

Concatenated linear systems over rings and their application to construction of concatenated families of convolutional codes [☆]

Noemí DeCastro–García

Departamento de Matemáticas, Universidad de León. Spain

M. I. García-Planas

Departament de Matemàtiques. Universitat Politècnica de Catalunya. Spain

Abstract

We present a generalization of the theory of concatenated linear systems to commutative rings with identity. Moreover, we highlight sufficient conditions to obtain reachable and observable concatenated linear systems. This approach provides us with minimal input-state-output representations by means of which we can construct observable concatenated families of convolutional codes with different parameters over some particular rings. This work focuses on the characterization of models of serialized, systematic serialized and parallelized concatenation.

Keywords: Linear systems, convolutional codes, concatenation, control properties, linear representations

2010 MSC: 13C10, 15A21, 93B10, 93B55, 93C05, 05A17

1. Introduction

The algebraic theory of discrete-time linear systems over arbitrary fields was introduced by Kalman in 1965 (see [13]). In particular, the class of discrete time-invariant linear systems over commutative rings with identity has been extensively studied by different authors (see [1, 14, 22, 26], among others). This class of systems provides us with an input/state/output (I/S/O) representation of the behavior of the system. The part of the state-space representation provides detailed descriptions of the internal behavior of the system, and the

[☆]This work has been partially supported by the Spanish National Institute of Cyber-Security (INCIBE) accordingly to the rule 19 of The Digital Confidence Plan and the Universidad de León under the contract A18.

Email addresses: ncasg@unileon.es (Noemí DeCastro–García),
maria.isabel.garcia@upc.edu (M. I. García-Planas)

input/output part gives information about the external behavior of the system. Moreover, in the case of finite-dimensional dynamical systems, many qualitative properties can be studied in terms of initial-value problems.

One of the most recent applications of discrete time-invariant linear systems has been proposed by Rosenthal *et al.* in [23, 24, 25, 28]. They show that for a convolutional code over a finite field exists a unique and minimal I/S/O representation (a reachable linear system) that describes the code. They use this connection to construct observable convolutional codes with good distance properties. From these works, there is a considerable body of literature about the construction of convolutional codes using the approach of linear systems. In particular, some authors as [2, 3, 9, 10, 27] had exploited this relation for the construction of concatenated convolutional codes and, to deduce control properties.

In coding theory, concatenated convolutional codes are a class of convolutional codes that are obtained by combining an inner code and an outer code. They were conceived by Forney in [8] to solve the problem of under-utilization of memory since with concatenation, it is possible to join two encoders in a single block. In turn, it provides a solution to the problem of finding a code that has both exponentially decreasing error probability with increasing block length and polynomial time decoding complexity. This type of codes is used to detect, correct and hide information, and they are handy when it is necessary to communicate highly sensitive topics. An important example of concatenated convolutional codes is the turbo codes.

The study of error-correcting codes initially took place in the setting of vector spaces over finite fields. Nevertheless, recently, the research of linear codes over finite rings has become increasingly important, that is due to the realization that many significant and apparently non-linear codes are, in fact, equivalent to linear codes over a modular integer ring. Regarding its applications, for example, in [17] an encoder over $\mathbb{Z}/4\mathbb{Z}$ is developed for decoding MPEG-4 images. Recently, in [12], a steganographic protocol has been performed based on convolutional codes over the ring $\mathbb{Z}/4\mathbb{Z}$.

Massey and Mittelholzer developed the first approach to convolutional codes over rings in [19] and [20] where they showed that the convolutional codes over \mathbb{Z}_n are usually more appropriate for some contexts as the phase modulation. They also focused on the study of minimal and systematic encoders over rings. Minimal encoders, properties or trellis representations of convolutional codes over rings have been developed in [7, 11, 15, 16] or [29], among others.

However, it is important to recall that convolutional codes over rings do not behave in the same way as convolutional codes over fields because their behavior depends strongly on the structure of the underlying ring. For this reason, the extension of the relation between linear systems and convolutional codes is not easily generalized to all commutative ring with identity. In [4] and [6], this connection is given to $R = \mathbb{Z}_n$ where n is square free in terms of linear and commutative algebra. This result let us to construct observable families of convolutional codes over the ring. These families allow us to construct an algebraic system of simultaneous signal encoding in linear coding networks over

the ring R , growing the security of the system. The same message m , encoded over the ring R , is sent to n receivers and every receiver decodes its message μ_j over $\mathbb{F}_j = R/\mathfrak{m}_j$ where \mathfrak{m}_j is the j -th maximal ideal in the spectrum of R . Note that a continuity between receivers is not needed. Moreover, if the messages over \mathbb{F}_j are shared, it would be possible to create the original message that we assume unique: that is to say, $m = (\mu_1, \dots, \mu_t)$. This approximation is used for the construction of block codes over \mathbb{Z}_6 in [5]. It is shown that, for given block codes over \mathbb{Z}_2 and \mathbb{Z}_3 , the composition yields codes that are equal or better than the codes obtained from the standard coset coding technique in terms of performance.

This paper is devoted to extend the concatenation of linear systems over a commutative rings with identity R (serialized, systematic serialized and parallelized concatenation). Also, properties of reachability and observability are highlighted in order to be able to construct (observable) concatenated families of convolutional codes over the ring R with different complexities and parameters. We wonder about these properties from the patching concatenated systems over the residue fields of the ring or from conditions over the systems to concatenate. The extension is considered in the real understanding that, it is not a direct extension of the existing results on fields because, as we have remarked above, the behavior of the code depends strongly on the ring. In this study, the difference is revealed to ensure reachability on rings, since the full rank of the reachability matrix it is not enough to ensure the code's reachability.

This paper is structured as follows: In Section 2, we give the preliminaries. In Section 3, we describe the concatenation of linear systems over rings. In Section 4, control properties of concatenated linear systems over rings are studied. In Section 5, we emphasize the application of our results in the construction of concatenated families of convolutional codes over noetherian von Neumann regular rings. Finally, the conclusions with the future work and the references are shown.

2. Preliminaries.

The first part of this section is devoted to basic preliminaries about linear systems over rings and some important properties such as reachability and observability. In the second part, we give a review about convolutional codes over finite fields and their connection with linear systems.

2.1. Linear systems over rings.

Let R be a commutative ring with identity. A time-invariant linear system $\Sigma = (A, B, C, D) \in R^{\delta \times \delta} \times R^{\delta \times k} \times R^{p \times \delta} \times R^{p \times k}$ is described as follows

$$\begin{cases} x_{t+1} = Ax_t + Bu_t \\ y_t = Cx_t + Du_t \\ v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix}, x_0 = 0, \exists \gamma : x_{\gamma+1} = 0. \end{cases} \quad (1)$$

where $x_t \in R^\delta$ is the state vector, $u_t \in R^k$ is the control vector, and $v_t \in R^p$ is the output vector for each time instant t . The dimension of the state space δ is known as the McMillan degree of the linear system.

Firstly, we clarify some notations: let $A = (a_{ij})$ and $\Sigma^R = (A, B, C, D)$ be a matrix and a linear system over R , respectively. Let \mathfrak{p} be a prime ideal of the spectrum of the ring R . In the following, we will denote $A(\mathfrak{p}) = \overline{(a_{ij})} = (a_{ij}) \pmod{\mathfrak{p}}$ and $\Sigma(\mathfrak{p}) = [A(\mathfrak{p}), B(\mathfrak{p}), C(\mathfrak{p}), D(\mathfrak{p})]$ the restrictions of A and Σ^R to each prime ideal $\mathfrak{p} \in \text{Spec}(R)$.

We review some results about reachability properties of systems over commutative rings with identity.

Proposition 2.1. *Let Σ be a linear system over R . The following statements are equivalent*

- 1) Σ is reachable.
- 2) The columns of $\Phi_\delta = (B \ AB \ \dots \ A^{\delta-1}B)$ generate R^δ .
- 3) The map $\phi: R^{k\delta} \rightarrow R^\delta$ given by multiplication by Φ_δ is residually surjective at each maximal ideal \mathfrak{m} of R .
- 4) The ideal $\mathcal{U}_\delta(\Phi_\delta)$ generated by the $\delta \times \delta$ minors of Φ_δ equals R .
- 5) The map $(zI - A, B) : R[z]^{\delta+k} \rightarrow R[z]^\delta$ is surjective.

Proof. 1 \Leftrightarrow 2, 3, 4) It follows from Theorem 2.3 in [1].

