Open Mathematics

Research Article

Noemí DeCastro-García*

Feedback equivalence of convolutional codes over finite rings

https://doi.org/10.1515/math-2017-0124
Received November 14, 2016; accepted October 20, 2017.

Abstract: The approach to convolutional codes from the linear systems point of view provides us with effective tools in order to construct convolutional codes with adequate properties that let us use them in many applications. In this work, we have generalized feedback equivalence between families of convolutional codes and linear systems over certain rings, and we show that every locally Brunovsky linear system may be considered as a representation of a code under feedback convolutional equivalence.

Keywords: Convolutional codes, Linear systems, Feedback equivalence, Finite rings, Coding theory

MSC: 94B10, 93C05, 13C10, 93B20

1 Introduction

Convolutional codes are a powerful tool that is used to correct digital data. These error correcting codes are applied in numerous situations such as the communications with the deep space, the mobile communications or the hard decision codes. Regarding cybersecurity, convolutional codes are applied in several areas in order to improve the efficiency and security of different processes. For instance, these codes are used in cryptography to construct cryptosystems (see [1]). They are also employed in [2] as an alternative scheme that avoids the need for global connection in the modeling of networks by trellis representations. On the other hand, concatenated convolutional codes, developed in [3], have been strongly exploited when it is necessary to transmit and hide sensitive information. Recent advances in parallel and serial concatenated convolutional codes focus on their implementation in the construction of turbo codes.

The connection between linear systems and convolutional codes over finite fields has been studied from different points of view depending on the approach to convolutional codes that is being used (see [4]). The available representations let us describe the dynamics of the encoders of the codes or constructing convolutional codes with certain good properties such as observability. Recently, the study of convolutional codes over finite fields has been developed through these relations based on first order representations and input/state/output (I/S/O) representations and references therein [5–8].

Although the study of error-correcting codes initially started over finite fields, the research of codes over rings has increased due to the applications and properties of these codes. For example, in [9] an encoder over $\mathbb{Z}/4\mathbb{Z}$ is developed for decoding MPEG-4 images. Recently, in [10], a steganographic protocol has been performed based on convolutional codes over the ring $\mathbb{Z}/4\mathbb{Z}$.

Convolutional codes over rings were introduced by Massey and Mittleholzer in [11] and [12]. They also focused on the study of minimal and systematic encoders over rings. However, convolutional codes over rings do not behave in the same way as convolutional codes over fields because their behavior depends strongly

*Corresponding Author: Noemí DeCastro-García: Departamento de Matematicas, Campus de Vegazana, 24071, Universidad de León, León, Spain, E-mail: ncasg@unileon.es

© 2017 DeCastro-García, published by De Gruyter Open. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.
on the structure of the underlying ring. The study of properties, encoders, \( p \)-basis and dual convolutional codes over finite rings, has been developed in [13–16] among others. In [17], a bound on the free distance of convolutional codes over \( \mathbb{Z}_p \) was developed generalizing the results described in [7]. A construction of nonfree MDS convolutional codes over \( \mathbb{Z}_p \) is also given in [18] with new upper-bounds on the free distance.

The extension of the duality between linear systems and convolutional codes is not easily generalized to all commutative rings with identity. It depends strongly on the ring and the realization theory that we will want to extend. This paper is based on the generalization given in [19, 20] of the theory studied in [21–23] about the connection between linear systems (reachable input/state/output representations) and convolutional codes (with finite support). The extension developed in [19, 20] let us construct observable families of convolutional codes over a finite ring \( R \). We consider noetherian von Neumann regular rings: that is, finite products of fields. In particular, we suppose that \( R \simeq F_1 \times F_2 \times \ldots \times F_t \simeq \oplus_{j=1}^t F_j \) where \( F_j \) is a finite field.

More precisely, these families of convolutional codes over \( R \) allow us to construct an algebraic system of simultaneous signal encoding in linear coding networks over the ring \( R \), improving the security of the system. This system lets us send the same message \( m \) encoded over the ring \( R \) to several receivers and every receiver decodes its message \( \mu_j \) over \( F_j = R/m_j \) where \( m_j \) is the \( j \)-th maximal ideal in the spectrum of \( R \). In this situation, if the messages over \( F_j \) are shared, it would be possible to create the original message that we assume unique: \( m = (\mu_1, \ldots, \mu_t) \). In this case, a finite base of \( t \) communication systems is used, so that the message is encoded over the ring \( R \) (see Figure 1). Moreover, a continuous net among receivers is not needed.

In cybersecurity framework, this multicast encoding could be applied to effective coding in the cloud where many agents would use the same cloud resources to different purposes and several scripts.

![Fig. 1. Diagram of communications](image)

On the other hand, feedback equivalence of linear systems over commutative rings is one of the main holistic matters in science and engineering (see [24–26]). Two linear systems are feedback equivalent if one can transform one into the other by changes of coordinates together with feedback loops. Regarding equivalence relations in coding literature, due to the fact that a convolutional code can have many encoders, most works on the topic are focused on the study of equivalence relations between encoders of the same convolutional code: that is, the study of the conditions in which two encoding matrices are equivalent, and thus they generate the same code (see [4] for a general overview). In the theory of block codes over finite fields, MacWilliams stated that linear block codes are related by weight-preserving isomorphism (see [27]). However, the weight enumerator does not form a complete invariant under monomial equivalence. In [28], a generalization of the above theory for certain convolutional codes over finite fields is given by making use of classical realization theory (driving representation of the code). They proved that all minimal realizations of a given code are feedback equivalent in the sense that the adjacency matrix of reduced encoders turns into an invariant of the code. Regarding linear codes over finite Frobenius rings, the theorem of monomial equivalence of MacWilliams is extended in [29].

In this paper, we use the study of feedback isomorphisms of linear systems over commutative rings (see [30–32]) to define a feedback convolutional equivalence for families of convolutional codes over a noetherian von Neumann regular ring \( R \). The key is that the set of Kronecker indices of both objects (partitions of the rank of the state space of the system and the complexity of the code) forms a complete family of invariant elements
under feedback isomorphism. Moreover, the relation between locally Brunovsky linear systems and families of convolutional codes over $R$ by I/S/O representations allows us to know how many equivalence classes of families of convolutional codes there are with the same Kronecker’s indices; i.e. with the same degree under feedback convolutional equivalence. Note that this feedback equivalence relation is valid in the case of finite fields.

This paper is organized as follows: In Section 2 we give the related work with the basic results of linear systems, convolutional codes and the relation between them. In Section 3 we give our main results supported by examples. Finally, we give the conclusions, future work and references.

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 of convolutional codes over finite fields and their connection with linear systems. Finally, we give an overview of the theory of families of convolutional codes over rings and the I/S/O representation considered in this paper.

