mathematics

MDPI

Article

On the State Approach Representations of Convolutional Codes over Rings of Modular Integers

Ángel Luis Muñoz Castañeda *, Noemí DeCastro-García and Miguel V. Carriegos

Department of Mathematics, Universidad de León, 24007 León, Spain; ncasg@unileon.es (N.D.-G.); miguel.carriegos@unileon.es (M.V.C.)
* Correspondence: amunc@unileon.es

Abstract: In this study, we prove the existence of minimal first-order representations for convolutional codes with the predictable degree property over principal ideal artinian rings. Further, we prove that any such first-order representation leads to an input/state/output representation of the code provided the base ring is local. When the base ring is a finite field, we recover the classical construction, studied in depth by J. Rosenthal and E. V. York. This allows us to construct observable convolutional codes over such rings in the same way as is carried out in classical convolutional coding theory. Furthermore, we prove the minimality of the obtained representations. This completes the study of the existence of input/state/output representations of convolutional codes over rings of modular integers.

Keywords: convolutional codes; representations; rings of modular integers

Citation: Muñoz Castañeda, Á.L.; DeCastro-García, N.; Carriegos, M.V. On the State Approach Representations of Convolutional Codes over Rings of Modular Integers. *Mathematics* **2021**, *9*, 2962. https://doi.org/10.3390/math9222962

Academic Editor: Patrick Solé

Received: 19 October 2021
Accepted: 11 November 2021
Published: 20 November 2021

1. Introduction

The relation between convolutional codes and linear dynamical systems has been and still is largely studied. This relationship appears when one considers studying the coding dynamics of a convolutional code, and it depends, to some degree, on the notion of convolutional code used. If we describe a convolutional code as a linear subspace, $\mathcal{C} \subset \mathbb{F}_q(z)^n$, the linear system associated with the code is known as driving input/output representation ([1,2]). If we describe a convolutional code as a submodule, $\mathcal{C} \subset \mathbb{F}_q[z]^n$, the coding dynamics can be modeled by a linear dynamical system known as input/state/output (I/S/O) representation [3–6], since k components of the output drive the remaining $n-k$ components. One can also define a convolutional code as a time-invariant complete behavior. In such a case, there is also a representation theory [7–9]. Another perspective deals, for instance, with the dynamic symbolic point of view [10].

The case we are interested in is that of submodules and I/S/O representations. I/S/O representations are useful because, among other reasons, they allow one to construct convolutional codes with desirable properties (such as observability and good distances), to define (algebraic) decoding algorithms, to study concatenated convolutional codes, and to study finite support $2D$ convolutional codes, periodically time-invariant convolutional codes and product convolutional codes ([11–17]).

Massey and Mittleholzer introduced convolutional codes over rings to model the phase modulation problem ([18,19]) and, currently, they are also used for decoding, steganography, and networks models, among other applications. The study of their algebraic structure was focused on in [20] for general base rings, and completed in [21] for convolutional codes over the ring $\mathbb{Z}_{p^r}$, where r is a positive integer and p is a prime number.

Although the mathematical formalism of the theory of convolutional codes over general rings is very similar to that of fields, their properties may be quite different, and they need to be studied for particular rings ([22–24]). Despite their importance, the extension of the relation between minimal I/S/O representations and convolutional codes

to an arbitrary commutative ring may not be that close. In the case of the module-theoretic approach, it has only been extended, to the knowledge of the authors, to noetherian von Neumann regular rings, that is, finite product of fields ([25,26]).

In this work, we address the problem of the existence of first-order and I/S/O representations for convolutional codes over principal ideal artinian rings, such as $\mathbb{Z}_M$ with M a natural number. Furthermore, we study the minimality conditions of these representations through control properties of the associated linear systems.

This article is organized as follows: in Section 2, we give an overview of basic notions concerning convolutional codes and their first-order and I/S/O representations. In Section 3, we recall and prove some results about the predictable degree property of a convolutional encoder. In Section 4, we prove the existence of first-order representations for convolutional codes with the predictable degree property over principal artinian rings. Then, the existence of I/S/O representations is also studied. In Section 5, we prove that the obtained I/S/O representations are minimal. Furthermore, we study the relation between the observability of a convolutional code and the observability of the corresponding I/S/O representations. Finally, we give some conclusions concerning these results.

