v(d)\right)_{2\ell}, \tag{2.4}$$

where for $v(d) = \sum_{i=0}^{+\infty} v_i d^i \in \mathbb{F}^n[d]$, $d^{-1}v(d)$ is defined as $d^{-1}v(d) = \sum_{i=0}^{+\infty} v_{i+1} d^i \in \mathbb{F}^n[d]$.

We associate with a periodic convolutional code of period 2, $\mathcal{C}_p$, a time-invariant convolutional code $\mathcal{C}^L$, the *lifted* version of $\mathcal{C}_p$, defined as

$$\mathcal{C}^L = \left\{\widetilde{v}(d) \in \mathbb{F}^{2n}[d] : \widetilde{v}(d) = \mathcal{L}(v(d)),\ v(d) \in \mathcal{C}_p\right\}.$$

If

$$G(d) = \sum_{i=0}^{s} G_i d^i \text{ and } J(d) = \sum_{i=0}^{s} J_i d^i$$

are two full column rank matrices with $G_i, J_i \in \mathbb{F}^{n\times k}$, $i = 0, 1, \ldots, s$, then $v(d) = \Phi_{(G,J)}(u(d))$ can be written as

$$\left(\begin{bmatrix} I_n \\ d^{-1} I_n \end{bmatrix} v(d)\right)_{2\ell} = \left(\begin{bmatrix} G(d) \\ d^{-1} J(d) \end{bmatrix} u(d)\right)_{2\ell},\ \ell \in \mathbb{N}_0,$$

where $d^{-1}J(d) = \sum_{i=0}^{s-1} J_{i+1}d^i$. Moreover, it is possible to make the decomposition

$$\begin{bmatrix} G(d) \\ d^{-1}J(d) \end{bmatrix} = L\left(d^2\right) \begin{bmatrix} I_k \\ d^{-1}I_k \end{bmatrix}$$

with

$$L(d) = \begin{bmatrix} G_0 & 0 \\ J_1 & J_0 \end{bmatrix} + \begin{bmatrix} G_2 & G_1 \\ J_3 & J_2 \end{bmatrix} d + \begin{bmatrix} G_4 & G_3 \\ J_5 & J_4 \end{bmatrix} d^2 + \cdots . \tag{2.5}$$

In shorter notation,

$$L(d) = \begin{bmatrix} L_0(d) & | & L_1(d) \end{bmatrix},$$

where the blocks $L_t(d)$ have size $2n \times k,\ t = 0, 1$, and are given by

$$L_0(d) = \sum_{i \in \mathbb{N}_0} \begin{bmatrix} G_{2i} \\ J_{2i+1} \end{bmatrix} d^i,$$

$$L_1(d) = \sum_{i \in \mathbb{N}_0} \begin{bmatrix} G_{2i-1} \\ J_{2i} \end{bmatrix} d^i, \text{ with } G_{-1} = 0.$$

Thus, the lifted code can be represented as

$$\mathcal{C}^L = \left\{ \widetilde{v}(d) : \widetilde{v}(d) = L(d)\widetilde{u}(d),\, \tilde{u}(d) \in \mathbb{F}^{2k}[d] \right\}, \tag{2.6}$$

where $\widetilde{v}(d) = \mathcal{L}(v(d))$ and $\widetilde{u}(d) = \mathcal{L}(u(d))$. This immediately leads to the following result.

LEMMA 2.2. *Let $\mathcal{C}_p$ and $\widetilde{\mathcal{C}}_p$ be two periodic convolutional codes as in Definition 2.3. Then $\mathcal{C}_p = \widetilde{\mathcal{C}}_p$ if and only if the corresponding lifted codes $\mathcal{C}_p^L$ and $\widetilde{\mathcal{C}}_p^L$, respectively, coincide.*

The next theorem easily follows from (2.5) and characterizes the time-invariant encoders which can be regarded as lifted versions of periodic encoding maps.

THEOREM 2.1. *Let $L(d)$ be an encoder of a $(2n, 2k, \delta)$ convolutional code $\mathcal{C} = \mathrm{Im}_{\mathbb{F}[d]} L(d)$. Then there exists $G(d), J(d)$ such that $\mathcal{C} = \mathcal{L}\left(\mathrm{Im}_{\mathbb{F}[d]} \Phi_{(G,J)}\right)$ if and only if there exists $U \in \mathbb{F}^{2k \times 2k}$ invertible such that*

$$L(0)U = \begin{bmatrix} * & 0 \\ * & * \end{bmatrix}.$$

Proof. "If part:" Consider the encoder of $\mathcal{C}$, $L(d)U$, and write

$$L(d)U = \begin{bmatrix} L_{11}(d) & dL_{12}(d) \\ L_{21}(d) & L_{22}(d) \end{bmatrix},$$

with $L_{11}(d), dL_{12}(d), L_{21}(d), L_{22}(d) \in \mathbb{F}[d]^{n \times k}$. Then

$$G(d) = L_{11}(d^2) + dL_{12}(d^2) \text{ and } J(d) = dL_{21}(d^2) + L_{22}(d^2)$$

are such that $\mathcal{C} = \mathcal{L}\left(\mathrm{Im}_{\mathbb{F}[d]} \Phi_{(G,J)}\right)$.

The "only if part" is immediate. ∎

2.4. Injectivity. Injectivity is a fundamental property of an encoding map since it allows one to recover unambiguously the message from the codeword. If $G(d)$ is an encoder of a time-invariant convolutional code, then it is injective because it has full column rank. However, full column rank matrices $G(d)$ and $J(d)$ may yield noninjective periodic encoding maps, and this fact is illustrated in the next example. However, if G_0 and J_0 are full column rank, i.e., if $G(d)$ and $J(d)$ are delay-free, then we have injectivity; see Corollary 2.1 below.

Example 2.2. Consider the polynomials

$$G(d) = G_1 d + G_3 d^3 \quad \text{and} \quad J(d) = J_0 + J_2 d^2.$$

Then $\Phi_{(G,J)}$ is not injective since with $u = 1$ we obtain $v = 0$.

The next result is straightforward.

THEOREM 2.2. *$\Phi_{(G,J)}$ is injective if and only if $L(d)$ in (2.5) is full column rank.*

As $L(0) = \begin{bmatrix} G_0 & 0 \\ J_1 & J_0 \end{bmatrix}$ the next corollary follows.