2.1 Linear systems and feedback isomorphisms 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

$$
\begin{align*}
  x_{t+1} &= Ax_t + Bu_t \\
  y_t &= Cx_t + Du_t,
\end{align*}
$$

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

The generalization of linear systems over a commutative ring with identity $R$ starts from considering a triple $\Sigma = (X, f, B)$ where $X$ is an $R$-module of rank $\delta$ (state space of the system), $f : X \to X$ is an endomorphism of $X$, and $B$ is a finitely generated submodule of $X$ (see [26]). When $X \simeq R^\delta$, then a pair of matrices $(A, B) \in R^{\delta \times \delta} \times R^{\delta \times k}$ gives a linear map as the one described above by the assignment

$$(A, B) \mapsto (R^\delta, A, B := \text{Im}(B))$$

and thus, we can consider the dynamical system $\Sigma = (A, B)$ over $R$.

We review some results about reachability (controllability from the origin) properties of linear systems over $R$. In the case of time-invariant systems, the reachability of a system refers to the ability of the system to reach $x_1$ from the origin in some finite time. We review the main characterization of the reachability of a time-invariant linear system in terms of the pair $(A, B)$.

**Proposition 2.1** (c.f. [25] and [33]). Let $\Sigma$ be a linear system over $R$. The following statements are equivalent

1) $\Sigma$ is reachable.
2) The columns of $\Phi_\delta = \begin{pmatrix} B & AB & \cdots & A^{\delta-1}B \end{pmatrix}$ generate $R^\delta$.
3) The map $\Phi : R^{k\delta} \to R^\delta$ given by multiplication by $\Phi_\delta$ is residually surjective at each maximal ideal $m$ of $R$.
4) The ideal $\mathfrak{I}_\delta(\Phi_\delta)$ generated by the $\delta \times \delta$ minors of $\Phi_\delta$ equals $R$.
5) The map $(zI - A, B) : R[z]^{\delta \times k} \to R[z]^\delta$ is surjective (generalization of Hautus Test).

State observability is the ability to determine the state vector of the system knowing the input and the corresponding output over some finite time interval. The following result describes observability properties in terms of the pair of matrices $(A, C)$ of the system.
Kronecker’s Indices

We compute the invariant indices using the indices.

Let invariant elements is, in some cases, easier than the direct computation. We can use Young’s diagram.

Table 1.

Therefore, \( \delta \times \delta \) minors of \( \Omega_\delta \), then, the annihilator of \( \cup_\delta(\Omega_\delta) \) is zero.

On the other hand, it is known that two linear systems over a field \( \mathbb{K} \) are feedback equivalent when they have a similar feedback dynamical behavior (they have the same feedback invariant elements).

By [34] and [35], feedback classification of dynamical linear systems over a field \( \mathbb{K} \) becomes the feedback classification of reachable systems and thus, we can compute the number of feedback equivalence classes of dynamical linear systems over a \( \delta \)-dimensional \( \mathbb{K} \)-vectorial space, \( fe_\mathbb{K}(\delta) \), by the classification of reachable systems. The number of feedback classes of \( \delta \)-dimensional reachable systems over \( \mathbb{K} \) may be computed by using the indices \( \{\xi_1, \xi_2, \ldots, \xi_p\} \) where

\[
\xi_1 = \text{rk}(B) \text{ and } \xi_i = \text{rk}(B, AB, \ldots, A^{i-1} B) - \text{rk}(B, AB, \ldots, A^{i-2} B). \tag{2}
\]

The set of indices described in Equation (2) is a complete family of invariants of reachable systems under the group of feedback transformations. If we reorder them, then they are equal to the Kronecker’s minimal column indices for the matrix pencil \((zI - A, B)\) associated to \(\Sigma\). We denote them by \( \mathcal{K}^\Sigma = \{\kappa_1, \ldots, \kappa_p\} \). The set \( \mathcal{K}^\Sigma \) is called the set of control invariants of \(\Sigma\). Moreover, Kronecker indices \( \{\kappa_1 \preceq \kappa_2 \preceq \ldots \preceq \kappa_p\} \) form an ordered partition of the integer \( \delta \), the dimension of the system; that is, \( \delta = \kappa_1 + \ldots + \kappa_p \). And then, \( fe_\mathbb{K}(\delta) \) is equal to the number of partitions of the integer \( \delta \), \( p_\mathbb{K}(\delta) \).

We recall that both sets of indices \( \{\xi_i\} \) and \( \{\kappa_i\} \) are conjugated with each other (see [35]). Note that computing the Kronecker’s indices of a dynamical linear system by the computation of the conjugated invariant elements is, in some cases, easier than the direct computation. We can use Young’s diagram.

Example 2.3. Let \(\Sigma\) be the following linear system over \(\mathbb{Z}/2\mathbb{Z}\):

\[
\Sigma = [A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ C = \begin{pmatrix} 1 & 1 \\ \end{pmatrix}, \ D = \begin{pmatrix} 0 & 1 \end{pmatrix}].
\]

We compute the invariant indices \(\xi_1\) and \(\xi_2\)

\[
\xi_1 = \text{rk}(B) = \text{rk} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1 \text{ and } \xi_2 = \text{rk}(B AB) = \text{rk} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = 2 - 1 = 1.
\]

Therefore, \(\mathcal{K}^\Sigma = (1, 1)\). We can represent these indices by the Young’s diagram and thus, we transpose the diagram in order to compute the Kronecker indices, then \( \mathcal{K}^\Sigma = (k_1, k_2) = (2, 0)\), see Table 1.

Table 1. Kronecker’s indices in \(\mathbb{Z}/2\mathbb{Z}\) by Young’s diagrams.

| Conjugate Kronecker’s Indices | Kronecker’s Indices |
|------------------------------|---------------------|
| \(\xi_1\) | \(\xi_2\) |
| \(\kappa_1\) | \(\kappa_2\) |

Definition 2.4 ([32]). Let \(\Sigma\) and \(\Sigma^\prime\) be a couple of linear systems over \(R\). \(\Sigma\) is feedback isomorphic with \(\Sigma^\prime\) \(\Leftrightarrow\) there exists an isomorphism \(\phi : X \to X^\prime\) such that \(\phi(B) = B^\prime\) and \(\text{Im}(\phi f - f^\prime \phi) \subset B^\prime\).
The existence of feedback invariants for $\Sigma$ is studied in [30–32], for a specific type of systems: locally Brunovsky linear systems (systems having locally a Brunovsky Canonical Form). In this case, the invariant modules $N_i = B + f(N_{i-1})$, $M_i = X/N_i$ and $I_i = N_i/N_{i-1}$ are extended to the invariant modules $Z_i = \text{Ker}(I_i \to I_{i+1})$ which form a complete family of invariant elements.