2. Convolutional Codes and Linear Systems

In this section, we review the basic definitions and properties of convolutional codes over rings. In addition, we recall the notions of first-order and I/S/O representations of convolutional codes over rings, as stated in [27].

2.1. Algebraic Preliminaries about Convolutional Codes

Let R be a commutative ring and z an indeterminate. We consider the polynomial ring $R[z]$. Given a polynomial $p(z) \in R[z]$, its trailing coefficient is the coefficient of least degree. Consider the multiplicatively closed system

$$S := \{q(z) \in R[z] : \text{ trailing coefficient of } q(z) \in R^*\},$$

with R^* being the group of invertible elements of R. Then, the ring of rational functions is defined as the localized ring:

$$R(z) := S^{-1}R[z] := \left\{ \frac{p(z)}{q(z)} : q(z) \in S,\ p(z) \in R[z] \right\}.$$

The ring of realizable functions is defined as

$$\begin{aligned} R_r(z) :=& \left\{ \frac{p(z)}{q(z)} \in R(z) : q(0) \in R^* \right\} \\ =& \left\{ \frac{p(z)}{q(z)} : q(z) \in S, q(0) \in R^* \text{ and } p(z) \in R[z] \right\}. \end{aligned}$$

Let $R[[z]]$ be the ring of formal power series with coefficients in R, and $R((z))$ the ring of Laurent series with coefficients in R. Note that $R_r(z) \subseteq R[[z]] \subseteq R((z))$ and $R_r(z) \subseteq R(z) \subseteq R((z))$. There are different definitions of convolutional codes, depending on what we demand to the message transmission process, i.e., if there is a time origin in the transmission process, if the transmission process can be extended infinitely, etc. This choice is reflected on the algebraic structure of the space of code words, $\mathcal{A} \in \{R((z)), R[[z]], R(z)\}$, and it provides us with different types of encoders.

In the following, when we refer to $\mathcal{A}$ as a space of code words, we mean that $\mathcal{A}$ can be one of the rings $R((z))$, $R[[z]]$ or $R(z)$.

Definition 1 ([19]). *Let $k \leq n \in \mathbb{N}$. Let $\mathcal{A}$ be a space of code words. A (k, n) convolutional encoder over $\mathcal{A}$ is a realizable matrix $G(z) \in R_r(z)^{n \times k}$ whose columns are linearly independent as elements of $\mathcal{A}^n$.*

$G(z)$ defines, by left multiplication, an R-linear map $G(z)\cdot : \mathcal{A}^k \to \mathcal{A}^n$. In the above definition, the condition imposed on the columns of $G(z)$ means that the above R-linear map is injective. In some works such as [20], the above matrix $G(z)$ is called a generator matrix.

Definition 2. *Let $\mathcal{A}$ be a space of code words and let $G(z) \in R_r(z)^{n\times k}$ be a (k,n) convolutional encoder over $\mathcal{A}$. The $\mathcal{A}$-submodule of $\mathcal{A}^n$ given by*

$$Im(G(z)\cdot) = \{G(z)\cdot x(z) :\ x(z) \in \mathcal{A}^k\}$$

is called a (k,n) convolutional code $\mathcal{C}$ over R. The elements of $\mathcal{A}^k$ are called information words, while the elements of $Im(G(z)\cdot)$ are called code words.

There is a natural and well-known equivalence relation in the set of encoders once we fix a space of code words $\mathcal{A}$.