COROLLARY 2.1. *If $G(d)$ and $J(d)$ are delay-free, then the periodic encoding map $\Phi_{(G,J)}$ is injective.*

The next result states that injectivity of a periodic convolutional code $\mathcal{C}_p$ is a property of $\mathcal{C}_p$ and it is an immediate consequence of Lemma 2.2 and Theorem 2.2.

LEMMA 2.3. *The polynomial matrices $G(d)$ and $J(d)$ generate an injective periodic encoding map $\Phi_{(G,J)}$ if and only if all equivalent pairs of polynomial matrices generate an injective periodic encoding map.*

3. State-space realizations. In this section we review an additional way of generating convolutional codes. More concretely, we consider linear systems theory descriptions known as state-space representations. These descriptions were first adopted by Massey and Sain [2] and studied later on by many researchers [35, 11, 36]. We start by recalling basic facts on these representations together with a simple state-space realization for LTI convolutional codes. We then propose two different, but equivalent, classes of state-space realizations of the periodic encoding map $\Phi_{(G,J)}$. The notions of realizations of codes and of encoding maps are defined below.

3.1. State-space realizations of time-invariant convolutional codes. In what follows, we sometimes identify an element $a(d) = \sum_{i \in \mathbb{N}_0} a_i d^i \in \mathbb{F}[d]$ with the sequence $a_0 = (a(d))_0$, $a_1 = (a(d))_1, \ldots$ formed by its coefficients and also use the notation $a(\ell)$ to denote $a_\ell = (a(d))_\ell$. The same applies for vectors with components in $\mathbb{F}[d]$.

A state-space system

$$\begin{cases} x(\ell+1) &= Ax(\ell) + Bu(\ell), \\ v(\ell) &= Cx(\ell) + Du(\ell), \end{cases} \quad \ell \in \mathbb{N}_0,$$

denoted by (A, B, C, D), where $A \in \mathbb{F}^{m \times m}, B \in \mathbb{F}^{m \times k}, C \in \mathbb{F}^{n \times m}$, and $D \in \mathbb{F}^{n \times k}$, with state x, input u, and output v, is said to be an m-dimensional state-space realization of the time-invariant (n, k, δ) convolutional code $\mathcal{C}$ if $\mathcal{C}$ is the output behavior of (A, B, C, D) corresponding to finite support input sequences u (i.e., to information sequences $u(d) \in \mathbb{F}^k[d]$) and to zero initial conditions, i.e., $x(0) = 0$. Since $\mathcal{C}$ consists of codewords $v(d) \in \mathbb{F}^n[d]$, (A, B, C, D) must produce finite support output sequences v for all finite support input sequences u and zero initial state.

Remark 3.1. The state-space realizations considered in this work are the ones usually found in the coding literature and differ from the realizations considered in [35, 40], where convolutional codes are represented by

$$\left\{\begin{array}{rcl} x(\ell+1) & = & Ax(\ell)+Bu(\ell), \\ y(\ell) & = & Cx(\ell)+Du(\ell), \\ v(\ell) & = & \begin{bmatrix} y(\ell) \\ u(\ell) \end{bmatrix}, \end{array}\right. \quad x(0)=0, \tag{3.1}$$

and the convolutional code is constituted by the finite support input-output sequences, v, corresponding to finite support state sequences; see [35] for details on this realization.

State-space realizations of convolutional codes can be obtained as state-space realizations of encoders. If $G(d) \in \mathbb{F}^{n\times k}[d]$ is an encoder of $\mathcal{C}$, (A,B,C,D) is a state-space realization of $G(d)$ if

$$G(d) = C(I-Ad)^{-1}Bd + D.$$

If $G(d) = \sum_{i\in\mathbb{N}_0} G_i d^i$, with $G_i \in \mathbb{F}^{n\times k}$, then this means that

$$G_0 = D, \;\; G_i = CA^{i-1}B, \; i \geq 1.$$

It is well known that $G(d)$ admits many realizations. Moreover, a state-space realization (A,B,C,D) of $G(d)$ has minimal dimension among all the realizations of $G(d)$ if (A,B) is reachable and (A,C) is observable, i.e., the polynomial matrices $\begin{bmatrix} d^{-1}I-A & | & B \end{bmatrix}$ and $\begin{bmatrix} d^{-1}I-A \\ C \end{bmatrix}$ have, respectively, right and left polynomial inverses (in d^{-1}). In this case, (A,B,C,D) is called a *minimal realization* of $G(d)$. The minimal dimension $\mu(G)$ of a state-space realization of $G(d)$ is called the McMillan degree of $G(d)$ [6].

The next lemma gives a way to compute the McMillan degree of a polynomial matrix.

LEMMA 3.1 (see [36]). *Let $G(d) \in \mathbb{F}^{n\times k}[d]$ be a polynomial matrix. The McMillan degree of $G(d)$ is equal to the maximal degree of the full size minors of $\begin{bmatrix} G(d) \\ I_k \end{bmatrix}$ or, equivalently, to the maximal degree of the minors of $G(d)$.*

Note that if $G(d)$ is column reduced, $\mu(G)$ is equal to the sum of the column degrees of $G(d)$; i.e., $\mu(G)$ is equal to the degree of the code. Column reduced encoders of a code have minimal McMillan degree among all encoders of the code, and they are also called *minimal* encoders.

If $G(d) \in \mathbb{F}^{n\times k}[d]$ is an encoder of a code $\mathcal{C}$, there exists a unimodular matrix $U(d) \in \mathbb{F}^{k\times k}[d]$ such that $\widetilde{G}(d) = G(d)U(d)$ is column reduced and therefore a minimal encoder of $\mathcal{C}$.

The next proposition, adapted from [11, 36], provides a minimal state-space realization for a column reduced encoder, and therefore a minimal state-space realization of the code, in the sense that it is a state-space realization of minimal dimension among all the state-space realizations for which the output behavior corresponding to polynomial inputs and zero initial state is equal to the code.