1 \Leftrightarrow 5) Σ is reachable \Leftrightarrow the map $\phi: R^{k\delta} \rightarrow R^\delta$ given by multiplication by Φ is residually surjective at each maximal ideal \mathfrak{m} of R ; that is, the map

$$\phi(\mathfrak{m}) : k(\mathfrak{m})^{k\delta} \rightarrow k(\mathfrak{m})^\delta$$

(where $k(\mathfrak{m}) = R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$ is the residue field of the ring R at the maximal ideal \mathfrak{m}) is surjective for each maximal ideal of $R \Leftrightarrow \Sigma(\mathfrak{m})$ is reachable for each $\mathfrak{m} \in \text{Spec}(R)$. Then, from Hautus Test, $\text{rank}(z_0I - A(\mathfrak{m}), B(\mathfrak{m})) = \delta$ for all $z_0 \in k(\mathfrak{m})$. So, by Proposition 2.8 of [4], the map

$$(zI - A(\mathfrak{m}), B(\mathfrak{m})) : k(\mathfrak{m})^{k+\delta} \rightarrow k(\mathfrak{m})^\delta$$

is surjective. Then, $(zI - A, B)$ is surjective over R . \square

We recall the following result regarding observability properties,

Proposition 2.2 (c.f. Theorem 2.6, [1]). *Let Σ be a linear system over R . The following statements are equivalent*

- 1) Σ is observable.
- 2) Let $\Omega_\delta = [C, CA, \dots, CA^{\delta-1}]^t$ be the observability matrix. The rank $(\Omega_\delta) = \delta$.
- 3) The map $\tau: R^\delta \rightarrow R^{p\delta}$ given by multiplication by Ω_δ is injective.
- 4) If $\mathcal{U}_\delta(\Omega_\delta)$ is the ideal of R generated by the $\delta \times \delta$ minors of Ω_δ , then, the annihilator of $\mathcal{U}_\delta(\Omega_\delta)$ is zero.

Due to the fact that a map can be injective without being residually injective we cannot complete Proposition 2.2 in a similar way that in Proposition 2.1. Since a residually injective homomorphism is always injective, the following result is a direct consequence of Theorem 2.7 [1]:

Proposition 2.3. *Let Σ be a linear system over R . If one of the following conditions is verified*

1. *The map*

$$\begin{pmatrix} zI - A \\ C \end{pmatrix} : R[z]^\delta \rightarrow R[z]^{\delta+p}$$

is residually injective,

2. *The dual system of Σ , that we will denote it by Σ^T is reachable,*

then, Σ is observable.

2.2. Convolutional codes and linear systems.

We are interested in the generalization of the relation between convolutional codes and linear systems given in [23, 25, 28]. In this case, a rate $\frac{k}{n}$ -convolutional code \mathcal{C} of degree δ over a finite field is a free submodule of $\mathbb{F}[z]^n$ of rank k . In the following, we use the notation of McEliece (see [18]) and we say that \mathcal{C} is a (n, k, δ) -convolutional code. This convolutional code \mathcal{C} can be described by an I/S/O representation $\Sigma^{\mathbb{F}} = (A, B, C, D)$, that is, a linear system defined as Equation (1) where $x_t \in \mathbb{F}^\delta$ is the state vector, $u_t \in \mathbb{F}^k$ is the information vector, $y_t \in \mathbb{F}^p$ is the parity vector and v_t is a codeword of \mathcal{C} for each time instant t . We assume that v_t is a finite-weight codeword (see [24]) and the code sequence has finite weight. Then, for a finite weight codeword both the input, the state and the output sequences need to have finite support. This I/S/O representation comes from a minimal first order representation in the following way: Every \mathcal{C} has a minimal first order representation (K, L, M) , a triple of matrices such that

$$\mathcal{C} = \{v(z) \in \mathbb{F}[z]^n \mid \exists x(z) \in \mathbb{F}[z]^\delta \text{ such that } (zK + L)x(z) + Mv(z) = 0\} \quad (2)$$

Moreover, we can make elementary transformations over the matrices (K, L, M) obtaining the triple of matrices $(\mathcal{K}, \mathcal{L}, \mathcal{M})$ such that $\text{Ker}(zK + L \mid M) \simeq \text{Ker}(z\mathcal{K} + \mathcal{L} \mid \mathcal{M})$ and it verifies that

$$\mathcal{K} = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, \mathcal{L} = \begin{pmatrix} A \\ C \end{pmatrix} \text{ and } \mathcal{M} = \begin{pmatrix} O & B \\ -I_{(n-k)} & D \end{pmatrix} \quad (3)$$

where the system $\Sigma^{\mathbb{F}} \in \mathcal{M}_{\delta \times \delta}(\mathbb{F}) \times \mathcal{M}_{\delta \times k}(\mathbb{F}) \times \mathcal{M}_{(n-k) \times \delta}(\mathbb{F}) \times \mathcal{M}_{(n-k) \times k}(\mathbb{F})$ is a reachable I/S/O representation of the convolutional code \mathcal{C} .

The finite weight convolutional code generated from the I/S/O representation is denoted by $\mathcal{C}(A, B, C, D)$. In this paper, we will denote it by $\mathcal{C}(\Sigma^{\mathbb{F}})$.

Remark 2.4. Note that the I/S/O representation of the code \mathcal{C} obtained as Equation (1) is different from the driving variable representation given in [21].

An essential property of convolutional codes over finite fields constructed by I/S/O representations as described in Equation (1) is the observability:

Definition 2.5 (c.f. Lemma 3.3.2, [28]). Let $\mathcal{C} \subset \mathbb{F}[z]^n$ be a (n, k, δ) convolutional code. It is observable if there exists a syndrome of Forner $\psi : \mathbb{F}[z]^n \rightarrow \mathbb{F}[z]^{n-k}$ such that $\text{Ker}(\psi) = \mathcal{C}$

Note that the above property is equivalent to say that a convolutional code \mathcal{C} is observable if the quotient $\mathbb{F}[z]^n/\mathcal{C}$ is a flat $\mathbb{F}[z]$ -module. Lemma 2.11 in [24] ensures us that if the pair of matrices (A, B) of an I/S/O representation Σ is reachable (controllable in coding literature), then, the observability of the pair (A, C) of the linear system is a necessary and sufficient condition in order to describe an observable convolutional code (non-catastrophic convolutional encoder).

Another important property verified by a convolutional code computed by I/S/O representation is that their encoders are rational and systematic (see [25]).

3. Concatenated linear systems over rings.

In this section, we describe different types of concatenation of systems over a commutative ring with identity R . The definition of serialized, systematic serialized and parallelized concatenated linear systems over rings is given generalizing the usual concatenation of linear systems over fields. In particular, we study concatenated linear systems over noetherian von Neumann regular rings.

3.1. Concatenated linear systems over rings.

Notation 3.1. 1. For the sake of notation, we denote a linear system over a ring R by $\Sigma_i^R = (A_i^R, B_i^R, C_i^R, D_i^R)$.

2. Since all the linear systems Σ^R of this section are over the ring R , we use Σ instead of Σ^R in the general case. We appoint specifically the ring in those cases that it is necessary as in the examples.

Definition 3.2. We consider the sets

$$\mathfrak{M}_1 = R^{\delta_1 \times \delta_1} \times R^{\delta_1 \times k} \times R^{(m-k) \times \delta_1} \times R^{(m-k) \times k}$$

$$\mathfrak{M}_2 = R^{\delta_2 \times \delta_2} \times R^{\delta_2 \times (m-k)} \times R^{(n-m+k) \times \delta_2} \times R^{(n-m+k) \times (m-k)}$$

Given the following couple of linear systems over R , $\Sigma_1 \in \mathfrak{M}_1$ and $\Sigma_2 \in \mathfrak{M}_2$, the serialized concatenation of Σ_1 and Σ_2 is defined by

$$\begin{aligned} \square_S: \mathfrak{M}_1 \times \mathfrak{M}_2 &\longrightarrow \mathfrak{M}_S \\ (\Sigma_1, \Sigma_2) &\longrightarrow \square_S(\Sigma_1, \Sigma_2) := \Sigma_{\square_S} = (A_S, B_S, C_S, D_S) \end{aligned}$$

where

$$\Sigma_{\square_S} = \left[\begin{pmatrix} A_1 & 0 \\ B_2 C_1 & A_2 \end{pmatrix}, \begin{pmatrix} B_1 \\ B_2 D_1 \end{pmatrix}, (D_2 C_1 \ C_2), (D_2 \cdot D_1) \right]$$

and $\mathfrak{M}_S = R^{(\delta_1 + \delta_2) \times (\delta_1 + \delta_2)} \times R^{(\delta_1 + \delta_2) \times k} \times R^{(n-m+k) \times (\delta_1 + \delta_2)} \times R^{(n-m+k) \times k}$.

Example 3.3. Let $\Sigma_1^{\mathbb{Z}_6}$ and $\Sigma_2^{\mathbb{Z}_6}$ be the following couple of linear systems over \mathbb{Z}_6

$$\begin{aligned} \Sigma_1^{\mathbb{Z}_6} &= \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 4 & 3 \end{pmatrix}, (5 \ 4), (0 \ 1) \right], \\ \Sigma_2^{\mathbb{Z}_6} &= \left[\begin{pmatrix} 4 & 1 \\ 5 & 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, (1 \ 1), (5) \right] \end{aligned}$$

If we compute $\square_S^{\mathbb{Z}_6}(\Sigma_1^{\mathbb{Z}_6}, \Sigma_2^{\mathbb{Z}_6}) = \Sigma_{\square_S}^{\mathbb{Z}_6}$, then, we get

$$\Sigma_{\square_S}^{\mathbb{Z}_6} = \left[\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & 4 & 1 \\ 2 & 4 & 5 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 4 & 3 \\ 0 & 5 \\ 0 & 4 \end{pmatrix}, (1 \ 2 \ 1 \ 1), (0 \ 5) \right]$$

Definition 3.4. We consider the set

$$\mathfrak{M}_3 = R^{\delta_2 \times \delta_2} \times R^{\delta_2 \times (m-k)} \times R^{(n-m) \times \delta_2} \times R^{(n-m) \times (m-k)}$$

Given the following couple of linear systems over R , $\Sigma_1 \in \mathfrak{M}_1$ and $\Sigma_2 \in \mathfrak{M}_3$, the systematic serialized concatenation of Σ_1 and Σ_2 is defined by

$$\begin{aligned} \square_{SS}: \mathfrak{M}_1 \times \mathfrak{M}_3 &\longrightarrow \mathfrak{M}_{SS} \\ (\Sigma_1, \Sigma_2) &\longrightarrow \square_{SS}(\Sigma_1, \Sigma_2) := \Sigma_{\square_{SS}} \end{aligned}$$

where

$$\Sigma_{\square_{SS}} = \left[\begin{pmatrix} A_1 & 0 \\ B_2 C_1 & A_2 \end{pmatrix}, \begin{pmatrix} B_1 \\ B_2 D_1 \end{pmatrix}, \begin{pmatrix} C_1 & 0 \\ D_2 C_1 & C_2 \end{pmatrix}, \begin{pmatrix} D_1 \\ D_2 \cdot D_1 \end{pmatrix} \right]$$

and $\mathfrak{M}_{SS} = R^{(\delta_1 + \delta_2) \times (\delta_1 + \delta_2)} \times R^{(\delta_1 + \delta_2) \times k} \times R^{(n-k) \times (\delta_1 + \delta_2)} \times R^{(n-k) \times k}$.