Definition 3 (Definition 4, [20])**.** *Let $\mathcal{A}$ be a space of code words and $k \leq n \in \mathbb{N}$. Two convolutional encoders, $G(z)$ and $G'(z) \in R_r(z)^{n\times k}$, are equivalent if they generate the same convolutional code, $\mathcal{C} \subset \mathcal{A}^n$. This equivalence relation is denoted by $G(z) \sim G'(z)$.*

Lemma 1 (Theorem 1, [20])**.** *Let $\mathcal{A}$ be a space of code words and $k \leq n \in \mathbb{N}$. Two convolutional encoders, $G(z)$, $G'(z) \in R_r(z)^{n\times k}$, are equivalent if and only if there is an invertible matrix $U(z) \in \mathcal{A}^{k\times k}$ such that $G'(z) = G(z)\cdot U(z)$.*

Note that any matrix

$$G(z) = \left(\frac{p_{ij}(z)}{q_{ij}(z)}\right) \in R_r(z)^{n\times k},$$

with $q_{ij}(z) \in S$ and $q_{ij}(0) \in R^*$, can be written in the form

$$G(z) = \frac{G'(z)}{h(z)},$$

with $G'(z)$ being a polynomial matrix and $h(z) = \prod q_{ij}(z) \in R[z]$ a realizable polynomial, i.e., $h(0) \in R^*$. In the case where the definition of convolutional code is taken over $R((z))$ or $R(z)$, it follows from the above observation that any convolutional encoder is equivalent to a polynomial encoder, which, in turn, defines a submodule of $R[z]^n$.

Definition 4. *Let $k \leq n \in \mathbb{N}$. The $R[z]$-submodule of $R[z]^n$ given by*

$$Im(G(z)\cdot) = \{v(z) = G(z)\cdot u(z) :\ u(z) \in R[z]^k\}$$

where $G(z)$ is a (k,n) polynomial convolutional encoder whose rows are free over $R[z]$, is called a (k,n) (polynomial) convolutional code over R.

Any convolutional encoder over $R((z))$ or $R(z)$ defines a convolutional code in the sense of Definition 4 by erasing denominators and taking its image as a homomorphism of $R[z]$-modules. However, it is important to note that not every polynomial convolutional encoder over $R((z))$ or $R(z)$ of the same convolutional code defines the same polynomial convolutional code. This happens because two equivalent polynomial encoders $G(z), G'(z)$ over $R((z))$ or $R(z)$ might not be equivalent as convolutional encoders for polynomial convolutional codes. For example, $(1+z)$ and (1) are equivalent convolutional encoders over $R((z))$ but not over $R[z]$.

In the sequel, we only consider polynomial convolutional encoders and Definition 4 for convolutional code over a ring R.

One of the main features of a polynomial convolutional encoder is its degree, δ, which is closely related to the number of memory containers needed to realize it. This concept was first defined for convolutional codes over finite fields in [28] and generalized to commutative rings in [29].

Definition 5. *Let $k \leq n \in \mathbb{N}$ and let $G(z) \in R[z]^{n\times k}$ be a polynomial convolutional encoder. Its i-th constraint length, ν_i, is defined as the maximum degree of the components of its i-th column. Its degree or complexity is defined as $\delta_{G(z)} := \sum_{i=1}^{k} \nu_i$. The memory of $G(z)$ is defined as the maximum among the ν_is. We may assume without loss of generality that $\nu_1 \geq \ldots \geq \nu_k$.*

Let $G(z)$ be a (k, n) polynomial convolutional encoder, and let $u(z) \in R[z]^k$ be an information word, where $u(z) = (u_1(z), \ldots, u_k(z))$. Let us denote by $\theta(v(z))$ the maximum degree of the components of the code word $v(z) = G(z) \cdot u(z)$. For the sake of notation, we drop the dependency of $v(z)$ on the above notation if there is no risk of confusion. Then, we clearly have $\theta \leq \max\{\deg(u_i(z)) + \nu_i\}$, where $deg(u_i)$ stands for the degree of each component of $u(z)$.

Finally, we recall several properties of polynomial convolutional encoders. The relation between some of these properties in a specific ring is shown in [20]. Here, we include the needed properties for general rings in order to show some results in the following sections. These definitions are the usual ones when the base ring is a finite field (Definitions 4 and 5 in [28]).

Definition 6 (Section IIIA, [21])**.** *A polynomial convolutional encoder $G(z) \in R[z]^{n\times k}$ is basic (or observable) if it has a polynomial right inverse, i.e., $Coker(G(z)\cdot)$ is a projective $R[z]$-module. Equivalently, if the following exact sequence*

$$0 \longrightarrow R[z]^k \xrightarrow{G(z)\cdot} R[z]^n \longrightarrow Coker(G(z)) = R[z]^n/\mathcal{C} \longrightarrow 0$$

splits.