PROPOSITION 3.1. *Let $G(d) \in \mathbb{F}^{n\times k}[d]$ be a column reduced matrix with rank k and column degrees $\nu_1, \dots, \nu_k$. Consider $m = \sum_{i=1}^{k} \nu_i$. Let $G(d)$ have columns $g_i(d) = \sum_{\ell=0}^{\nu_i} g_{\ell,i} d^\ell$, $i = 1, \dots, k$, where $g_{\ell,i} \in \mathbb{F}^n$. For $i = 1, \dots, k$ define the matrices*

$$A_i = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ 1 & & & \vdots \\ & \ddots & & \vdots \\ & & 1 & 0 \end{bmatrix} \in \mathbb{F}^{\nu_i \times \nu_i}, \; B_i = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in \mathbb{F}^{\nu_i}, \; C_i = \begin{bmatrix} g_{1,i} & \cdots & g_{\nu_i,i} \end{bmatrix} \in \mathbb{F}^{n\times \nu_i}.$$

Then a minimal state-space realization of $G(d)$ is given by the matrix quadruple $(A, B, C, D) \in \mathbb{F}^{m\times m} \times \mathbb{F}^{m\times k} \times \mathbb{F}^{n\times m} \times \mathbb{F}^{n\times k}$, where

$$A = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix}, \quad B = \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix},$$

$$C = \begin{bmatrix} C_1 & \cdots & C_k \end{bmatrix}, \qquad D = \begin{bmatrix} g_{0,1} & \cdots & g_{0,k} \end{bmatrix} = G(0).$$

In the case where $\nu_i = 0$, the ith blocks of A and C are void and in B a zero column occurs.

We immediately conclude that the dimension of a minimal realization of a convolutional code is equal to its degree.

Remark 3.2. The above procedure gives a state-space realization (A, B, C, D) of any polynomial matrix $G(d) \in \mathbb{F}^{n\times k}[d]$. Such a realization is always reachable, but it might be nonobservable, and in this case it will be not a minimal state-space realization of $G(d)$. However, if $G(d)$ is column reduced, then (A, B, C, D) is observable and hence minimal.

3.2. State-space realizations of 2-periodic convolutional codes. In this section we study how the theory of LTI systems can be used to obtain state-space realizations for periodic convolutional codes. We shall propose two different, but equivalent, classes of state-space representations for periodic convolutional codes and study their properties.

3.2.1. Switched output realizations. Let $G(d), J(d) \in \mathbb{F}^{n\times k}[d]$ be two full column rank matrices and $\mathcal{C}_p$ the 2-periodic convolutional code with encoding map $\Phi_{(G,J)}$. Moreover, let $\Sigma = (A, B, C, D)$ be a realization of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$, with $C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$, $C_1, C_2 \in \mathbb{F}^{n\times m}$, where m is the state-space dimension of Σ, and $D = \begin{bmatrix} G_0 \\ J_0 \end{bmatrix}$, $G_0, J_0 \in \mathbb{F}^{n\times k}$.

Let $\begin{bmatrix} v^{(1)}(d) \\ v^{(2)}(d) \end{bmatrix}$, with $v^{(1)}(d) = \sum_{i\in\mathbb{N}} v_i^{(1)} d^i \in \mathbb{F}^n[d]$ and $v^{(2)}(d) = \sum_{i\in\mathbb{N}} v_i^{(2)} d^i \in \mathbb{F}^n[d]$, be the output of Σ corresponding to the input $u(d) \in \mathbb{F}^k[d]$. Now consider as a new output the sequence $w(d) \in \mathbb{F}^n[d]$ defined as $w_{2j} = v_{2j}^{(1)}$ and $w_{2j+1} = v_{2j+1}^{(2)}$, $j \in \mathbb{N}$.

In this way, we obtain the system Σ_p represented in Figure 1.

Note that in Σ_p only one switch is on at each time instant and the switches change from on to off alternatively. The switch corresponding to $v^{(1)}$ is on at the initial time

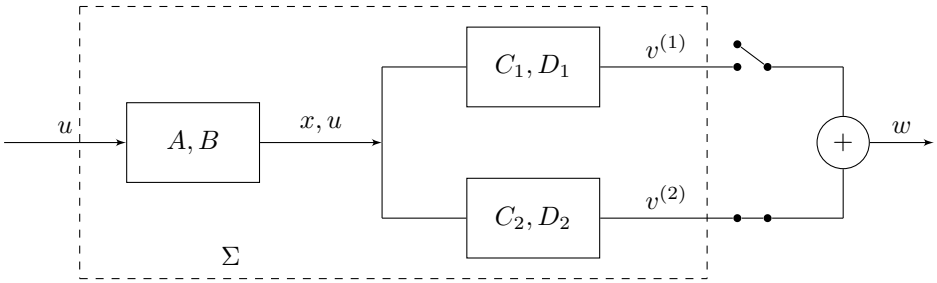

FIG. 1. *Representation of system* Σ_p.

instant, and the initial state is zero. The system Σ_p is called a *periodic switched output state-space system*, and it corresponds to the following periodic state-space equations:

$$\left\{ \begin{array}{rcl} x(\ell+1) & = & A(\ell)x(\ell) + B(\ell)u(\ell), \\ w(\ell) & = & C(\ell)x(\ell) + D(\ell)u(\ell), \end{array} \right. \tag{3.2}$$

with

$$\begin{aligned} A(\ell) &:= A \quad , \quad B(\ell) := B, \\ C(2\ell) &:= C_1 \quad , \quad D(2\ell) := G_0, \\ C(2\ell+1) &:= C_2 \quad , \quad D(2\ell+1) := J_0, \quad \ell \in \mathbb{N}_0. \end{aligned}$$

For short, we write $\Sigma_p = (A, B, C(\ell), D(\ell))$.

A system Σ_p given by (3.2) is a state-space realization of the periodic encoding map $\Phi_{(G,J)}$ if for zero initial state the output $w(d)$ of Σ_p that corresponds to an input $u(d)$ is equal to $\Phi_{(G,J)}(u(d))$ for all $u(d) \in \mathbb{F}^k[d]$.

The next result provides necessary and sufficient conditions for Σ_p to be a realization of $\Phi_{(G,J)}$. These conditions can be easily verified using the well-known realization theory for LTI systems.

THEOREM 3.1. *A periodic switched output system* Σ_p *described by* (3.2) *is a realization of the periodic encoding map* $\Phi_{(G,J)}$ *if and only if the system* Σ *given by* $\left(A, B, \left[\begin{array}{c} C_1 \\ C_2 \end{array}\right], \left[\begin{array}{c} G_0 \\ J_0 \end{array}\right]\right)$ *is a realization of* $\left[\begin{array}{c} G(d) \\ J(d) \end{array}\right]$.

Proof. "If part:" Clearly, if Σ is a realization of $\left[\begin{array}{c} G(d) \\ J(d) \end{array}\right]$, then Σ_p is a realization of $\Phi_{(G,J)}$.