Definition 3.5. Let us consider the following sets

$$\begin{aligned} \mathfrak{M}_4 &= R^{\delta_1 \times \delta_1} \times R^{\delta_1 \times k} \times R^{(n-k) \times \delta_1} \times R^{(n-k) \times k} \\ \mathfrak{M}_5 &= R^{\delta_2 \times \delta_2} \times R^{\delta_2 \times k} \times R^{(n-k) \times \delta_2} \times R^{(n-k) \times k} \end{aligned}$$

Given the following couple of linear systems $\Sigma_1 \in \mathfrak{M}_4$ and $\Sigma_2 \in \mathfrak{M}_5$, the parallelized concatenation of Σ_1 and Σ_2 is defined by

$$\begin{aligned} \square_{\parallel}: \mathfrak{M}_4 \times \mathfrak{M}_5 &\longrightarrow \mathfrak{M}_{\parallel} \\ (\Sigma_1, \Sigma_2) &\longrightarrow \square_{\parallel}(\Sigma_1, \Sigma_2) := \Sigma_{\square_{\parallel}} \end{aligned}$$

where

$$\Sigma_{\square_{\parallel}} = \left[\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}, (C_1 \ C_2), (D_1 + D_2) \right]$$

$$\text{and } \mathfrak{M}_{\parallel} = R^{(\delta_1 + \delta_2) \times (\delta_1 + \delta_2)} \times R^{(\delta_1 + \delta_2) \times k} \times R^{(n-k) \times (\delta_1 + \delta_2)} \times R^{(n-k) \times k}.$$

A state diagram of parallelized concatenated linear system over R is shown in Figure 1.

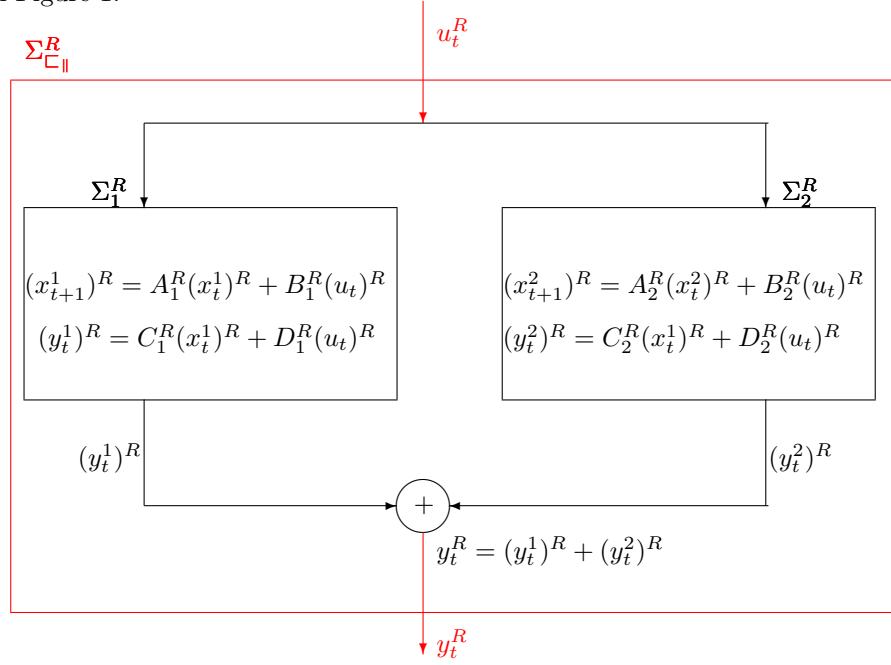


Fig. 1. Parallelized concatenated linear system over a ring

3.2. Concatenated linear systems over noetherian von Neumann regular rings.

We suppose that we have a concatenated linear system over a commutative ring with identity R . Then, someone may wonder if we can obtain concatenated linear systems over the ring by *patching* the restrictions of the system over the maximal ideals of the ring R . In this case, an interesting question is whether the operations of restricting and concatenating commute with each other. In another case, the order of operations in a network with such systems could affect both security and other parameters. The key point to solve these questions is to know when a ring decomposes into the product of its residue fields. The biggest class of rings in which this is verified is the class of the noetherian von Neumann regular rings.

Let R be a noetherian von Neumann regular ring. We recall some algebraic preliminaries about the ring R that will be used in the sequel.

R is zero dimensional and noetherian, and so, R is an artinian reduced ring, and then, $\text{Spec}(R)$ is a finite set of prime ideals. Moreover, every prime ideal is maximal, thus $\text{Spec}(R) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_t\}$. We denote $\mathbb{F}_j := R/\mathfrak{m}_j$. Moreover, we use the notation I_j for the ideal generated by all components except \mathbb{F}_j ; that is, $I_j = \mathbb{F}_1 \times \dots \times \mathbb{F}_{j-1} \times \mathbb{F}_{j+1} \times \dots \times \mathbb{F}_t$. Then, we have the following exact sequence for each $j = 1, \dots, t$

$$0 \rightarrow I_j \xrightarrow{i_j} R \xrightarrow{\pi_j} \mathbb{F}_j \rightarrow 0$$

We consider the canonical isomorphism φ_{rs}

$$\begin{aligned} \varphi_{rs} : \mathbb{F}_1^{r \times s} \times \dots \times \mathbb{F}_t^{r \times s} &\rightarrow R^{r \times s} \\ (M_1, \dots, M_t) &\mapsto \varphi(M_1, \dots, M_t) := M = (m_{ij}) \end{aligned}$$

where

$$M_l \equiv M \pmod{I_l} \text{ and } m_{ij}^l \equiv m_{ij} \pmod{I_l}$$

and m_{ij}^l is the ij -th component of the matrix M_l and $l = 1, \dots, t$.

Remark 3.6. a) If $r = s$, then φ_{rr} is a morphism of rings.

b) To avoid confusion, we will write φ for all maps φ_{rs} .

c) We will also use φ to denote $\varphi(\Sigma^{\mathbb{F}_1}, \dots, \Sigma^{\mathbb{F}_t}) = \Sigma^R$.

Theorem 3.7. *Let R be a noetherian von Neumann regular ring. Let Σ_1 and Σ_2 be a couple of linear systems over R . Then*

$$\sqsubset_*^R (\Sigma_1, \Sigma_2) = (\varphi \circ \sqsubset_*)[(\Sigma_1^{\mathbb{F}_1}, \Sigma_2^{\mathbb{F}_1}), \dots, (\Sigma_1^{\mathbb{F}_t}, \Sigma_2^{\mathbb{F}_t})]$$

where $\Sigma_1^R = \varphi(\Sigma_1^{\mathbb{F}_1}, \dots, \Sigma_1^{\mathbb{F}_t})$, $\Sigma_2^R = \varphi(\Sigma_2^{\mathbb{F}_1}, \dots, \Sigma_2^{\mathbb{F}_t})$ and $*$ denotes the type of concatenation (serialized, systematic serialized or parallelized).

Proof. We are going to show the theorem with the serialized concatenation. An analogous argument is performed with the another types of concatenation.