Moreover, in [32] it is proved that the classes of feedback isomorphisms of locally Brunovsky linear systems with state space $X$, a projective finitely generated $R$-module of constant rank $\delta$, is in bijective correspondence with the set of solutions of the following linear equation

$$X \simeq Z_1 \oplus (Z_2)^2 \oplus \cdots \oplus (Z_k)^k \oplus \cdots,$$  \hspace{1cm} (3)

in $\mathbf{P}(R)$, the monoid of isomorphism classes of finitely generated projective $R$-modules. Therefore we can compute the number of classes of feedback isomorphisms of locally Brunovsky linear systems with state space $X$, $fe_R(m)$ (where $m$ denotes the class of isomorphisms of $X$ in $\mathbf{P}(R)$) by

$$fe_R(m) = \# \{ \text{Solutions of the equation (3) in the abelian monoid } (\mathbf{P}(R), \oplus) \}.$$  

If the monoid is cancellative, the invariant modules $I_i^R \cong Z_i^R \oplus I_{i+1}^R$ classify too, and then,

$$fe_R(m) = \# \{ \text{Solutions of the equation } I_1 \oplus I_2 \oplus \ldots \oplus I_k \text{ in the abelian monoid } (\mathbf{P}(R), \oplus) \}.$$  

**Remark 2.5.** If we consider linear systems over a noetherian von Neumann regular ring $R$, by Proposition 4.2 in [36], we can perform the computation of the number of classes of feedback isomorphisms of locally Brunovsky linear systems over $R$ where $X \simeq R^k$, which is equal to $fe_R(m) = fe_R(\delta) = [p_\delta(\delta)]^{\mathit{Spec}(R)}$.

In the case of linear systems over commutative rings, we recall that $\xi_i = \dim(N_i^R) - \dim(N_{i-1}^R)$ and we can obtain another set of invariants $\zeta_i = \dim(Z_i) = \xi_i - \xi_{i-1}$ (see [32]).

If $R$ is a von Neumann regular ring, we also have available a characterization of the ring $R$ in terms of reachability and locally Brunovsky properties of linear systems over the ring.

**Theorem 2.6** (cf. Theorem 3.2 in [36]). Let $R$ be a commutative ring with identity. Let $\Sigma$ be a linear system over $R$ where $X$ is a finitely generated $R$-module. Then the following are equivalent

i) $R$ is a von Neumann regular ring.

ii) $\Sigma$ is reachable if and only if $\Sigma$ is a locally Brunovsky linear system.

### 2.2 Convolutional codes and linear systems

In literature regarding codes, one can find different definitions for a convolutional code over a finite field that are related, in different ways, with linear systems, see [4]. We have available the linear algebra point of view in which a convolutional code is a linear subspace and its associated linear system was given by Massey and Sain (see [37] and [38]). It is known as driving input/output representation. Another approach to convolutional codes over finite fields is the symbolic dynamics point of view. In this case, a convolutional code is a linear compact irreducible and shift invariant subset of $\mathbb{F}[z, z^{-1}]$ and the relation with linear systems is given in [39], among others. Also, convolutional codes can be defined as a class of time-invariant and complete behavior in the sense of Willems [40], and there is a realization theory too (see [41, 42]).

We are interested in the module-theoretical approach of convolutional codes that requires that the codewords have finite support (see [43]). We consider that a rate $\frac{k}{n}$ convolutional code $C$ of degree $\delta$ over a finite field is a free submodule of $\mathbb{F}[z]^{[n \times k]}$ of rank $k$. In the following, we use the notation of McEliece and we say that $C$ is an $(n, k, \delta)$ convolutional code (see [37]). With this point of view a convolutional code $C$ can be described by an I/S/O representation $\Sigma^C = (A, B, C, D)$; i.e. a reachable linear system over the finite field. Moreover, if we consider a reachable and observable linear system $\Sigma$ over a finite field, then we obtain an observable convolutional code that is usually denoted by $C(A, B, C, D)$ (see [21, 22]). In the sequel, we denote it by $\hat{C}(\Sigma)$. 


The above relation is extended to noetherian von Neumann regular rings in [19, 20]. We are going to recall the main results of this generalization:

An \((n, k)\)-family of convolutional codes over a commutative ring \(R, \mathcal{C}\), is a free submodule \(\mathcal{C} \subset R[z]^n\) of rank \(k\), and such that \(R[z]^n/\mathcal{C}\) is flat over \(R\). In this case, we can consider families of convolutional codes, one of each prime ideal \(p\) in \(\text{Spec}(R)\). The above definition allows us to understand a convolutional code over \(R\) as a family of convolutional codes parametrized by \(\text{Spec}(R)\): that is, \(\mathcal{C}\) over a ring \(R\) give rise to a convolutional code over every residue field of \(R\). Moreover, we have that an encoder for an \((n, k)\)-family of convolutional codes \(\mathcal{C}\) over \(R\) is a matrix

\[
G(z) : R[z]^k \to R[z]^n
\]

\[
u(z) \mapsto \nu(z) = G(z)u(z)
\]

such that \(\text{Im} \ G(z) = \mathcal{C}\) and \(G(z)\) is injective.

**Definition 2.7.** Let \(R\) be a commutative ring with identity. \(G(z)\) is a systematic encoder if there exists a unimodular matrix \(T(z) \in R(z)^{k \times k}\) such that

\[
G(z) \cdot T(z) = \begin{pmatrix} G'(z) \\ \text{Id}_k \end{pmatrix},
\]

where \(G'(z) \in R(z)^{(n-k) 	imes k}\). The encoder \(G(z)\) is systematic if we can find a \(k \times k\) minor in \(G(z), W(z)\), such that \(W(z) \in \text{Units}(R(z))\).

**Remark 2.8.** If we can consider a systematic encoder for a family of convolutional codes \(\mathcal{C}\), then all encoder of the family of codes will be systematic and thus, we say that \(\mathcal{C}\) is a systematic family of convolutional codes.

Let \(\mathcal{C} \subset R[z]^n\) be an \((n, k)\)-family of convolutional codes over \(R\) and let \(p \in \text{Spec} \ R\) be a prime ideal. Since \(R[z]^n/\mathcal{C}\) is \(R\)-flat, the reduction of \(\mathcal{C}\) modulo \(p\), \(\mathcal{C}(p) := \mathcal{C}/p\mathcal{C}\), is an \((n, k)\)-convolutional code over \(k(p) := R_p/pR_p\). For each \(p\), we denote by \(\delta(p)\) the degree of \(\mathcal{C}(p)\). Thus, in this setting the degree of the family \(\mathcal{C}\) is no longer an integer but a function

\[
\delta : \text{Spec}(R) \to \mathbb{N}.
\]

**Definition 2.9.** Fix \(\delta \in \mathbb{N}\). A family of convolutional codes over \(R, \mathcal{C}\), is said to be of degree \(\delta\) if its degree function (4) is constant and equal to \(\delta\).