"Only if part:" Assume now that Σ_p is a realization of $\Phi_{(G,J)}$. Then

$$(w(d))_{2m} = \left(\left[\sum_{j=1}^{2m} C_1 A^{j-1} B d^j + G_0 \right] u(d) \right)_{2m}$$

and

$$(w(d))_{2m+1} = \left(\left[\sum_{j=1}^{2m+1} C_2 A^{j-2} B d^j + J_0 \right] u(d) \right)_{2m+1}.$$

In particular, for $u(d) = e_i$, $i = 1, \ldots, k$, where e_i denotes the ith vector of the

canonical basis of $\mathbb{F}^k$, we obtain

$$(w(d))_{2m} = \left[\left(\sum_{j=1}^{2m} C_1 A^{j-1} B d^j + G_0\right) e_i\right]_{2m} = \begin{cases} G_0 e_i, & m = 0, \\ C_1 A^{2m-1} B e_i, & m \geq 1, \end{cases} \tag{3.3}$$

and

$$(w(d))_{2m+1} = \left[\left(\sum_{j=1}^{2m+1} C_2 A^{j-1} B d^j + J_0\right) e_i\right]_{2m+1} = C_2 A^{2m} B e_i,\ m \geq 0,$$

while for $u(d) = de_i$,

$$(w(d))_{2m} = \left[\left(\sum_{j=1}^{2m} C_1 A^{j-1} B d^j + G_0\right) de_i\right]_{2m} = C_1 A^{2m-2} B e_i,\ m \geq 1, \tag{3.4}$$

and

$$(w(d))_{2m+1} = \left[\left(\sum_{j=1}^{2m+1} C_2 A^{j-1} B d^j + J_0\right) de_i\right]_{2m+1} = \begin{cases} J_0 e_i, & m = 0, \\ C_2 A^{2m} B e_i, & m \geq 1. \end{cases}$$

On the other hand, for $u(d) = e_i$,

$$(w(d))_{2m} = (G(d)u(d))_{2m} = (G(d)e_i)_{2m} \tag{3.5}$$

and

$$(w(d))_{2m+1} = (J(d)u(d))_{2m+1} = (J(d)e_i)_{2m+1}\,,$$

whereas for $u(d) = de_i$,

$$(w(d))_{2m} = (G(d)u(d))_{2m} = (G(d)de_i)_{2m} = (G(d)e_i)_{2m-1} \tag{3.6}$$

and

$$(w(d))_{2m+1} = (J(d)u(d))_{2m+1} = (J(d)de_i)_{2m+1} = (J(d)e_i)_{2m}\,.$$

Now, from (3.3) and (3.5), and (3.4) and (3.6), we respectively get

$$(G(d)e_i)_{2m} = \begin{cases} G_0 e_i, & m = 0, \\ C_1 A^{2m-1} B e_i, & m \geq 1, \end{cases}$$

and

$$(G(d)e_i)_{2m-1} = C_1 A^{2m-2} B e_i,\ m \geq 1,$$

which implies that

$$G(d) = G_0 + \sum_{\ell=1}^{\infty} C_1 A^{\ell-1} B d^\ell.$$

Hence (A, B, C_1, G_0) is a state-space realization of $G(d)$. The proof that (A, B, C_2, J_0) is a state-space realization of $J(d)$ is analogous. ∎

In the next example we present a periodic switched output realization of a 2-periodic convolutional code of rate $\frac{2}{3}$ over $\mathbb{F}_2$.

Example 3.1. Let $\mathcal{C}_p$ be the 2-periodic convolutional code with encoding map $\Phi_{(G^0,G^1)} : \mathbb{F}_2^2[d] \to \mathbb{F}_2^3[d]$ such that

$$G^0(d) = \begin{bmatrix} 1+d & 0 \\ 1+d & 1+d \\ 1 & d \end{bmatrix} \text{ and } G^1(d) = \begin{bmatrix} 1+d & 1 \\ 1 & 1+d \\ 0 & 1+d \end{bmatrix}.$$

The system $\Sigma = \left(A, B, \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}, \begin{bmatrix} D_1 \\ D_2 \end{bmatrix}\right)$ with

$$A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

$$C_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix},\ C_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix},\ D_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}, D_2 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

is a realization of $\begin{bmatrix} G^0(d) \\ G^1(d) \end{bmatrix}$, and therefore the corresponding periodic switched output system Σ_p described in (3.2) is a realization of the encoding map $\Phi_{(G^0,G^1)}$ and consequently a realization of $\mathcal{C}_p$.

This code was introduced in [14], where it was shown to have distance 4, whereas any time-invariant convolutional code of the same rate $\frac{2}{3}$ and degree 2 over $\mathbb{F}_2$ cannot have distance larger than 3. Note that time-invariant $(3, 2, 2)$ convolutional codes have minimal realizations of dimension 2 (equal to its degree), which is the same dimension of the realization presented in the above example.

3.2.2. Switched input realizations. Consider now the polynomial matrices $R(d)$ and $S(d)$ defined as in (2.2). Let $\widehat{\Sigma} = (\widehat{A}, \widehat{B}, \widehat{C}, \widehat{D})$ be a realization of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$, with state-space dimension r, and let $\widehat{B} = \begin{bmatrix} \widehat{B}_1 & \widehat{B}_2 \end{bmatrix}$ and $\widehat{D} = \begin{bmatrix} \widehat{D}_1 & \widehat{D}_2 \end{bmatrix}$ be partitioned according to the partition of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$.

Write the input of Σ as $\begin{bmatrix} u^{(1)}(d) \\ u^{(2)}(d) \end{bmatrix}$, with $u^{(1)}(d) = p_0(d^2) \in \mathbb{F}^k[d]$ and $u^{(2)}(d) = dp_1(d^2) \in \mathbb{F}^k[d]$, where $p_0(d^2)$ and $p_1(d^2)$ are defined as in (2.3), that is, they are such that message $u(d)$ can be written as $u(d) = p_0(d^2) + dp_1(d^2)$.

In this way, we obtain the system $\widehat{\Sigma}_p$ represented in Figure 2.