Let $\sqsubset_{\square_s}^R$ be a serialized concatenated system over R . We can understand $\Sigma_{\square_s}^R$ as the composition of the maps $\sqsubset_S^R \circ \varphi$ in the following way

$$\begin{aligned} \Sigma_{\square_s}^R &= \sqsubset_S^R (\Sigma_1^R, \Sigma_2^R) = \sqsubset_S^R [(A_1^R, B_1^R, C_1^R, D_1^R), (A_2^R, B_2^R, C_2^R, D_2^R)] = \\ &= \sqsubset_S^R \left[\left(\varphi(A_1^{\mathbb{F}_1}, \dots, A_1^{\mathbb{F}_t}), \varphi(B_1^{\mathbb{F}_1}, \dots, B_1^{\mathbb{F}_t}), \varphi(C_1^{\mathbb{F}_1}, \dots, C_1^{\mathbb{F}_t}), \varphi(D_1^{\mathbb{F}_1}, \dots, D_1^{\mathbb{F}_t}) \right), \right. \\ &\quad \left. \left(\varphi(A_2^{\mathbb{F}_1}, \dots, A_2^{\mathbb{F}_t}), \varphi(B_2^{\mathbb{F}_1}, \dots, B_2^{\mathbb{F}_t}), \varphi(C_2^{\mathbb{F}_1}, \dots, C_2^{\mathbb{F}_t}), \varphi(D_2^{\mathbb{F}_1}, \dots, D_2^{\mathbb{F}_t}) \right) \right] \end{aligned}$$

In addition, it is possible to compose the maps $(\varphi \circ \sqsubset_S)[(\Sigma_1^{\mathbb{F}_1}, \Sigma_2^{\mathbb{F}_1}), \dots, (\Sigma_1^{\mathbb{F}_t}, \Sigma_2^{\mathbb{F}_t})]$ and construct the system $(\tilde{A}_S^R, \tilde{B}_S^R, \tilde{C}_S^R, \tilde{D}_S^R)$ where

$$\begin{aligned}
\tilde{A}_S^R &= \varphi(A^{\mathbb{F}_1}, \dots, A^{\mathbb{F}_t}) = \varphi \left[\left(\begin{array}{cc} A_1^1 & \\ B_2^1 C_1^1 & A_2^1 \end{array} \right), \dots, \left(\begin{array}{cc} A_1^t & \\ B_2^t C_1^t & A_2^t \end{array} \right) \right] = \\
&= \left(\begin{array}{cc} \varphi(A_1^1, \dots, A_1^t) & 0 \\ \varphi(B_2^1 C_1^1, \dots, B_2^t C_1^t) & \varphi(A_2^1, \dots, A_2^t) \end{array} \right) \\
\tilde{B}_S^R &= \varphi(B^{\mathbb{F}_1}, \dots, B^{\mathbb{F}_t}) = \varphi \left[\left(\begin{array}{c} B_1^1 \\ B_2^1 D_1^1 \end{array} \right), \dots, \left(\begin{array}{c} B_1^t \\ B_2^t D_1^t \end{array} \right) \right] = \left(\begin{array}{c} \varphi(B_1^1, \dots, B_1^t) \\ \varphi(B_2^1 D_1^1, \dots, B_2^t D_1^t) \end{array} \right) \\
\tilde{C}_S^R &= \varphi(C^{\mathbb{F}_1}, \dots, C^{\mathbb{F}_t}) = \varphi[(D_2^1 C_1^1 \quad C_2^1), \dots, (D_2^t C_1^t \quad C_2^t)] = \\
&= \varphi(D_2^1 C_1^1, \dots, D_2^t C_1^t), \varphi(C_2^1, \dots, C_2^t) \\
\tilde{D}_S^R &= \varphi(D^{\mathbb{F}_1}, \dots, D^{\mathbb{F}_t}) = \varphi(D_2^1 D_1^1, \dots, D_2^t D_1^t)
\end{aligned}$$

Since φ is a morphism of rings, the following equalities prove that $\Sigma_{\square_s}^R$ is equal to $(\tilde{A}_S^R, \tilde{B}_S^R, \tilde{C}_S^R, \tilde{D}_S^R)$

$$\varphi(B_2^1 C_1^1, \dots, B_2^t C_1^t) = \varphi(B_2^1, \dots, B_2^t) \cdot \varphi(C_1^1, \dots, C_1^t) \quad (4)$$

$$\varphi(B_2^1 D_1^1, \dots, B_2^t D_1^t) = \varphi(B_2^1, \dots, B_2^t) \cdot \varphi(D_1^1, \dots, D_1^t) \quad (5)$$

$$\varphi(D_2^1 C_1^1, \dots, D_2^t C_1^t) = \varphi(D_2^1, \dots, D_2^t) \cdot \varphi(C_1^1, \dots, C_1^t) \quad (6)$$

$$\varphi(D_2^1 D_1^1, \dots, D_2^t D_1^t) = \varphi(D_2^1, \dots, D_2^t) \cdot \varphi(D_1^1, \dots, D_1^t), \quad (7)$$

and we conclude the proof. Note that the equalities to verify are the same as in the case of systematic serialized concatenation. In the case of parallelized concatenation, it suffices to observe that

$$\varphi(D_1^1 + D_2^1, \dots, D_1^t + D_2^t) = \varphi(D_1^1, \dots, D_1^t) + \varphi(D_2^1, \dots, D_2^t)$$

and, it is also verified because φ is a morphism of rings. \square

Example 3.8. Let R be the integer modular ring \mathbb{Z}_6 . Let $(\Sigma_1^{\mathbb{Z}_2}, \Sigma_2^{\mathbb{Z}_2})$ and $(\Sigma_1^{\mathbb{Z}_3}, \Sigma_2^{\mathbb{Z}_3})$ be the following linear systems

$$\Sigma_1^{\mathbb{Z}_2} = \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, (1 \quad 0), (0 \quad 1) \right],$$

$$\Sigma_2^{\mathbb{Z}_2} = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, (1 \quad 1), (1) \right],$$

$$\Sigma_1^{\mathbb{Z}_3} = \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, (2 \quad 1), (0 \quad 1) \right]$$

$$\Sigma_2^{\mathbb{Z}_3} = \left[\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, (1 \quad 1), (2) \right]$$

Firstly, we compute $\square_S (\Sigma_1^{\mathbb{Z}_i}, \Sigma_2^{\mathbb{Z}_i})$, for $i = 2, 3$ and we get

$$\square_S (\Sigma_1^{\mathbb{Z}_2}, \Sigma_2^{\mathbb{Z}_2}) = \Sigma_{\square_S}^{\mathbb{Z}_2} = \left[\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, (0 \ 1) \right]$$

and

$$\square_S (\Sigma_1^{\mathbb{Z}_3}, \Sigma_2^{\mathbb{Z}_3}) = \Sigma_{\square_S}^{\mathbb{Z}_3} = \left[\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 \\ 2 & 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \\ 0 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, (0 \ 2) \right]$$

Note that $\varphi(\Sigma_{\square_S}^{\mathbb{Z}_2}, \Sigma_{\square_S}^{\mathbb{Z}_3})$ is equal to $\Sigma_{\square_S}^{\mathbb{Z}_6}$ that is described in Example 3.3. On the other hand we can compute the following systems

$$\begin{aligned} \varphi(\Sigma_1^{\mathbb{Z}_2}, \Sigma_1^{\mathbb{Z}_3}) &= \Sigma_1^{\mathbb{Z}_6} = \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 4 & 3 \end{pmatrix}, (5 \ 4), (0 \ 1) \right], \\ \varphi(\Sigma_2^{\mathbb{Z}_2}, \Sigma_2^{\mathbb{Z}_3}) &= \Sigma_2^{\mathbb{Z}_6} = \left[\begin{pmatrix} 4 & 1 \\ 5 & 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, (1 \ 1), (5) \right], \end{aligned}$$

If we perform $\square_S (\Sigma_1^{\mathbb{Z}_6}, \Sigma_2^{\mathbb{Z}_6})$ then obtain the same result than $\Sigma_{\square_S}^{\mathbb{Z}_6}$. The state diagram of this example is shown in Figure 2.

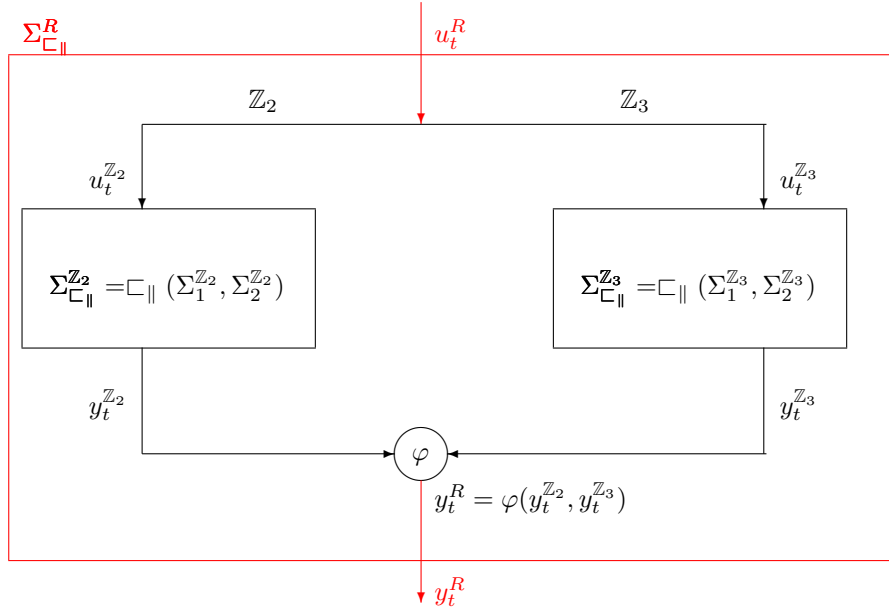


Fig. 2. Performance of a parallelized concatenated linear system over \mathbb{Z}_6

4. Control properties of concatenated linear systems over rings.

Let R be a commutative ring with identity. We are going to study the sufficient and necessary conditions to get reachable and observable concatenated linear systems over R .

Notation 4.1. Since the ring R is fixed in this section, we use the notation Σ instead of Σ^R in the general case. We will appoint the ring in another cases.

4.1. Reachability.

We are interested in obtaining conditions to get reachable concatenated linear systems over a ring R .