In the sequel, we focus on an \((n, k, \delta)\) · systematic family of convolutional codes, \(\mathcal{C}\), over a noetherian von Neumann regular ring \(R\). Since \(R\) is zero dimensional and noetherian, \(\text{Spec}(R)\) is a finite set of prime ideals. Moreover, every prime ideal is maximal and then \(\text{Spec}(R) = \{m_1, \ldots, m_r\}\). We denote \(F_j := R/m_j\). Thus we can consider an \((n, k, \delta)\) convolutional code, \(\mathcal{C}_j\), over each \(F_j\).

**Remark 2.10.**

1. The condition imposed over \(\text{Coker}(G(z))\) of being \(R\)-flat can be translated into some algebraic conditions on the entries of \(G(z)\). However, in case \(R\) is a von Neumann regular ring these conditions are superfluous, since every \(R\)-module is flat, i.e., in this case, any encoder \(G(z)\) satisfies this condition.

2. Note that if \(G(z)\) is a systematic encoder of \(\mathcal{C}\) in \(R\), then the encoders of each \(\mathcal{C}_j, G_j(z)\), are systematic too. The inverse does not hold true, in general.

By [19, 20] there exists a unique triple of matrices \((K, L, M) \in R^{(\delta+n-k) \times \delta} \times R^{(\delta+n-k) \times \delta} \times R^{(\delta+n-k) \times n}\) defining a first order representation of the code such that

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

and satisfying that the code is described by \(\text{Ker}(zK + L|M) \simeq \mathcal{C}\).

Moreover, the above matrices satisfy minimality conditions:
1. $K$ has column full size rank.
2. $(K \mid M)$ has row full size rank.
3. Map $(zK + L \mid M)$ defined by $(zK + L \mid M) : R[z]^{d \times n} \to R[z]^{d \times n-k}$ is surjective.

From the above representation, we also have available an input/state/output (I/S/O) representation that describes the code as a reachable linear system: We can make elementary operations over $(K, L, M)$ and obtain $(\mathcal{K}, \mathcal{L}, \mathcal{M})$ such that

$$\mathcal{K} = \begin{pmatrix} -I_{\delta} & 0 \\ O & C \end{pmatrix}, \quad \mathcal{L} = \begin{pmatrix} A \\ C \end{pmatrix} \quad \text{and} \quad \mathcal{M} = \begin{pmatrix} O & B \\ -I_{(n-k)} & D \end{pmatrix},$$

(6)

where $\Sigma^c \in R^{\delta \times \delta} \times R^{\delta \times k} \times R^{(n-k)\times \delta} \times R^{(n-k)\times k}$, and it verifies that

$$\text{Ker}(zK + L \mid M) \simeq \text{Ker}(z\mathcal{K} + \mathcal{L} \mid \mathcal{M}).$$

The matrices $A$, $B$, $C$ and $D$ over $R$ define a representation of the code as a controllability state spaces linear system from Equation (5) to

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

(7)

where $x_t \in R^\delta$ is the state vector, $u_t \in R^k$ is the information vector, $y_t \in R^p$ 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 and the code sequence has finite weight. Note that this I/S/O representation is different from the driving representation given in [38].

**Notation.** If we denote by $I_j$ the ideal generated by all components in which $R$ decomposes except $\mathbb{F}_j$; that is, $I_j = \mathbb{F}_1 \times \ldots \times \mathbb{F}_{j-1} \times \mathbb{F}_{j+1} \times \ldots \times \mathbb{F}_t$, then we have the following exact sequence for each $j = 1, \ldots, t$

$$0 \to I_j \to R \to \mathbb{F}_j \to 0.$$

Then we denote by $\varphi_{rs}$ the canonical isomorphism

$$\varphi_{rs} : \mathbb{F}_1^{rs} \times \ldots \times \mathbb{F}_t^{rs} \to R^{rs},$$

$$(M_1, \ldots, M_t) \to \varphi(M_1, \ldots, M_t) := M = (m_{ij}),$$

where

$$M_i \equiv M(\text{mod } I_j) \text{ and } m_{ij} \equiv m_{ij}(\text{mod } I_j)$$

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

**Remark 2.11.** Note that the triple of matrices $(K, L, M)$ can be constructed through $\varphi_{rs}$ by taking $K_j \equiv K(\text{mod } I_j)$, $L_j \equiv L(\text{mod } I_j)$ and $M_j \equiv M(\text{mod } I_j)$ where $(K_j, L_j, M_j)$ is a minimal first order representation of $\mathcal{C}_j$ for each $\mathbb{F}_j$.

In a similar way, we can obtain $\Sigma^c$ over $R$ by patching $\Sigma^c$, the I/S/O representations of the convolutional codes $\mathcal{C}_j$ over each $\mathbb{F}_j$.

Regarding control properties, by Proposition 2.1 the minimality condition 3) of the first order representation of a family of convolutional codes is actually equivalent to say that $\Sigma^c$ is a reachable linear system.

**Remark 2.12.** By [21] every $\Sigma_j$ is a reachable linear system over $\mathbb{F}_j$. Thus, $\Sigma$ over $R$ is residually surjective. By Proposition 2.1, $\Sigma$ is reachable over $R$. 
In addition, if \( \Sigma^C = (A, B)^C \) is the dynamical part of an I/S/O representation of a family of convolutional codes, \( \mathcal{C} \), over \( R \), then \( \Sigma^C \) is a locally Brunovsky linear system over \( R \) by \([36]\). So it verifies all properties of feedback isomorphism of linear systems described in Subsection 2.1.

An essential property of convolutional codes over finite fields constructed by I/S/O representations as described in Equation (7) is the observability:

**Definition 2.13** (c.f. Lemma 3.3.2, [23]). Let \( \mathcal{C} \subseteq \mathbb{F}[z]^n \) be an \((n, k, \delta)\)-convolutional code. It is observable if there exists a syndrome Former \( \psi : \mathbb{F}[z]^n \to \mathbb{F}[z]^{n-k} \) 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 [22] ensures that \( \mathcal{C}(\Sigma) \) is observable (non-catastrophic convolutional encoder) if and only if \( \Sigma^C \) is an observable linear system. Note that \( \Sigma \) is also reachable by minimality conditions.

Moreover, the generalization of the above lemma is given in [19] and [20] and it is as follows: if we consider a reachable and observable linear system \( \Sigma \) over \( R \), then \( \mathcal{C}(\Sigma) \) is an observable family of convolutional codes in the sense that \( R[z]^n / \mathcal{C} \) is flat over \( R[z] \).