In the scheme, the switches alternate between the positions on and off at each time instant; at time $t = 0$, the switch corresponding to $u^{(1)}$ is on, and the state initial condition is zero. $\widehat{\Sigma}_p$ will be called a *periodic switched input state-space system.* It corresponds to the following periodic state-space equations:

$$\begin{cases} \widehat{x}(\ell+1) &= \widehat{A}(\ell)\widehat{x}(\ell) + \widehat{B}(\ell)u(\ell), \\ w(\ell) &= \widehat{C}(\ell)\widehat{x}(\ell) + \widehat{D}(\ell)u(\ell), \end{cases} \tag{3.7}$$

where $\widehat{A}(\ell) = \widehat{A}$ and $\widehat{C}(\ell) = \widehat{C}$ are fixed and

$$\widehat{B}(2\ell) = \widehat{B}_1,\ \widehat{B}(2\ell+1) = \widehat{B}_2\ ,$$

$$\widehat{D}(2\ell) = \widehat{D}_1 = R(0) = G_0 \text{ and } \widehat{D}(2\ell+1) = \widehat{D}_2 = S(0) = J_0,\ \ell \in \mathbb{N}_0.$$

For short, we write $\widehat{\Sigma}_p = (\widehat{A}, \widehat{B}(\ell), \widehat{C}, \widehat{D}(\ell))$.

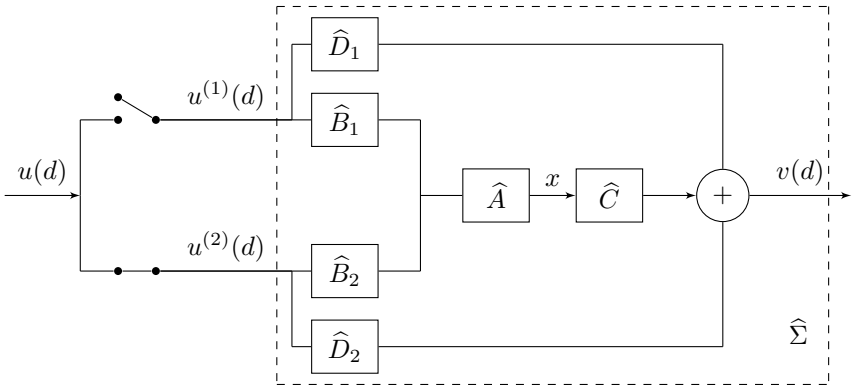

FIG. 2. *Representation of system* $\widehat{\Sigma}_p$.

$\widehat{\Sigma}_p$ is said to be a state-space realization of the periodic encoding map $\Phi_{(G,J)}$ if, for zero initial state, the output $v(d)$ of $\widehat{\Sigma}_p$, corresponding to an input $u(d)$, is equal to $\Phi_{(G,J)}(u(d))$ for all $u(d) \in \mathbb{F}^k[d]$.

The following result is important since it explicitly provides a relation between the realizations of the periodic encoding maps and time-invariant realizations.

THEOREM 3.2. *A periodic switched input system* $\widehat{\Sigma}_p$*, described by* (3.7)*, is a realization of the periodic encoding map* $\Phi_{(G,J)}$ *if and only if the system* $\widehat{\Sigma}$ *described by* $\left(\widehat{A}, \begin{bmatrix} \widehat{B}_1 & \widehat{B}_2 \end{bmatrix}, \widehat{C}, \begin{bmatrix} \widehat{D}_1 & \widehat{D}_2 \end{bmatrix}\right)$ *is a time-invariant realization of* $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$.

Proof. "If part:" Assume that $\widehat{\Sigma}$ is a realization of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$. Then, clearly, $\widehat{\Sigma}_1 = \left(\widehat{A}, \widehat{B}_1, \widehat{C}, \widehat{D}_1\right)$ is a realization of $R(d)$ while $\widehat{\Sigma}_2 = \left(\widehat{A}, \widehat{B}_2, \widehat{C}, \widehat{D}_2\right)$ is a realization of $S(d)$. Consider a message

$$u(d) = \sum_{j\in\mathbb{N}} u_j d^j = p_0(d^2) + dp_1(d^2) = \sum_{j\in\mathbb{N}} u_{2j} d^{2j} + d\sum_{j\in\mathbb{N}} u_{2j+1} d^{2j}.$$

When $u(d)$ is fed into $\widehat{\Sigma}_p$, due to the way the switches work, the sequences fed into $\widehat{\Sigma}_1$ and $\widehat{\Sigma}_2$ are, respectively, $p_0(d^2)$ and $dp_1(d^2)$. Therefore the output of $\widehat{\Sigma}_1$ is equal to $R(d)p_0(d^2)$ whereas the output of $\widehat{\Sigma}_2$ is equal to $S(d)dp_1(d^2)$. Consequently, the corresponding output of $\widehat{\Sigma}_p$ is

$$R(d)p_0(d^2) + S(d)dp_1(d^2) = \begin{bmatrix} R(d) & dS(d) \end{bmatrix} \begin{bmatrix} p_0(d^2) \\ p_1(d^2) \end{bmatrix} = \Phi_{(G,J)}(u(d)),$$

as previously seen in section 2.2. In this way we conclude that $\widehat{\Sigma}_p$ is a realization of $\Phi_{(G,J)}$.

"Only if part:" Assume now that $\widehat{\Sigma}_p$ is a realization of $\Phi_{(G,J)}$. Let $u(d) = e_i$, where e_i is the ith basis vector of the canonical basis of $\mathbb{F}^k$. When $u(d)$ is fed into $\widehat{\Sigma}_p$, the corresponding output is

$$w(d) = \Phi_{(G,J)}(e_i) = R(d)e_i.$$

On the other hand,

$$w(d) = \sum_{j\in\mathbb{N}} w_j d^j \quad \text{with} \quad w_j = \begin{cases} \widehat{D}_1 e_i, & j = 0, \\ \widehat{C}\widehat{A}^{j-1}\widehat{B}_1 e_i, & j \geq 1, \end{cases}$$

that is, $w(d) = \left[\widehat{C}(I - \widehat{A}d)^{-1}d\widehat{B}_1 + \widehat{D}_1\right] e_i$. Thus,

$$R(d)e_i = \left[\widehat{C}(I - \widehat{A}d)^{-1}d\widehat{B}_1 + \widehat{D}_1\right] e_i.$$

Making i vary from 1 to k, this allows us to conclude that

$$R(d) = \widehat{C}(I - \widehat{A}d)^{-1}d\widehat{B}_1 + \widehat{D}_1,$$

i.e., $\widehat{\Sigma}_1$ is a time-invariant realization of $R(d)$.