By Proposition 2.1, a concatenated linear system over R , Σ_{\square_*} , where $*$ denotes the type of concatenation (serialized/systematic serialized/parallelized), is reachable if the following map

$$(zI - A_*, B_*) : R[z]^{\delta_1 + \delta_2 + k} \rightarrow R[z]^{\delta_1 + \delta_2}$$

is surjective where

$$(zI - A_S, B_S) = \begin{pmatrix} zI_{\delta_1} - A_1 & O & B_1 \\ -B_2 C_1 & zI_{\delta_2} - A_2 & B_2 D_1 \end{pmatrix}$$

is the matrix of the map in the case of serialized concatenation and

$$(zI - A_{\parallel}, B_{\parallel}) = \begin{pmatrix} zI_{\delta_1} - A_1 & O & B_1 \\ O & zI_{\delta_2} - A_2 & B_2 \end{pmatrix}.$$

is the matrix of the map in the parallelized concatenation case.

Remark 4.2. Since the study of reachability properties of concatenated linear systems depends on the conditions over the pair of matrices (A, B) , and the serialized and systematic serialized concatenations are equal over this pair of matrices, we refer by $* = S$ to both types of concatenation (\square_S and \square_{SS}).

The first question to solve is if we can get global conditions of reachability for concatenated linear systems over a ring R from local properties of reachability and viceversa. From Proposition 2.1, it can be said that Σ_{\square_*} is a reachable linear system over R if and only if $\Sigma_{\square_*}(\mathfrak{m})$ is a reachable system for each maximal ideal $\mathfrak{m} \in \text{Spec}(R)$.

Example 4.3. Let $\Sigma_1^{\mathbb{Z}_6}$ and $\Sigma_2^{\mathbb{Z}_6}$ be the following linear systems

$$\Sigma_1^{\mathbb{Z}_6} = \left[\begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, (1 \ 0), (5) \right]$$

and

$$\Sigma_2^{\mathbb{Z}_6} = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, (0 \ 1), (5) \right]$$

The parallelized concatenated system is defined by

$$\Sigma_{\square_{\parallel}}^{\mathbb{Z}_6} = \left[A_{\parallel}^{\mathbb{Z}_6} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, B_{\parallel}^{\mathbb{Z}_6} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, C_{\parallel}^{\mathbb{Z}_6} = (1 \ 0 \ 0 \ 1), D_{\parallel}^{\mathbb{Z}_6} = (4) \right]$$

We can verify that $\Sigma_{\square_{\parallel}}^{\mathbb{Z}_6}$ is reachable because

$$|\Phi_4| = \left| \begin{array}{cccc} B_{\parallel}^{\mathbb{Z}_6} & A_{\parallel}^{\mathbb{Z}_6} B_{\parallel}^{\mathbb{Z}_6} & (A_{\parallel}^{\mathbb{Z}_6})^2 B_{\parallel}^{\mathbb{Z}_6} & (A_{\parallel}^{\mathbb{Z}_6})^3 B_{\parallel}^{\mathbb{Z}_6} \end{array} \right| = \begin{vmatrix} 0 & 1 & 0 & 1 \\ 1 & 5 & 1 & 5 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix} = 5$$

and so, $\mathcal{U}_4 = \langle 5 \rangle = \mathbb{Z}_6 = R$.

The maximal ideals of \mathbb{Z}_6 are $\mathfrak{m}_1 = (2)$ and $\mathfrak{m}_2 = (3)$. So, $\Sigma_{\square_{\parallel}}^{\mathbb{Z}_6}(\mathfrak{m}_1) = \Sigma_{\square_{\parallel}}^{\mathbb{Z}_2}$ and $\Sigma_{\square_{\parallel}}^{\mathbb{Z}_6}(\mathfrak{m}_2) = \Sigma_{\square_{\parallel}}^{\mathbb{Z}_3}$ are

$$\Sigma_{\square_{\parallel}}^{\mathbb{Z}_2} = \left[A_{\parallel}^{\mathbb{Z}_2} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, B_{\parallel}^{\mathbb{Z}_2} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, C_{\parallel}^{\mathbb{Z}_2} = (1 \ 0 \ 0 \ 1), D_{\parallel}^{\mathbb{Z}_2} = (0) \right]$$

and

$$\Sigma_{\square_{\parallel}}^{\mathbb{Z}_3} = \left[A_{\parallel}^{\mathbb{Z}_3} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, B_{\parallel}^{\mathbb{Z}_3} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, C_{\parallel}^{\mathbb{Z}_3} = (1 \ 0 \ 0 \ 1), D_{\parallel}^{\mathbb{Z}_3} = (1) \right]$$

The linear systems $\Sigma_{\square_{\parallel}}^{\mathbb{Z}_2}$ and $\Sigma_{\square_{\parallel}}^{\mathbb{Z}_3}$ are reachable because

$$\text{rank} \begin{pmatrix} B_{\parallel}^{\mathbb{Z}_2} & A_{\parallel}^{\mathbb{Z}_2} B_{\parallel}^{\mathbb{Z}_2} & (A_{\parallel}^{\mathbb{Z}_2})^2 B_{\parallel}^{\mathbb{Z}_2} & (A_{\parallel}^{\mathbb{Z}_2})^3 B_{\parallel}^{\mathbb{Z}_2} \end{pmatrix} = \text{rank} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = 4$$

$$\text{rank} \begin{pmatrix} B_{\parallel}^{\mathbb{Z}_3} & A_{\parallel}^{\mathbb{Z}_3} B_{\parallel}^{\mathbb{Z}_3} & (A_{\parallel}^{\mathbb{Z}_3})^2 B_{\parallel}^{\mathbb{Z}_3} & (A_{\parallel}^{\mathbb{Z}_3})^3 B_{\parallel}^{\mathbb{Z}_3} \end{pmatrix} = \text{rank} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 2 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = 4$$

Now, the natural question is what conditions have to verify the systems to concatenate in order to get reachable concatenated linear systems over a ring R . For example, we can consider the following reachable dynamical linear systems over \mathbb{Z}_2

$$\Sigma_1^{\mathbb{Z}_2} = [A_1 = (1), B_1 = (1), C_1 = (1), D_1 = (1)]$$

and

$$\Sigma_2^{\mathbb{Z}_2} = [A_2 = (0), B_2 = (1), C_2 = (1), D_2 = (1)]$$

However, the serialized concatenated linear system $\Sigma_{\square_S}^{\mathbb{Z}_2}$ given by

$$\Sigma_{\square_S}^{\mathbb{Z}_2} = \left[\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, (1 \quad 1), (1) \right]$$

is not reachable.

Remark 4.4. In the case of serialized (and systematic serialized) concatenation, if the systems to concatenate are reachable, then, the following maps

$$\begin{aligned} (zI_{\delta_1} - A_1, B_1) : R[z]^{\delta_1+k} &\rightarrow R[z]^{\delta_1} \\ (zI_{\delta_2} - A_2, B_2) : R[z]^{\delta_2+m-k} &\rightarrow R[z]^{\delta_2} \end{aligned}$$

are surjective. So, if $k \geq \delta_1 + \delta_2$, it would be enough that the following map

$$\begin{pmatrix} B_1 \\ B_2 D_1 \end{pmatrix} : R[z]^k \rightarrow R[z]^{\delta_1+\delta_2} \quad (8)$$

is surjective in order to get a reachable system over R .

However, the condition $k \geq \delta_1 + \delta_2$ on the dimensions of the matrices of the system could be too restrictive in terms of the applications of concatenated linear systems. Since we have properties that ensure the reachability of a concatenated linear system over a finite field (see [27]), the question is whether we can generalize them to all type of rings.

We denote by $\Lambda(M)$ the set of eigenvalues of a matrix M .

Proposition 4.5. *Let Σ_1 and Σ_2 be linear systems over a commutative ring with identity R . Suppose that $\Sigma_1(\mathfrak{m})$ and $\Sigma_2(\mathfrak{m})$ are reachable for all maximal ideal $\mathfrak{m} \in \text{Spec}(R)$.*

1. *If the following conditions are verified:*
 - i) $\Lambda(A_1(\mathfrak{m})) \cap \Lambda(A_2(\mathfrak{m})) = \emptyset$ or all maximal ideal \mathfrak{m} of $\text{Spec}(R)$.
 - ii) $G_1(z)$, the transfer matrix of $(A_1(\mathfrak{m}), B_1(\mathfrak{m}), C_1(\mathfrak{m}), D_1(\mathfrak{m}))$, has full row rank for $z \notin \Lambda(A_1(\mathfrak{m}))$, then Σ_{\square_S} is a reachable serialized concatenated linear system over R .
2. *If $\Lambda(A_1(\mathfrak{m})) \cap \Lambda(A_2(\mathfrak{m})) = \emptyset$ for all maximal ideal \mathfrak{m} of $\text{Spec}(R)$, then $\Sigma_{\square_{\parallel}}$ is a reachable parallelized concatenated linear system over R .*

Proof. If conditions 1i) and 1ii) are verified for each pair $\Sigma_1(\mathfrak{m})$ and $\Sigma_2(\mathfrak{m})$ for all $\mathfrak{m} \in \text{Spec}(R)$, then, by Proposition 3.3.1 in [27], the concatenated linear system $\Sigma_{\square_S}(\mathfrak{m})$ is reachable. Then, Σ_{\square_S} is residually reachable for each maximal ideal of $\text{Spec}(R)$ and so, by Proposition 2.1, we conclude that Σ_{\square_S} is a reachable linear system. In the case of the condition 2), by Proposition 3.3.3 in [27], we conclude the proof. \square

It is important to recall that the conditions of item 1) of the above Proposition are also verified when the system is systematic serialized concatenated.