### 3 Feedback convolutional equivalence over noetherian von Neumann regular rings

Before defining the feedback convolutional equivalence between families of convolutional codes, we recall some results above the degree and the controllability indices of convolutional codes over finite fields (see [23]). These results will be used in the sequel:

i) The degree of the encoder \( G(z) \) of a convolutional code \( \mathcal{C} \) over a finite field, that is denoted by \( \delta(G(z)) \), is defined by their column degrees, \( v_i := \max\{\deg(g_{i,j}(z)| i = 1, \ldots, n, j \} \), as \( \delta(G(z)) := \sum_{i=1}^k v_i \).

ii) The complexity of a convolutional code \( \mathcal{C} \), denoted by \( \delta(\mathcal{C}) \), is defined as the highest degree of the full size minors of any encoder \( G(z) \).

iii) An encoder matrix \( G(z) \) of \( \mathcal{C} \) is minimal if and only if \( \delta(G(z)) = \delta(\mathcal{C}) \).

iv) The set of column degrees of any minimal encoder of \( \mathcal{C} \) are known as the Forney or controllability indices of the code. We can reorder them if it is necessary such that \( k_1 \geq \cdots \geq k_k \). The invariant \( \delta = \sum_{i=1}^k k_i \) is the degree of the code \( \mathcal{C} \). The complexity of a convolutional code over a finite field equals its degree. In the following, we denote the set of controllability indices by \( \delta^C = (k_1, \ldots, k_k) \).

v) Note that the controllability indices of a convolutional code are unique and invariants of the code.

**Remark 3.1.** Forney or controllability indices are known, in the case of minimal encoders, as the Kronecker indices of the code. In the sequel, by abuse of notation we call them controllability indices of the code.

Since by first order representation we can compute an I/S/O representation for a convolutional code \( \mathcal{C} \) ([21–23]), the relation between controllability indices of the code and controllability (reachability) indices of the I/S/O representation associated as dynamical linear system is clear and it is given in the following theorem:

**Theorem 3.2** (c.f. Theorem 2, [44]). If \( \Sigma = (A, B) \) forms a controllable pair such that \( A \in \mathbb{F}^{\delta \times \delta} \) and \( B \in \mathbb{F}^{\delta \times k} \), then there exist positive integers \( k_1 \geq \cdots \geq k_k \) (often referred to as the controllability or Kronecker indices of the pair \( \Sigma \)) only dependent on the \( \text{GL}_n \) equivalence class of \( \Sigma \) having the following properties:

1. \( k_1 = \kappa \), the controllability index of \( \Sigma \).
2. \( \sum_{i=1}^k k_i = \delta \), the size of matrix \( A \).
3. There exists polynomial matrices \( X(z) \), \( Y(z) \), \( U(z) \) satisfying
De/f_inition 3.4. Ideal convolutional codes over
De/f_inition 3.6. \( R \) where each component is the set of Kronecker indices of each
vectors where each component is the set of controllability indices of each
Let De/f_inethesetofKroneckerindicesof
Example 3.7. By de/f_inition of
Remark 3.5. where
Since I/S/O representations over a finite field allow us to represent a convolutional code as \( \mathfrak{c} \simeq \text{Ker}(zK + L \mid M) = \text{Ker}(zI - A \begin{pmatrix} 0 & -B \\ -C & I - D \end{pmatrix}) \), Theorem 3.2 could be applied and then controllability indices of \( \mathfrak{c} \) equal the Kronecker indices of the pair \( \Sigma^e = (A, B)^e \). In particular, one has that \( \mathfrak{c}^e = \mathfrak{k}^e \).

**Example 3.3.** Consider the encoder of a \((3, 2, 2)\)-convolutional code \( \mathfrak{c} \) over \( \mathbb{Z}/2\mathbb{Z} \)
whose controllability indices are \( \mathfrak{c}^e = (\kappa_1, \kappa_2) = (2, 0) \).
We can compute a minimal first order representation of \( \mathfrak{c} \); that is, the matrices \( K, L \) and \( M \) that characterize the encoder \( G(z) = \begin{pmatrix} z + 1 & 1 \\ z^2 & 0 \\ 0 & 1 \end{pmatrix} \)
From the above triple of matrices, we compute its I/S/O representation \( \Sigma^c \) that is equal to the system \( \Sigma \) obtained in the Example 2.3. Thus \( \mathfrak{k}^e = (\kappa_1, \kappa_2) = (2, 0) \).
Let \( R \) be a noetherian von Neumann regular ring. Let \( \mathfrak{c} \simeq \oplus_{i=1}^t \mathfrak{c}_j \) be an \((n, k, \delta)\) systematic family of convolutional codes over \( R \) where \( \mathfrak{c}_j \) is an \((n, k, \delta)\) convolutional code over each \( R/m_j = \mathbb{F}_j \) for each maximal ideal \( m_j \in \text{Spec}(R) \).

**Definition 3.4.** We define the set of controllability indices of \( \mathfrak{c} \), and we denote them by \( \mathfrak{c}^e \), as the \( t \)-uple of vectors where each component is the set of controllability indices of each \( \mathfrak{c}_j \), namely
where \( (\kappa^e_i) \) is the \( i \)-th controllability index of the convolutional code \( \mathfrak{c}_j \).

**Remark 3.5.** By definition of \( \mathfrak{c} \) every convolutional code \( \mathfrak{c}_j \) has the same number of controllability indices, \( k \), and \( \sum_{i=1}^k \kappa^e_i = \delta \), the degree of the code, for all \( j = 1 \ldots t \).

**Definition 3.6.** We define the set of Kronecker indices of \( \Sigma^c \), and we denote them by \( \mathfrak{k}^e \), as the \( t \)-uple of vectors where each component is the set of Kronecker indices of each \( \Sigma^c_j \), namely
where \( (\kappa^e_i) \) is the \( i \)-th Kronecker index of the associated I/S/O representation \( \Sigma^c_j \) of the convolutional code \( \mathfrak{c}_j \).

**Example 3.7.** Let \( \mathfrak{c} \) be the following encoder of a family of convolutional codes over \( \mathbb{Z}/6\mathbb{Z} \)
where \( \mathfrak{c}^e = [(2, 1), (0, 1)] \) because

\[
\text{Ker} \begin{pmatrix} zI - A & 0 & -B \\ -C & I - D \end{pmatrix} = \text{Im} \begin{pmatrix} X(z) \\ Y(z) \\ U(z) \end{pmatrix}
\]
and having the property that the \( i \)-th column degree of \( G(z) = \begin{pmatrix} Y(z) \\ U(z) \end{pmatrix} \) is equal to \( \kappa_i \), and the \( i \)th column degree of \( X(z) \) is equal to \( \kappa_i - 1 \) for \( i = 1, \ldots, k \).
\[ C \otimes \mathbb{Z}/2\mathbb{Z} = C_{E(z/2Z)} = \begin{pmatrix} 1 + z & 1 \\ z^2 & 0 \\ 0 & 1 \end{pmatrix} \text{ with } R^{E(z/2Z)} = [(2, 0)] \text{ and }
\]
\[ C \otimes \mathbb{Z}/3\mathbb{Z} = C_{E(z/3Z)} = \begin{pmatrix} 1 + z & 2z \\ 2z & 0 \\ 0 & 2\pi \end{pmatrix} \text{ with } R^{E(z/3Z)} = [(1, 1)]. \]