Let now $u(d) = de_i$, and feed this input into $\widehat{\Sigma}_p$. Then the corresponding output is given by

$$w(d) = \Phi_{(G,J)}(de_i) = S(d)de_i.$$

On the other hand,

$$w(d) = \sum_{j\in\mathbb{N}} w_j d^j \quad \text{with} \quad w_j = \begin{cases} \widehat{D}_2 e_i, & j = 1, \\ \widehat{C}\widehat{A}^{j-2}\widehat{B}_2 e_i, & j \geq 2. \end{cases}$$

Thus,

$$\begin{aligned} S(d)de_i &= \left(\widehat{D}_2 d + \sum_{j\geq 2} \widehat{C}\widehat{A}^{j-2}\widehat{B}_2 d^j\right) e_i \\ &= d\left(\widehat{D}_2 + \sum_{j\geq 2} \widehat{C}\widehat{A}^{j-2}\widehat{B}_2 d^{j-1}\right) e_i \\ &= d\left(\widehat{D}_2 + \sum_{\ell\geq 1} \widehat{C}\widehat{A}^{\ell-1}\widehat{B}_2 d^{\ell}\right) e_i \\ &= d\left(\widehat{D}_2 + \widehat{C}(I - \widehat{A}d)^{-1}d\widehat{B}_2\right) e_i. \end{aligned}$$

Letting i vary from 1 to k, one concludes that

$$S(d)d = \left(\widehat{D}_2 + \widehat{C}(I - \widehat{A}d)^{-1}d\widehat{B}_2\right) d$$

and hence

$$S(d) = \widehat{C}(I - \widehat{A}d)^{-1}d\widehat{B}_2 + \widehat{D}_2,$$

which means that $\widehat{\Sigma}_2$ is a time-invariant realization of $S(d)$.

Finally, since $\widehat{\Sigma}_1$ and $\widehat{\Sigma}_2$ are time-invariant realizations of $R(d)$ and $S(d)$, respectively, it follows that $\widehat{\Sigma}$ is a time-invariant realization of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$. ∎

4. Minimality. In section 3 we studied switched output and switched input realizations of a periodic encoding map of a periodic convolutional code $\mathcal{C}_p$. In this section we will consider these realizations of $\mathcal{C}_p$ and study the question of their minimality.

A switched output (input) system Σ_p $\left(\widehat{\Sigma}_p\right)$ is said to be a switched output (input) realization of a periodic convolutional code $\mathcal{C}_p$ if the output behavior of Σ_p $\left(\widehat{\Sigma}_p\right)$ corresponding to polynomial inputs and zero initial state is equal to $\mathcal{C}_p$. A minimal switched output (input) realization of $\mathcal{C}_p$ is a realization of $\mathcal{C}_p$ of this type with minimal dimension among all realizations of $\mathcal{C}_p$ of the same type.

It is obvious that if $\Phi_{(G,J)}$ is a periodic encoding map of $\mathcal{C}_p$, for some $G(d), J(d) \in \mathbb{F}^{n\times k}[d]$, then all switched output realizations and switched input realizations of $\Phi_{(G,J)}$ are realizations of the same type of $\mathcal{C}_p$. On the other hand, if Σ_p is a switched output realization of $\mathcal{C}_p$ with associated system $\Sigma = \left(A, B, \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}, \begin{bmatrix} G_0 \\ J_0 \end{bmatrix}\right)$, with $A \in \mathbb{F}^{s\times s}$, $B \in \mathbb{F}^{s\times k}$, $C_1, C_2 \in \mathbb{F}^{n\times s}$, and $G_0, J_0 \in \mathbb{F}^{n\times k}$, it is clear that $\mathcal{C}_p = \operatorname{Im}\Phi_{(G,J)}$, where

$$G(d) = G_0 + \sum_{\ell=1}^{\infty} C_1 A^{\ell-1} B d^{\ell} \quad \text{and} \quad J(d) = J_0 + \sum_{\ell=1}^{\infty} C_2 A^{\ell-1} B d^{\ell}.$$

The same happens when we consider switched input realizations; i.e., if $\widehat{\Sigma}_p$ is a realization of $\mathcal{C}_p$ of this type, with associated systems $\widehat{\Sigma}_1 = (\widehat{A}, \widehat{B}_1, \widehat{C}, \widehat{D}_1)$ and $\widehat{\Sigma}_2 = (\widehat{A}, \widehat{B}_2, \widehat{C}, \widehat{D}_2)$ and

$$R(d) = \widehat{D}_1 + \sum_{\ell=1}^{\infty} \widehat{C}\widehat{A}^{\ell-1}\widehat{B}_1 d^{\ell} = \sum_{i=0}^{s} R_i d^i \quad \text{and} \quad S(d) = \widehat{D}_2 + \sum_{\ell=1}^{\infty} \widehat{C}\widehat{A}^{\ell-1}\widehat{B}_2 d^{\ell} = \sum_{i=0}^{s} S_i d^i,$$

then $\widehat{\Sigma}_p$ is a switched input realization of $\Phi_{(G,J)}$ where

$$G(d) = \sum_{i=0}^{s} G_i d^i \quad \text{and} \quad J(d) = \sum_{i=0}^{s} J_i d^i,$$

with $G_i = R_i$ and $J_i = S_i$ for $i = 2j$, and $G_i = S_i$ and $J_i = R_i$ for $i = 2j+1$, $j \in \mathbb{N}$.

So, we conclude that the switched output realizations and switched input realizations of a periodic convolutional code $\mathcal{C}_p$ are the realizations of the same type of the periodic encoding maps of $\mathcal{C}_p$. Thus, in order to investigate the minimal encoders of $\mathcal{C}_p$ we study first the minimal realizations of the encoding maps of $\mathcal{C}_p$ since a minimal encoder of $\mathcal{C}_p$ is also a minimal realization of a suitable periodic encoding map of $\mathcal{C}_p$.

The next lemmas are direct consequences of Lemma 3.1 and Theorem 3.1 and study the minimality of switched output realizations of periodic encoding maps.