Example 4.6. Let $\Sigma_1^{\mathbb{Z}_4}$ and $\Sigma_2^{\mathbb{Z}_4}$ be the following linear systems

$$\Sigma_1^{\mathbb{Z}_4} = \left[\begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}, (1 \ 0), (1) \right]$$

and

$$\Sigma_2^{\mathbb{Z}_4} = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, (0 \ 1), (3) \right]$$

The parallelized concatenated linear system $\sqsubset_S (\Sigma_1^{\mathbb{Z}_4}, \Sigma_2^{\mathbb{Z}_4})$ is defined by

$$\Sigma_{\sqsubset}^{\mathbb{Z}_4} = \left[A_{\sqsubset}^{\mathbb{Z}_4} = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, B_{\sqsubset}^{\mathbb{Z}_4} = \begin{pmatrix} 0 \\ 3 \\ 3 \\ 0 \end{pmatrix}, C_{\sqsubset}^{\mathbb{Z}_4} = (1 \ 0 \ 0 \ 1), D_{\sqsubset}^{\mathbb{Z}_4} = (0) \right]$$

Since the only maximal ideal of \mathbb{Z}_4 is $\mathfrak{m} = (2)$, by Proposition 4.5, we assure that $\Sigma_{\sqsubset}^{\mathbb{Z}_4}$ is reachable because

$$\wedge(A_1(2)) = \wedge \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right] = \{1\}$$

and

$$\wedge(A_2(2)) = \wedge \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right] = \{0\}$$

We can verify that $\Sigma_{\sqsubset}^{\mathbb{Z}_4}$ is reachable because

$$|\Phi_4| = \begin{vmatrix} B_{\sqsubset}^{\mathbb{Z}_4} & A_{\sqsubset}^{\mathbb{Z}_4} B_{\sqsubset}^{\mathbb{Z}_4} & (A_{\sqsubset}^{\mathbb{Z}_4})^2 B_{\sqsubset}^{\mathbb{Z}_4} & (A_{\sqsubset}^{\mathbb{Z}_4})^3 B_{\sqsubset}^{\mathbb{Z}_4} \end{vmatrix} = \begin{vmatrix} 0 & 3 & 2 & 1 \\ 3 & 1 & 3 & 1 \\ 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{vmatrix} = 3$$

and so, $\mathcal{U}_4 = \langle 3 \rangle = \mathbb{Z}_4 = R$.

4.2. Observability.

Let Σ be a linear system over R . By Propositions 2.2 and 2.3, Σ is observable if

$$\begin{pmatrix} zI - A \\ C \end{pmatrix} : R[z]^\delta \rightarrow R[z]^{\delta+p} \quad (9)$$

is injective.

In the case of concatenated linear systems over a ring R ,

i) If the following map

$$\begin{pmatrix} zI - A_S \\ C_S \end{pmatrix} = \begin{pmatrix} zI_{\delta_1} - A_1 & O \\ -B_2C_1 & zI_{\delta_2} - A_2 \\ D_2C_1 & C_2 \end{pmatrix} : R[z]^{\delta_1 + \delta_2} \rightarrow R[z]^{\delta_1 + \delta_2 + n - m + k}$$

is injective, then, Σ^{\square_S} is an observable serialized concatenated system.

ii) If the following map

$$\begin{pmatrix} zI - A_{SS} \\ C_{SS} \end{pmatrix} = \begin{pmatrix} zI_{\delta_1} - A_1 & O \\ -B_2C_1 & zI_{\delta_2} - A_2 \\ C_1 & 0 \\ D_2C_1 & C_2 \end{pmatrix} : R[z]^{\delta_1 + \delta_2} \rightarrow R[z]^{\delta_1 + \delta_2 + n - k}$$

is injective, then, $\Sigma^{\square_{SS}}$ is an observable systematic serialized concatenated system.

iii) If the following map

$$\begin{pmatrix} zI - A_{\parallel} \\ C_{\parallel} \end{pmatrix} = \begin{pmatrix} zI_{\delta_1} - A_1 & 0 \\ 0 & zI_{\delta_2} - A_2 \\ C_1 & C_2 \end{pmatrix} : R[z]^{\delta_1 + \delta_2} \rightarrow R[z]^{\delta_1 + \delta_2 + n - k}$$

is injective, then, $\Sigma^{\square_{\parallel}}$ is an observable parallelized concatenated system.

We highlight some conditions to make sure that we obtain observable concatenated linear systems over a commutative ring R .

Lemma 4.7. *Let Σ_{\square_*} be a concatenated linear system over R . If $\Sigma_{\square_*}(\mathfrak{m})$ is an observable linear system for each maximal ideal $\mathfrak{m} \in \text{Spec}(R)$, then Σ_{\square_*} is an observable concatenated linear system.*

Proof. If $\Sigma_{\square_*}(\mathfrak{m})$ is an observable system, then, its dual system $[\Sigma_{\square_*}(\mathfrak{m})]^T$ is reachable (Theorem 2.9 in [1]). Then, $[\Sigma_{\square_*}]^T$ is reachable and, by Theorem 2.7 in [1], Σ_{\square_*} is an observable linear system. \square

Remark 4.8. If R is a ring that is equal to its quotient ring, then, the Duality Theorem 2.9 in [1] is verified and Σ_{\square_*} is observable if and only if the maps $\begin{pmatrix} zI - A(\mathfrak{m}) \\ C(\mathfrak{m}) \end{pmatrix} : k(\mathfrak{m})^{\delta} \rightarrow k(\mathfrak{m})^{\delta + m}$ are injective for each maximal ideal $\mathfrak{m} \in \text{Spec}(R)$. So, Σ^{\square_*} is an observable concatenated system over R if and only if its dual system is a reachable linear system.

Another question to solve is what conditions have to verify the systems we want to concatenate in order to obtain an observable concatenated linear system.

Proposition 4.9. *Let Σ_1 and Σ_2 be linear systems over a commutative ring with identity R . Suppose that $\Sigma_1(\mathfrak{m})$ and $\Sigma_2(\mathfrak{m})$ are observable linear systems for all maximal ideal $\mathfrak{m} \in \text{Spec}(R)$.*

1. If the following conditions are verified:
 - i) $\Lambda(A_1(\mathfrak{m})) \cap \Lambda(A_2(\mathfrak{m})) = \emptyset$ for all maximal ideal \mathfrak{m} of $\text{Spec}(R)$.
 - ii) B_2 has full row rank,
 then, $\Sigma^{\square_s^R}$ is an observable serialized concatenated linear system.
2. If $\Lambda(A_1(\mathfrak{m})) \cap \Lambda(A_2(\mathfrak{m})) = \emptyset$ for all maximal ideal \mathfrak{m} of $\text{Spec}(R)$, then, $\Sigma^{\square_{\parallel}^R}$ is an observable parallelized concatenated linear system.

Proof. If the above conditions are verified by Proposition 3.4.1, Proposition 3.4.3 and Theorem 3.4.5 in [27], $\Sigma_{\square_*}(\mathfrak{m})$ is an observable linear system for all maximal ideal $\mathfrak{m} \in \text{Spec}(R)$. By Lemma 4.7, we conclude the proof. \square

Remark 4.10. Note that if $\Sigma_1(\mathfrak{m})$ and $\Sigma_2(\mathfrak{m})$ are observable linear systems for all maximal ideal $\mathfrak{m} \in \text{Spec}(R)$, then, $\Sigma^{\square_{ss}^R}$ is always an observable systematic serialized concatenated linear system without more necessary conditions.

5. Construction of concatenated families of convolutional codes over noetherian von Neumann regular rings.

In this section, we first give a brief overview of the basic definition of families of convolutional codes over a commutative ring with identity (see [4] and [6]). Moreover, we describe the relation of families of convolutional codes and linear systems over noetherian von Neumann regular rings by minimal first order and I/S/O representations. This approach let us to construct observable families of convolutional codes over this class of rings.

5.1. Basic definitions.

Definition 5.1 (cf. Definition 4.1.1, [6]). A rate (n, k) convolutional code over R is a submodule $\mathfrak{C} \subset R[z]^n$ such that $R[z]^n/\mathfrak{C}$ is R -flat and $\text{rank}(\mathfrak{C})(\mathfrak{p}) = k$ for any prime ideal of $\text{Spec}(R)$.

The above definition allows us to understand a convolutional code over R as a family of convolutional codes parametrized by $\text{Spec}(R)$: that it is, \mathfrak{C} over a ring R gives rise a convolutional code over every residue field by means of $\{\mathfrak{C} \otimes_R k(\mathfrak{p})\}_{\mathfrak{p} \in \text{Spec}(R)}$.

Definition 5.2 (cf. Definition 4.1.2, [6]). We say that \mathfrak{C} has degree δ if $\delta(\mathfrak{p}) = \delta$ for all $\mathfrak{p} \in \text{Spec}(R)$.

Remark 5.3. In this setting, the complexity, or the degree, of \mathfrak{C} is no longer an integer but a function $\delta : \text{Spec}(R) \rightarrow \mathbb{N}$. In the rest of the paper, we will assume that the degree function δ is a constant.