Moreover, note that \( \Sigma^{E(z/z)} \) described by
\[ \Sigma^{E(z/z)} = [A = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}, C = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}, D = \begin{pmatrix} 2 & 1 \end{pmatrix}] \]
has Kronecker’s indices \( \chi^{E(z/z)} = [(2, 1), (0, 1)] \) because \( \chi^{E(z/z)} = \chi^{E(z/z)} = [2, 0] \) (see Example 3.3) and \( \chi^{E(z/z)} = [1, 1] \) because
\[ \Sigma^{E(z/z)} = [A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, D = \begin{pmatrix} 2 & 1 \end{pmatrix}] \]
and then \( \xi_1 = \text{rk}(B_2) = 2 \) and \( \xi_2 = \text{rk}(B_2A_2B_2) = 2 - 2 = 0. \) So, by Table 2, \( \chi^{E(z/z)} = [1, 1]. \)

| Conjugated Kronecker’s Indices | Kronecker’s Indices |
|-------------------------------|--------------------|
| \( \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \) | \( \begin{pmatrix} \chi_1 \\ \chi_2 \end{pmatrix} \) |

Now we define the feedback convolutional relation between families of convolutional codes over a noetherian von Neumann regular ring \( R \).

**Definition 3.8.** Let \( C \) and \( \bar{C} \) be \((n, k, \delta)\)-systematic families of convolutional codes over \( R \). The feedback convolutional relation between families of convolutional codes, \( f.c.e. \), is defined as
\[ C \overset{f.c.e.}{\sim} \bar{C} \iff R^C = R^\bar{C}. \]

Note that \( f.c.e. \) is an equivalence relation.

**Lemma 3.9.** The number of feedback equivalence classes of a systematic family of convolutional codes with degree \( \delta \) under feedback equivalence is \( p_n(\delta) \) where \( p_n(\delta) \) denotes the number of partitions of the degree of the code.

**Proof.** Feedback equivalence classes of a family of convolutional codes \( C \) such that the components of their controllability indices verify \( \sum_{j=1}^{k} \eta_i^j = \delta \) for each \( i = 1, \ldots, t \), are the possible ways to get \( \delta \), \( t \) times; that is, \( p_n(\delta) \).

**Remark 3.10.** Note that Definition 3.8 and Lemma 3.9 hold for convolutional codes over finite fields. In this case, the number of feedback equivalence classes of convolutional codes with the same degree \( \delta \) under \( f.c.e. \) relation is equal to the partitions of the degree of the code; that is,
# feedback equivalence classes of $C$ = $p(\delta)$,

where $p(\delta)$ denotes the partitions of integer $\delta$.

We give our main result.

**Theorem 3.11.** Let $C$ and $\overline{C}$ be systematic families of convolutional codes over $R$. Let $\Sigma^C$ and $\overline{\Sigma}^C$ be the corresponding I/S/O representations. Then

$$C^f \times \Sigma^C \sim \overline{C}^f \times \overline{\Sigma}^C,$$

where $f \times i$ denotes the feedback isomorphism between locally Brunovsky linear systems with state space of rank $\delta$ and $\Sigma^C = (A, B)^C$ (respectively for $\overline{\Sigma}^C$).

**Proof.** An I/S/O representation of a family of convolutional codes over $R$ is a reachable linear system, thus $R$ is a Locally Brunovsky ring by [36]. Therefore, we can apply the results of feedback classification of locally Brunovsky linear systems described in Subsection 2.1. Since $P(R) = \mathbb{N}$ is cancellative, the invariants $I_i$ classify too, and thus,

$$\Sigma^C \sim \overline{\Sigma}^C \Rightarrow [Z_i^{\Sigma^C}] = [Z_i^{\overline{\Sigma}^C}] \Leftrightarrow [I_i^{\Sigma^C}] = [I_i^{\overline{\Sigma}^C}].$$

From $P(R) = P(\mathbb{F}_1) \times \ldots \times P(\mathbb{F}_k)$, Equation (8) implies that

$$[I_1^{\Sigma^C} \otimes_R F_j] = [I_1^{\overline{\Sigma}^C} \otimes_R F_j] \text{ for } j = 1, \ldots, t \Rightarrow [I_i^{\Sigma^C}] = [I_i^{\overline{\Sigma}^C}].$$

Now, $\Sigma^C_i$ and $\overline{\Sigma}^C_i$ are I/S/O representations (reachable dynamical linear systems) over $\mathbb{F}_j$. The set of finitely generated projective modules of a finite field is the cancellative monoid $P(\mathbb{F}_j) = \mathbb{N}$. So,

$$[I_i^{\Sigma^C_i}] = [I_i^{\overline{\Sigma}^C_i}] \Leftrightarrow \Sigma^C_i \sim \overline{\Sigma}^C_i \Leftrightarrow X_1^{\Sigma^C_i} = X_1^{\overline{\Sigma}^C_i}.$$

Then, by [44], $\mathfrak{r}^{\Sigma^C_i} = \mathfrak{r}^{\overline{\Sigma}^C_i}$ and

$$[(\kappa^i_1, \ldots, \kappa^i_j), \ldots, (\kappa^i_k_1, \ldots, \kappa^i_k_j)] = [(\kappa^{\Sigma^C_i}_1, \ldots, \kappa^{\overline{\Sigma}^C_i}_1), \ldots, (\kappa^{\Sigma^C_i}_k, \ldots, \kappa^{\overline{\Sigma}^C_i}_k)] \Rightarrow \mathfrak{r}^{\Sigma^C} = \mathfrak{r}^{\overline{\Sigma}^C} \Leftrightarrow C^f \sim \overline{C}^f \sim \Sigma^C \sim \overline{\Sigma}^C.\quad \square$$

**Theorem 3.12.** Let $R$ be a noetherian von Neumann regular ring that decomposes in finite fields. Then

$$\{\Sigma^C / \sim\} = \{\text{Br}(R) / \sim\},$$

where $\{\text{Br}(R)\}$ denotes the set of locally Brunovsky linear systems over $R$ with state space of rank $\delta$, $\sim$ denotes the feedback isomorphism, and $\Sigma^C = (A, B)^C$ (respectively for $\overline{\Sigma}^C$).

**Proof.** Since $R$ is a Locally Brunovsky ring, and by Theorem 3.11,

$$\# \{\text{feedback classes of } C\} = \# \{\{\Sigma^C\}\} \subseteq \# \{\text{Br}(R)\} = \text{fe}_R(\delta).$$

By Lemma 3.9, $\# \{\text{feedback classes of } C\} = p(\delta)^f$ and since $R$ is a noetherian von Neuman regular ring, this number is equal to $\text{fe}_R(\delta)$, so we conclude the proof. \qed

Note that Kronecker indices of a linear system $\Sigma$ are obtained from the pair $(A, B)$ and hence, they are independent of $C$ and $D$. Therefore, since controllability invariant indices of an $(n, k, \delta)$-family of convolutional codes, $C$, are obtained from its I/S/O representation $\Sigma^C$, it follows that controllability indices of $C$ are obtained from pair $(A, B)^C$, and they are independent of $(C, D)^C$. We highlight this property in the following example.