LEMMA 4.1. *Let $\mathcal{C}_p$ be a periodic convolutional code and $\Phi_{(G,J)}$ a periodic encoding map of $\mathcal{C}_p$ for some full column rank matrices $G(d), J(d) \in \mathbb{F}^{n\times k}[d]$. A switched output periodic system Σ_p is a minimal switched output realization of $\Phi_{(G,J)}$ if and only if the associated system Σ is a minimal realization of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$. Moreover, the minimal dimension of a switched output realization of $\Phi_{(G,J)}$ is equal to the maximal degree of the minors of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ and it is called the switched output McMillan degree of $\Phi_{(G,J)}$.*

DEFINITION 4.1. *Given a 2-periodic convolutional code $\mathcal{C}_p$, a periodic encoding map of $\mathcal{C}_p$ is said to be* switched output minimal *if it has minimal switched output McMillan degree, among all the encoding maps of $\mathcal{C}_p$.*

LEMMA 4.2. *If* $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ *is not column reduced, then there exists a unimodular matrix $U(d)$ such that*

$$\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix} = \begin{bmatrix} G(d) \\ J(d) \end{bmatrix} U(d)$$

is column reduced, produces a periodic encoding map, $\Phi_{(\widetilde{G},\widetilde{J})}$, equivalent to $\Phi_{(G,J)}$ and is such that

$$\mu\left(\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix}\right) \leq \mu\left(\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}\right).$$

Proof. The proof follows from the fact that

$$\Phi_{(\widetilde{G},\widetilde{J})}(u(d)) = \Phi_{(G,J)}(U(d)u(d))$$

for all $u(d) \in \mathbb{F}^k[d]$ and $U(d)$ is unimodular. ∎

So, given an encoding map $\Phi_{(G,J)}$ of a periodic code we can always find an equivalent encoding map $\Phi_{(\widetilde{G},\widetilde{J})}$ such that the corresponding time-invariant encoder $\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix}$ is a column reduced encoder with McMillan degree smaller than or equal to the McMillan degree of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$. This is achieved by right multiplication by a unimodular matrix. In the case of time-invariant codes, this procedure allows us to obtain a minimal encoder of the code since all column reduced encoders are minimal. But the same does not hold for periodic codes; i.e., periodic encoding maps $\Phi_{(G,J)}$ such that $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ is a time-invariant column reduced encoder not necessarily switched output minimal, as the following example shows.

Example 4.1. Consider the periodic code $\mathcal{C}_p = \Phi_{(G,J)}$ with

$$G(d) = G_0 \quad \text{and} \quad J(d) = J_0 + J_1 d + J_2 d^2 + J_2 d^3,$$

where $G_0, J_0, J_1, J_2 \in \mathbb{F}^{n\times k}$ and G_0 and J_2 are full column rank matrices. Then

$$\begin{bmatrix} G(d) \\ J(d) \end{bmatrix} = \begin{bmatrix} G_0 \\ J_0 + J_1 d + J_2 d^2 + J_2 d^3 \end{bmatrix}$$

is column reduced, which implies $\Phi_{(G,J)}$ has switched output McMillan degree equal to the sum of the column degrees of $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$, which is equal to $3k$. The corresponding lifted code has encoder

$$L(d) = \begin{bmatrix} G_0 & 0 \\ J_1 & J_0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ J_2 & J_2 \end{bmatrix} d,$$

and therefore

$$L(d) \begin{bmatrix} I_k & 0 \\ -I_k & I_k \end{bmatrix} = \begin{bmatrix} G_0 & 0 \\ J_1 - J_0 & J_0 + J_2 d \end{bmatrix}$$

is another encoder of the lifted code, which means that

$$\widetilde{G}(d) = G_0 \quad \text{and} \quad \widetilde{J}(d) = J_0 + (J_1 - J_0)d + J_2 d^2$$

are such that $\Phi_{(\widetilde{G},\widetilde{J})}$ is another encoding map which originates the periodic code $\mathcal{C}_p$. Since

$$\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix} = \begin{bmatrix} G_0 \\ J_0 + (J_1 - J_0)d + J_2 d^2 \end{bmatrix}$$

is also column reduced, we have that the switched output McMillan degree of $\Phi_{(\widetilde{G},\widetilde{J})}$ is equal to $2k$.

The previous example shows that there can exist two encoding maps, $\Phi_{(G,J)}$ and $\Phi_{(\widetilde{G},\widetilde{J})}$, of a periodic code, with $\begin{bmatrix} G(d) \\ J(d) \end{bmatrix}$ and $\begin{bmatrix} \widetilde{G}(d) \\ \widetilde{J}(d) \end{bmatrix}$ column reduced, but with different switched output McMillan degrees.

Regarding switched input realizations of periodic encoding maps, their minimality is characterized in the next lemma, which is a consequence of Theorem 3.2.

LEMMA 4.3. *Let $\mathcal{C}_p$ be a periodic convolutional code, $\Phi_{(G,J)}$ a periodic encoding map of $\mathcal{C}_p$, for some $G(d), J(d) \in \mathbb{F}^{n\times k}[d]$, and $R(d), S(d) \in \mathbb{F}^{n\times k}[d]$ the matrices obtained from $G(d)$ and $J(d)$ as defined in* (2.2). *The switched input periodic system $\widehat{\Sigma}_p$ is a minimal switched input realization of $\Phi_{(G,J)}$ if and only if the associated system $\widehat{\Sigma}$ is a minimal realization of $\begin{bmatrix} R(d) & S(d) \end{bmatrix}$.*

5. Conclusions and open questions. In this paper we have studied the algebraic properties of periodic convolutional codes and their representation by means of input-state-output representations. The main ideas and results presented in this work have to do with novel representations of this important class of convolutional codes. First we show how these codes can be seen as $\mathbb{F}[d^2]$-modules and present concrete representations of their equivalent encoders. As for the state-space representations, we present two original different approaches to implement periodic codes that lead to simple state realizations and investigate their minimality. Switched systems realizations form a more involved class of systems than standard LTI systems, which prevents us from applying directly well known mathematical results in systems theory. Although some fundamental results were derived in this work, several questions remain unanswered. Among them is the important issue of the minimality of the switched output (input) realizations of a periodic code $\mathcal{C}_p$ rather than of a corresponding periodic encoding map. This was only partially addressed here and is the subject of current research.

REFERENCES

[1] J. ROSENTHAL, *Connections between linear systems and convolutional codes*, in Codes, Systems and Graphical Models, IMA Vol. Math. Appl. 123, B. Marcus and J. Rosenthal, eds., Springer, New York, 2001, pp. 39–66.

[2] J. L. MASSEY AND M. K. SAIN, *Codes, automata, and continuous systems: Explicit interconnections*, IEEE Trans. Automat. Control, 12 (1967), pp. 644–650.

[3] G. D. FORNEY, *Algebraic structure of convolutional codes, and algebraic system theory*, in Mathematical System Theory, Springer, Berlin, Heidelberg, 1991, pp. 527–557.

[4] G. D. FORNEY, *The Viterbi algorithm*, Proc. IEEE, 61 (1973), pp. 268–278.

[5] G. D. FORNEY, *Minimal realizations of linear systems: The shortest basis approach*, IEEE Trans. Inform. Theory, 57 (2011), pp. 726–737.