The definition of the generator matrix and the encoder of a family of convolutional codes over a ring is extended following the classical case.

Definition 5.4 (cf. Definition 4.1.3 and 4.1.4, [6]). A generator matrix $G(z)$ of a (n, k, δ) -family of convolutional codes \mathfrak{C} over R is given by a matrix

$$\begin{aligned} G(z) : R[z]^l &\longrightarrow R[z]^n \\ u(z) &\mapsto v(z) = G(z) \cdot u(z) \end{aligned}$$

such that $\text{Im } G(z) = \mathfrak{C}$ where $l \leq k$. An encoder $G(z)$ of \mathfrak{C} is a generator matrix with $l = k$ and $G(z)$ injective.

We extend the classical definition of observable convolutional code to rings:

Definition 5.5 (cf. Definition 4.1.5, [6]). Let $\mathfrak{C} \subset R[z]^n$ be a (n, k, δ) -family of convolutional codes over R . We say that \mathfrak{C} is observable if the quotient $R[z]^n / \mathfrak{C}$ is flat over $R[z]$.

5.2. Families of convolutional codes over noetherian von Neumann regular rings.

In the following, we fix a noetherian von Neumann regular ring R . It is known that every R -module is flat. Thus, a morphism between finitely generated R -module is injective if and only if is residually injective. If we consider a (n, k, δ) -family of convolutional codes over R , then, $\mathfrak{C} \simeq \bigoplus_{j=1}^t \mathcal{C}_j$ where \mathcal{C}_j is a (n, k, δ) -convolutional code over \mathbb{F}_j . Then, \mathfrak{C} is observable if and only if \mathcal{C}_j is observable $\forall j$ [cf. Proposition 4.1.3, [6]].

The extension of the relation between convolutional codes and linear systems by minimal first order and I/S/O representations to noetherian von Neumann regular rings is developed in [4] and [6] and it is due to the ring R is a product ring. Let \mathfrak{C} be a family of convolutional codes over R . We suppose that the triple (K_j, L_j, M_j) is a minimal first order representation of $\mathcal{C}_j \subseteq \mathbb{F}_j[z]^n$ for each \mathbb{F}_j . We can construct matrices (K, L, M) over R by φ in the way $K_j \simeq K(\text{mod } I_j)$, $L_j \simeq L(\text{mod } I_j)$ and $M_j \simeq M(\text{mod } I_j)$. These matrices (K, L, M) form a minimal and unique first order representation of \mathfrak{C} over R (see Theorem 4.2.4, Corollary 4.2.5 and Theorem 4.2.6 in [6]). Finally, we can construct an I/S/O representation Σ over R from (K, L, M) or by patching the systems $\Sigma_j^{\mathbb{F}_j}$ obtained as in Equation (3) for each \mathbb{F}_j (Theorem 4.3.2 and Proposition 4.3.4 in [6]).

Notation 5.6. In the case that Σ is a reachable linear system over R , we will denote by $\mathfrak{C}(\Sigma)$ the family of convolutional codes that is constructed taking Σ as a minimal I/S/O representation of \mathfrak{C} .

Let \mathfrak{C} be a (n, k, δ) -family of convolutional codes over R . Let Σ be its associated minimal I/S/O representation. Then, the following statements are verified:

1. Σ is a reachable linear system (Proposition 4.3.6 in [6]).
2. Σ is a locally Brunovsky linear system (Theorem 4.3.7 in [6]).
3. If Σ is observable then, $\mathfrak{C}(\Sigma)$ is an observable family of convolutional codes (Proposition 4.3.8. in [6]).

5.3. *Concatenated families of convolutional codes over noetherian von Neumann regular rings.*

In coding theory, concatenated codes are a class of codes that are obtained by combining an inner code, \mathfrak{C}_i , and an outer code \mathfrak{C}_o .

Definition 5.7. Let \mathfrak{C} be a (n, k, δ) - family of convolutional codes over a noetherian von Neumann regular ring R . We say that $\mathfrak{C}(\Sigma_{\square_*}^R)$ is a concatenated family of convolutional codes.

The first question to solve is when a linear system over the ring R can be considered as a minimal representation of a concatenated family of convolutional codes over the ring R . By, [4] and [6], all concatenated linear system that verifies reachability conditions will be a minimal concatenated I/S/O representation and, so, it provides us with a concatenated family of convolutional codes over R , $\mathfrak{C}(\Sigma_{\square_*}^R)$. Note that all concatenated linear system verifying reachability conditions described in Section IV will be useful in this question.

Remark 5.8. Note that the condition $k \geq \delta_1 + \delta_2$ of Remark 4.4, from convolutional codes point of view, restricts our results to a finite number of convolutional codes (most of them, block codes because δ_1 and δ_2 represents the memories of the codes).

The choice of the type of concatenation in the reachable concatenated linear system gives us concatenated families of convolutional codes with different parameters.

1. If the outer code $\mathfrak{C}_o(\Sigma_1^R)$ is a (m, k, δ_1) - code and the inner code $\mathfrak{C}_i(\Sigma_2^R)$ is a $(n, m - k, \delta_2)$ code, then $\mathfrak{C}(\Sigma_{\square_s}^R)$ is a $(n - m + 2k, k, \delta_1 + \delta_2)$ - serialized concatenated family of convolutional codes.
2. If the outer code $\mathfrak{C}_o(\Sigma_1^R)$ is a (n, k, δ_1) -family of convolutional codes and the inner code $\mathfrak{C}_i(\Sigma_2^R)$ is a $(n, m - k, \delta_2)$ family of convolutional codes, then $\mathfrak{C}(\Sigma_{\square_{ss}}^R)$ is a $(n + k, k, \delta_1 + \delta_2)$ - systematic serialized concatenated family of convolutional codes.
3. If the outer code $\mathfrak{C}_o(\Sigma_1^R)$ is a (n, k, δ_1) -family of convolutional codes and the inner code $\mathfrak{C}_i(\Sigma_2^R)$ is a (n, k, δ_2) family of convolutional codes, then $\mathfrak{C}(\Sigma_{\square_{||}}^R)$ is a $(n, k, \delta_1 + \delta_2)$ - parallelized concatenated family of convolutional codes.

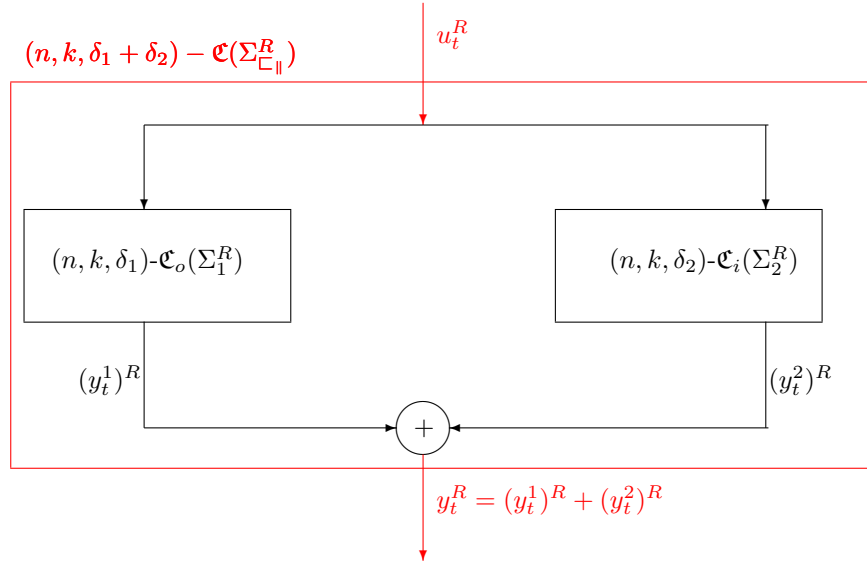


Fig.3. Parallelized concatenated convolutional code over the ring R

Example 5.9. We consider the linear systems $\Sigma_1^{\mathbb{Z}_6}$, $\Sigma_2^{\mathbb{Z}_6}$ and $\Sigma_{C||}^{\mathbb{Z}_6}$ given in Example 4.3. We recall the last one in order to clarify this example,

$$\Sigma_{C||}^{\mathbb{Z}_6} = \left(A_{||}^{\mathbb{Z}_6} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, B_{||}^{\mathbb{Z}_6} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, C_{||}^{\mathbb{Z}_6} = (1 \ 0 \ 0 \ 1), D_{||}^{\mathbb{Z}_6} = (4) \right)$$

The above system is reachable and so, we can consider it as a minimal I/S/O representation of a $(n = 2, k = 1, \delta = 4)$ -parallelized concatenated family of convolutional codes. Then, the minimal first order representation of $\Sigma_{C||}^{\mathbb{Z}_6}$ is

$$K_{||}^{\mathbb{Z}_6} = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix}, L_{||}^{\mathbb{Z}_6} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, M_{||}^{\mathbb{Z}_6} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \\ 5 & 4 \end{pmatrix}$$

and the encoder of the concatenated family $\mathfrak{C}_{||}^{\mathbb{Z}_6}$ is

$$G(z)_{||}^{\mathbb{Z}_6} = \begin{pmatrix} 2z^4 + 2z^2 + 4 \\ 5z^4 + z^2 \end{pmatrix}$$

Moreover, we are able to construct observable concatenated families of convolutional codes over R from a reachable concatenated linear systems if a necessary condition is verified:

Lemma 5.10. *If $\Sigma_{\mathbb{C}_*}^R$ is reachable and observable, then $\mathfrak{C}(\Sigma_{\mathbb{C}_*}^R)$ is an observable concatenated family of convolutional codes.*

Proof. By Proposition 4.3.8 in [6] we conclude the proof. \square

Finally, since $\mathfrak{C}(\Sigma_{\mathbb{C}_*}^R) \simeq \bigoplus \mathfrak{C}(\Sigma_{\mathbb{C}_*}^{\mathbb{F}_j})$, we can construct (observable) concatenated families of convolutional codes over the ring R by reachable (and observable) concatenated linear systems (I/S/O representations) over the ring, or by patching concatenated linear systems over each \mathbb{F}_j . From the point of view of a network of convolutional codes, if $\varphi(\Sigma_1^{\mathbb{Z}_2}, \Sigma_1^{\mathbb{Z}_3}) = \Sigma_1^{\mathbb{Z}_6}$ and $\varphi(\Sigma_2^{\mathbb{Z}_2}, \Sigma_2^{\mathbb{Z}_3}) = \Sigma_2^{\mathbb{Z}_6}$, the scheme given in Figure 3 behaves in a similar way to the representation in Figure 4.