**Example 3.13.** Let $R$ be the ring of modular integers $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $\Sigma_i$ be the following classes of feedback isomorphisms of locally Brunovsky linear systems over $\mathbb{Z}/6\mathbb{Z}$$$

$$\Sigma_1 = \left[\begin{array}{c}
(0 & 0 \\
1 & 0
\end{array}\right], \quad \Sigma_2 = \left[\begin{array}{c}
(0 & 0 \\
0 & 1
\end{array}\right],$$

$$\Sigma_3 = \left[\begin{array}{c}
(1 & 0 \\
0 & 0
\end{array}\right].$$

Here, $\Sigma_1$ and $\Sigma_2$ are the feedback isomorphisms of locally Brunovsky linear systems with state space of rank $\delta$, and $\Sigma_3$ is the feedback isomorphism of locally Brunovsky linear systems with state space of rank $\delta$.
Then, we obtain the minimal first order representation

\[
\Sigma_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \Sigma_2 = \begin{bmatrix} 5 & 0 \\ 0 & 2 \end{bmatrix} \quad \text{and } \Sigma_4 = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 5 & 0 \\ 0 & 3 \end{bmatrix}.
\]

By Theorem 3.12 we can consider the above systems as I/S/O representations over \( \mathbb{Z}/6\mathbb{Z} \) obtaining the corresponding classes of feedback convolutional equivalence of families of convolutional codes. In order to compute them, we have added random pairs of matrices \( C \) and \( D \),

\[
\Sigma_1 = \begin{bmatrix} A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, & B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, & C = \begin{bmatrix} 1 & 0 \end{bmatrix}, & D = \begin{bmatrix} 4 & 1 \end{bmatrix} \end{bmatrix}.
\]

Then, we obtain the minimal first order representation

\[
K_1 = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \quad L_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad M_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}
\]

and the family of convolutional codes

\[
\mathcal{C}_1(\Sigma_1) = \begin{bmatrix} 1z + 4z^2 + 1 \\ 5z^2 \\ 0 \\ 1 \end{bmatrix} \quad \text{where } \kappa^{\mathcal{C}_1(\Sigma_1)} = [(2, 2), (0, 0)].
\]

The following system is \( \Sigma_2 \):

\[
\Sigma_2 = \begin{bmatrix} A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, & B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & C = \begin{bmatrix} 3 & 2 \end{bmatrix}, & D = \begin{bmatrix} 1 & 2 \end{bmatrix} \end{bmatrix}.
\]

Then, we obtain the following minimal first order representation

\[
K_2 = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}
\]

and the family of convolutional codes

\[
\mathcal{C}_2(\Sigma_2) = \begin{bmatrix} 3 + z + 2z + 2z \\ z \\ 0 \\ z \end{bmatrix} \quad \text{where } \kappa^{\mathcal{C}_2(\Sigma_2)} = [(1, 1), (1, 1)].
\]

We are going to compute the results for \( \Sigma_3 \)

\[
\Sigma_3 = \begin{bmatrix} A = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}, & B = \begin{bmatrix} 5 & 0 \\ 0 & 2 \end{bmatrix}, & C = \begin{bmatrix} 1 & 3 \end{bmatrix}, & D = \begin{bmatrix} 2 & 1 \end{bmatrix} \end{bmatrix}.
\]

Then, we obtain the minimal first order representation

\[
K_3 = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 0 & 5 & 0 \\ 0 & 0 & 2 \end{bmatrix}
\]

and the family of convolutional codes

\[
\mathcal{C}_3(\Sigma_3) = \begin{bmatrix} 1 + z + 2z + 3 \\ 3z^2 + 2z + 3 \\ 0 \\ 0 \end{bmatrix} \quad \text{where } \kappa^{\mathcal{C}_3(\Sigma_3)} = [(2, 1), (0, 1)].
\]

Finally,

\[
\Sigma_4 = \begin{bmatrix} A = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, & B = \begin{bmatrix} 5 & 0 \\ 0 & 3 \end{bmatrix}, & C = \begin{bmatrix} 1 & 1 \end{bmatrix}, & D = \begin{bmatrix} 3 & 2 \end{bmatrix} \end{bmatrix}.
\]
Then, we obtain its minimal first order representation

\[
K_4 = \begin{pmatrix} 5 & 0 \\ 0 & 5 \\ 0 & 0 \end{pmatrix}, \quad L_4 = \begin{pmatrix} 0 & 0 \\ 2 & 0 \\ 1 & 1 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 0 & 5 & 0 \\ 0 & 0 & 3 \\ 5 & 3 & 2 \end{pmatrix}
\]

and the following family of convolutional codes

\[
C_4(\Sigma_4) = \begin{pmatrix} 1 + 5z & 5 \\ 3z + 4z^2 & 0 \\ 0 & 4 + 3z \end{pmatrix}
\]

where \( R[C_4(\Sigma_4)] = [(1, 2), (1, 0)] \).

4 Conclusions and future work

We conclude that there exists a bijective correspondence between feedback isomorphisms of locally Brunovsky linear systems and feedback convolutional classes of families of convolutional codes over a noetherian von Neumann regular ring \( R \).

Future work is focused on the construction of canonical forms of families of convolutional codes by using Brunovsky canonical forms of their associated I/S/O representations over \( R \) as well as the development of the decoding process. Moreover, we will study the generalization of the feedback convolutional equivalence to other interesting classes of rings. From an engineering point of view, it would be interesting to perform algorithms in order to get effective computations of multicast convolutional coding depicted in this paper.