[6] T. Kailath, *Linear Systems*, Prentice Hall Inform. System Sci. Ser., Prentice-Hall, Englewood Cliffs, NJ, 1980.
[7] J. L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Inform. Theory, IT-15 (1969), pp. 122–127.
[8] J. Rosenthal, J. M. Schumacher, and E. V. York, *The Behavior of Convolutional Codes*, Report BS-R9533, CWI, Amsterdam, 1995.
[9] G. D. Forney, Jr., *Minimal bases of rational vector spaces, with applications to multivariable linear systems*, SIAM J. Control Optim., 13 (1975), pp. 493–520, https://doi.org/10.1137/0313029.
[10] G. D. Forney, R. Johannesson, and Z.-X. Wan, *Minimal and canonical rational generator matrices for convolutional codes*, IEEE Trans. Inform. Theory, IT-42 (1996), pp. 1865–1880.
[11] H. Gluesing-Luerssen and G. Schneider, *State space realizations and monomial equivalence for convolutional codes*, Linear Algebra Appl., 425 (2007), pp. 518–533.
[12] D. J. Costello, *Free distance bounds for convolutional codes*, IEEE Trans. Inform. Theory, 20 (1974), pp. 356–365.
[13] M. Mooser, *Some periodic convolutional codes better than any fixed code (Corresp.)*, IEEE Trans. Inform. Theory, 29 (1983), pp. 750–751.
[14] R. Palazzo, *A time-varying convolutional encoder better than the best time-invariant encoder*, IEEE Trans. Inform. Theory, 39 (1993), pp. 1109–1110.
[15] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, New York, 1999.
[16] P. J. Lee, *There are many good periodically time-varying convolutional codes*, IEEE Trans. Inform. Theory, 35 (1989), pp. 460–463.
[17] D. Truhachev, K. S. Zigangirov, and D. J. Costello, *Distance bounds for periodically time-varying and tail-biting LDPC convolutional codes*, IEEE Trans. Inform. Theory, 56 (2010), pp. 4301–4308.
[18] A. J. Feltstrom, D. Truhachev, M. Lentmaier, and K. S. Zigangirov, *Braided block codes*, IEEE Trans. Inform. Theory, 55 (2009), pp. 2640–2658.
[19] F. Fekri, M. Sartipi, R. M. Mersereau, and R. W. Schafer, *Convolutional codes using finite-field wavelets: Time-varying codes and more*, IEEE Trans. Signal Process., 53 (2005), pp. 1881–1896.
[20] J. Justesen, *New convolutional code constructions and a class of asymptotically good time-varying codes*, IEEE Trans. Inform. Theory, 19 (1973), pp. 220–225.
[21] J. J. Climent, V. Herranz, C. Perea, and V. Tomás, *A systems theory approach to periodically time-varying convolutional codes by means of their invariant equivalent*, in Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Springer, Berlin, Heidelberg, 2009, pp. 73–82.
[22] D. Napp, R. Pereira, and P. Rocha, *A state space approach to periodic convolutional codes*, in Coding Theory and Applications, Á. I. Barbero, V. Skachek, and Ø. Ytrehus, eds., Springer, Cham, 2017, pp. 238–247.
[23] D. Napp, R. Pereira, R. Pinto, and P. Rocha, *Periodic state-space representations of periodic convolutional codes*, Cryptogr. Commun., 11 (2019), pp. 585–595.
[24] M. Ait Rami and D. Napp, *Discrete-time positive periodic systems with state and control constraints*, IEEE Trans. Automat. Control, 61 (2016), pp. 234–239.
[25] S. Bittanti and P. Colaneri, *Periodic Systems, Filtering and Control*, Springer, London, 2009.
[26] J. C. Aleixo, P. Rocha, and J. C. Willems, *State space representation of SISO periodic behaviors*, in Proceedings of the 50th Annual IEEE Conference on Decision and Control and European Control Conference, 2011, pp. 1545–1550.
[27] P. Bolzern and P. Colaneri, *The periodic Lyapunov equation*, SIAM J. Matrix Anal. Appl., 9 (1988), pp. 499–512, https://doi.org/10.1137/0609041.
[28] M. Kuijper, *A periodically time-varying minimal partial realization algorithm based on twisting*, Automatica, 35 (1999), pp. 1543–1548.
[29] R. Bru, S. Romero, and E. Sánchez, *Structural properties of positive periodic discrete-time linear systems: Canonical forms*, Appl. Math. Comput., 153 (2004), pp. 697–719.
[30] M. Kuijper and J. C. Willems, *A behavioral framework for periodically time varying systems*, in Proceedings of the 36th Annual IEEE Conference on Decision and Control, Vol. 3, 1997, pp. 2013–2016.
[31] D. Napp, M. van der Put, and S. Shankar, *Periodic behaviors*, SIAM J. Control Optim., 48 (2010), pp. 4652–4663, https://doi.org/10.1137/100782577.
[32] J. C. Willems, *Paradigms and puzzles in the theory of dynamical systems*, IEEE Trans. Au-

tomat. Control, 36 (1991), pp. 259–294.
[33] D. Napp, S. Shankar, and H. L. Trentelman, *Regular implementation in the space of compactly supported functions*, Systems Control Lett., 57 (2008), pp. 851–855.
[34] E. Fornasini, D. Napp, R. Pereira, R. Pinto, and P. Rocha, *State realizations of 2-periodic convolutional codes: A switching system approach*, IFAC-PapersOnLine, 54 (2021), pp. 114–118.
[35] J. Rosenthal and E. V. York, *BCH convolutional codes*, IEEE Trans. Automat. Control, 45 (1999), pp. 1833–1844.
[36] E. Fornasini and R. Pinto, *Matrix fraction descriptions in convolutional coding*, Linear Algebra Appl., 392 (Supplement C) (2004), pp. 119–158.
[37] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, *Strongly MDS convolutional codes*, IEEE Trans. Inform. Theory, 52 (2006), pp. 584–598.
[38] R. J. McEliece, *The algebraic theory of convolutional codes*, in Handbook of Coding Theory, Vols. I and II, V. S. Pless and W. C. Huffman, eds., North-Holland, Amsterdam, 1998, pp. 1065–1138.
[39] G. Solomon and H. C. A. van Tilborg, *A connection between block and convolutional codes*, SIAM J. Appl. Math., 37 (1979), pp. 358–369, https://doi.org/10.1137/0137027.
[40] R. Hutchinson, *The existence of strongly MDS convolutional codes*, SIAM J. Control Optim., 47 (2008), pp. 2812–2826, https://doi.org/10.1137/050638977.