6. Conclusions.

Concatenated convolutional codes are used to detect, correct and hide information. Recent advances, in parallelized and serial concatenation, are being implemented in the construction of turbo codes and steganographic schemes in order to improve the transmission of data.

We have generalized the relation between concatenated families of convolutional codes and linear systems over certain commutative rings. Moreover, we have studied the necessary conditions to get I/S/O representations (reachable linear systems) and observable concatenated families of convolutional codes over finite rings.

Future work is focused on the generalization of concatenation of convolutional codes over other types of rings and the extension of other types of concatenations.

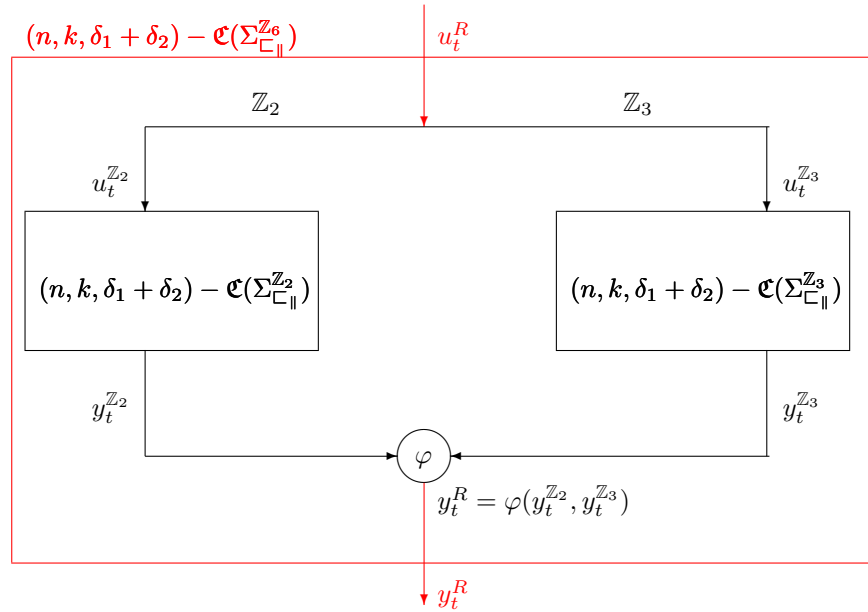


Fig. 4. Parallelized concatenated family of convolutional codes over \mathbb{Z}_6

7. References

- [1] J. W. Brewer, J. W. Bunce, F. S. Van Vleck, *Linear Systems over commutative Rings*, Marcel Dekker, New York, 1986.
- [2] J-J. Climent, V. Herranz, C. Perea, A first approximation of concatenated convolutional codes from linear systems theory viewpoint, *Linear Algebra Appl.*, 425 (23), (2007), 673-699.
- [3] J-J. Climent, V. Herranz, C. Perea, Linear system modelization of concatenated block and convolutional codes, *Linear Algebra Appl.*, 429, (2008), 1191-1212.
- [4] M.V. Carriegos, N. DeCastro-García, A. Muñoz Castañeda, Kernel representations of convolutional codes over rings, Preprint available in <https://arxiv.org/pdf/1609.05043v1.pdf>
- [5] C. Chen, Construction of linear ring codes for 6 PSK, *IEEE Transactions of Information Theory*, 40 (2), (2002), 563 - 566.
- [6] N. DeCastro- García, Feedback equivalence in linear systems and convolutional codes. Applications to Cybernetics, Coding and Cryptography, Ph. D. Dissertation, Universidad de León, Spain, 2016.
- [7] F. Fagnani, S. Zampieri, System-theoretic properties of convolutional codes over rings, *IEEE Trans. Inform. Theory*, 47, (2001), 2256-2274 .
- [8] G.D. Forney Jr., *Concatenated Codes*, MIT Press, Cambridge, MA, 1966.
- [9] M.I. García-Planas, M.I., S. Tarragona, Analysis of functional output-controllability of time-invariant Composite linear systems, *Recent advances in systems, control and informatics*, WSEAS Press, (2013), 40-47.
- [10] M. I. García-Planas, J. L. Domínguez-García, L. E. Um, Sufficient Conditions for Controllability and Observability of Serial and Parallel Concatenated Linear Systems, *Int. J. of circuits, systems and signal processing*, 8, (2014), 622-630,
- [11] R. Johannesson, Z. Wan, and E. Wittenmark. Some structural properties of convolutional codes over rings, *IEEE Trans. Inform. Theory*, 44 (2), (1998), 839 - 845.
- [12] H. Jouhari and E. M. Souidi. Improving Embedding Capacity by using the Z4-linearity of Preparata Codes. *Int J Comput Appl.*, 2012, 53, 18, 1-6.
- [13] R.E. Kalman, Algebraic structure of linear dynamical systems; I. The module of Σ , *Proc. Nat. Acad. Sci.*, 54, (1965), 1503 - 1508.
- [14] E. W. Kamen, Linear systems over rings: From R. E. Kalman to the present, in *Mathematical System Theory-The Influence of R. E. Kalman* (A. C. Antoulas, Ed.), Springer-Verlag, Berlin, (1991), 311-324.
- [15] M. Kuijper, R. Pinto, On minimality of convolutional ring encoders, *IEEE Trans. on Inform. Theory*, 55 (11), (2009), 4890-4897.

- [16] Kuijper, M., R. Pinto, J. W. Polderman, and P. Rocha, Autonomicity and the absence of free variables for behaviors over finite rings, *Proc. 7th Portuguese Conf. Autom. Control*, Lisbon, Portugal (2006).
- [17] S. Mahapakulchai and R. Van Dyck, , Design of ring convolutional trellis codes for MAP decoding of MPEG-4 images, *IEEE Trans. Commun.*, 2004, 52, 7, 1033 -1037.
- [18] R.J. McEliece, The algebraic theory of convolutional codes, in: V. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, vol. I, Elsevier, Amsterdam, 1998, 10651138.
- [19] J.L. Massey and T. Mittelholzer. Convolutional codes over rings, in *Proc. Joint Swedish-Soviet Int. Workshop on Inform. Theory*, Gotland, Sweden, (1989), 14-18.
- [20] J.L. Massey and T. Mittelholzer. Systematicity and rotational invariance of convolutional codes over rings. *In Proc. Int. Workshop on Alg. and Combinatorial Coding Theory*, pp. 154-158, Leningrad, (1990).
- [21] J.L. Massey, M.K. Sain, Codes, automata and continuous systems: explicit interconnections, *IEEE Trans. Automat. Control*, 12 (6), (1967) 644650.
- [22] Y. Rouchaleau, Linear discrete - time, finite-dimensional, dynamical systems over some classes of commutative rings, PhD. Dissertation, Stanford University, March 1972.
- [23] J. Rosenthal, Connections between linear systems and convolutional codes, in: B. Marcus, J. Rosenthal (Eds.), *Codes, Systems and Graphical Models*, IMA, vol. 123, Springer Verlag, Berlin, (2001), 3966.
- [24] J. Rosenthal, E. V. York, BCH Convolutional Codes, *IEEE Trans. on Inform. Theory*, 45 (6), (1999), 1833-1844.
- [25] J. Rosenthal, J. M. Schumacher, and E. V. York, On behaviors and convolutional codes, *IEEE Trans. on Inform. Theory*, 42 (6), (1996), 1881-1891.
- [26] E. D. Sontag, Linear systems over commutative rings: A survey , *Richerche Automat.* 7, (1976), 1-34.
- [27] L. E. Um, A contribution to the theory of convolutional codes from systems theory point of view . PhD Dissertation Universitat Politècnica de Catalunya (2015). Available in [http : //hdl.handle.net/10803/317953](http://hdl.handle.net/10803/317953).
- [28] E. V. York, *Algebraic description and construction of error correcting codes, a systems theory point of view.*, Ph.D. dissertation, Univ. Notre Dame, 1997. [Online].
- [29] E. Zerz, On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings, *Asian Journ. Control*, 12 (2), (2010), 119-126.