References

[1] Climent J.J., Herranz V., Perea C., Tomás V., Un criptosistema de clave pública basado en códigos convolucionales, In Proceedings of XXI Congreso de Ecuaciones Diferenciales y Aplicaciones & XI Congreso de Matemática aplicada (21-25 Septiembre, Ciudad Real, Spain), 2009, 1-8.
[2] Petsche T., Dickinson B.W., A Trellis - structured Neural Network, Neural Infor. Proc. Systems, 1988, 592 - 601.
[3] Forney Jr. G.D., Concatenated Codes, MIT Press, Cambridge, MA, 1966.
[4] Rosenthal J., Codes, systems and graphical models,IMA, vol. 123, ch. Connections between linear systems and convolutional codes, Springer - Verlag, 2001, 39 - 66.
[5] García-Planas M.I., Souidi El.M., Um L.E., Convolutional codes under linear systems point of view. Analysis of output-controllability. Wseas Transactions on Mathematics, 2012, 11 (4), 324-333.
[6] Climent J-J., Herranz V., Perea C., A first approximation of concatenated convolutional codes from linear systems theory viewpoint, Linear Algebra Appl., 2007, 425 (2-3), 673-699.
[7] Rosenthal J., Smarandache R., Maximum distance separable convolutional codes, Appl. Algebr. Eng. Comm., 1999, 10 (1), 15-32.
[8] Zerz E., On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings, Asian J. Control, 2010, 12 (2), 119-126.
[9] Mahpakulchai S., Van Dyck R., Design of ring convolutional trellis codes for MAP decoding of MPEG-4 images, IEEE Trans.Commun., 2004, 52 (7), 1033 -1037.
[10] Jouhari H., Souidi E. M., Improving Embedding Capacity by using the Z4-linearity of Preparata Codes. Int J Comput Appl., 2012, 53 (18), 1-6.
[11] Massey J.L., Mittelholzer T., Convolutional codes over rings, In Proceedings Joint Swedish-Soviet Int. Workshop on Inform. Theory, (Gotland, Sweden), 1989, 14-18.
[12] Massey J.L., Mittelholzer T., Systematicity and rotational invariance of convolutional codes over rings. In Proceedings Int. Workshop on Alg. and Combinatorial Coding Theory (Leningrad, Russia),1990, 154-158.
[13] Fagnani, F., Zampieri S., , System-theoretic properties of convolutional codes over rings, IEEE T. Infor. Theory, 2001, 47 (6), 2256-2274.
[14] Johannesson R., Wan Z., Wittenmark E., Some structural properties of convolutional codes over rings, IEEE T. Infor. Theory, 1998, 44 (2), 839-845.
[15] Kuijper M., Pinto R., On minimality of convolutional ring encoders, IEEE T. Inform. Theory, 2009, 55 (11), 4890-4897.
[16] El Oued, M., Napp, D., Pinto, R., Toste, M., The dual of convolutional codes over $\mathbb{Z}_p$. Volume entitled Applied and Computational Matrix Analysis. Springer Verlag, 2017, 192, 79–91.
[17] El Oued, M., Sole, P., MDS convolutional codes over a finite ring. IEEE T. Inform. Theory., 2013, 59 (11), 7305 – 7313.
[18] Napp, D., Pinto, R., Toste, M., On MDS convolutional codes over $\mathbb{Z}_p$. Des. Codes Cryptogr., 2017, 83, 101–114.
[19] Carriegos, M., DeCastro-García, N., Muñoz Casteñeda, A., Kernel representations of convolutional codes over rings, Preprint available in https://arxiv.org/pdf/1609.05043v1.pdf, unpublished data.
[20] DeCastro-García, N., Feedback equivalence in linear systems and convolutional codes. Applications to Cybernetics, Coding and Cryptography, Ph. D. Thesis, Universidad de León, Spain, 2016.
[21] Rosenthal, J., Schumacher, J. M., York E. V., On behaviors and convolutional codes, IEEE T. Inform. Theory, 1996, 42 (6), 1881-1891.
[22] Rosenthal, J., York E. V., BCH Convolutional Codes, IEEE T. Inform. Theory, 1999, 45 (6), 1833-1844.
[23] York E. V., Algebraic description and construction of error correcting codes, a systems theory point of view, Ph.D. thesis, Univ. Notre Dame, France, 1997.
[24] Brewer J. W., Klingler L., On feedback invariants for linear dynamical systems, Linear Algebra Appl., 2001, 325 (1-3), 209-220.
[25] Brewer J. W., Bunce J. W., Van Vleck F. S., Linear Systems over Commutative Rings, Marcel Dekker, New York, 1986.
[26] Hautus M.L.J., Sontag E.D., New results on pole-shifting for parametrized families of systems, J. Pure Appl. Algeb, 1986, 40, 229-244.
[27] MacWilliams F. J., A theorem on the distribution of weights in a systematic code. Bell Syst. Tech. J., 1963, 42, 79–94.
[28] Gluesing-Luerssen H., Schneider G., State space realizations and monomial equivalence for convolutional codes, Linear Algebra Appl., 2007, 425 (2-3), 518-533.
[29] Quang Dinh H., López-Permouth S. R., On the equivalence of codes over rings and modules, Finite Fields Th. App., 2004, 10, 615–625.
[30] Carriegos, M., Hermida-Alonso J.A., Sánchez-Giralda T., The pointwise feedback relation for linear dynamical systems, Linear Algebra Appl., 1998, 279 (1-3), 119-134.
[31] Hernida-Alonso J.A., Perez M.P., Sanchez-Giralda T., Brunovsky’s canonical form for linear dynamical systems over commutative rings, Linear Algebra Appl., 1996, 233, 131-147.
[32] Carriegos, M. V., Enumeration of classes of linear systems via equations and via partitions in a ordered abelian monoid, Linear Algebra App., 2013, 438 (3), 1132-1148.
[33] Hautus M.L.J., Controllability and observability condition for linear autonomous system. Ned. Akad. Wetenschappen, Proc. Ser. A, 1969, 72, 443-448.
[34] Brunovsky P. A., A classification of linear controllable systems, Kibernetika, 1970, 6 (3), 173-187.
[35] Kalman R. E., Kronecker invariants and Feedback, in Ordinary Differential Equations, Academic Press (New York), 1972, 459-471.
[36] DeCastro-García N., Carriegos M.V., Muñoz Castañeda A., A characterization of von Neumann rings in terms of linear systems, Linear Algebra App., 2016, 494, 236-244.
[37] McEliece R. J., The algebraic theory of convolutional codes. In V. Pless and W.C. Huffman, editors, Handbook of Coding Theory, 1998, 1, 1065-1138.
[38] Massey J.L., Sain M.K., Codes, automata and continuous systems: explicit interconnections, IEEE Trans. Automat. Contr., 1967, 12 (6), 644–650.
[39] Kitchens B. Symbolic Dynamics and Convolutional Codes. In: Marcus B., Rosenthal J. (eds) Codes, Systems, and Graphical Models. The IMA Volumes in Mathematics and its Applications, Springer, New York, NY, 2001, 123.
[40] Willems J. C., From time series to linear system-part I. Finite dimensional linear time invariant systems, Automatica (Journal of IFAC), 1986, 22 (5), 561-580.
[41] Kuijper M., First Order Representations of Linear Systems, Ph.D. Thesis, Boston, MA: Birkhäuser, 1994.
[42] Kuijper M., Schumacher J. M., Realization of Autoregressive Equations in Pencil and Descriptor Form, SIAM J. Control Optim., 1990, 28 (5), 1162-1189.
[43] Fornasini, Valcher M.E., Multidimensional systems with finite support behaviors, Signal structure generation and detection, SIAM J. Control Op., 1998, 36(2), 760 779.
[44] Popov V. M., Invariant description of linear time-invariant controllable systems, SIAM J. Control Opt., 1972, 10 (2), 252-264.