Remark 1. *Note that the above property is equivalent to saying that a convolutional code $\mathcal{C}$ is observable if the quotient $R[z]^n/\mathcal{C}$ is a flat $R[z]$-module of constant rank $n - k$. If R is a principal ideal ring, then a (k, n) convolutional code over R, $\mathcal{C} \subset R[z]^n$ is observable if and only if there exists a surjection $\psi : R[z]^n \to R[z]^{n-k} \to 0$ such that $Ker(\psi) = \mathcal{C}$. This follows from [30].*

Definition 7 ([31])**.** *A polynomial encoder $G(z)$ is minimal if $\delta_{G(z)}$ is the minimum among the degrees of its equivalent polynomial encoders. It is minimal–basic if it is both minimal and basic.*

All the above definitions also make sense when we consider general polynomial matrices instead of just injective polynomial matrices, that is, polynomial convolutional encoders.

2.2. A Review of the Representations of Convolutional Codes over Finite Fields

Given a convolutional encoder $G(z) \in R[z]^{n\times k}$, a natural problem in convolutional coding theory is to find a linear dynamical control system Σ whose finite-support orbits coincide with the outputs of the encoder (the code words). That is, to find a dynamical system Σ that realizes the dynamics of the coding process.

To begin with, let us define what a state-space representation of a convolutional encoder is (see [21] for a more general definition).

Definition 8. *Let $k \leq n \in \mathbb{N}$ and let $G(z) \in R[z]^{n\times k}$ be a polynomial convolutional encoder of degree δ. A state-space representation of $G(z)$ is a tuple of matrices $A \in R^{\delta\times\delta}$, $B \in R^{\delta\times k}$, $C \in R^{n\times\delta}$, $D \in R^{n\times k}$, such that, if $u(z) = \sum u_t z^t \in R[z]^k$ and $y(z) = \sum y_t z^t \in R[z]^n$, then $G(z)u(z) = y(z)$ if and only if there exists $x(z) = \sum x_t z^t \in R[z]^\delta$ with*

$$\left\{\begin{array}{rcl} x_{t+1} & = & A\cdot x_t + B\cdot u_t \\ v_t & = & C\cdot x_t + D\cdot u_t \\ x_0 & = & 0 \end{array}\right. \tag{1}$$

A state-space representation of a convolutional encoder $G(z)$ is minimal if among all possible state-space representations of the same $G(z)$, the dimension δ is the smallest possible.

In case the base ring is a finite field, a representation as defined in Equation (1) is sometimes known as *driven variable representation*, since the input $u(z)$ drives the output $v(z)$. There is, however, another kind of representation in which *k components of the output drive the remaining $n-k$ components*, and it is called the *input/state/output representation*, or just I/S/O representation for short [6,32]. I/S/O representations have already been defined for convolutional codes over noetherian von Neumann rings (finite product of fields) and used to construct concatenated convolutional codes [26,27].

Definition 9 ([27]). *Let $\mathcal{C}\subset R[z]^n$ be a (k,n) convolutional code. An I/S/O representation of $\mathcal{C}$ is a tuple of matrices $A\in R^{\delta\times\delta}$, $B\in R^{\delta\times k}$, $C\in R^{n-k\times\delta}$, $D\in R^{n-k\times k}$, δ being the degree of any of the minimal encoders of $\mathcal{C}$, such that*

$$\mathcal{C}=\left\{\begin{array}{l} v(z)=\begin{pmatrix} y(z)\\ u(z)\end{pmatrix}\in R[z]^{(n-k)+k} : \exists x(z)\in R[z]^{\delta} \\ \quad \textit{satisfying} \left\{\begin{array}{rcl} x_{t-1} & = & A\cdot x_t + B\cdot u_t \\ y_t & = & C\cdot x_t + D\cdot u_t \\ x_{deg(v(z))} & = & 0 \end{array}\right. \end{array}\right\}. \tag{2}$$

Observe that, defining the matrices

$$K:=\begin{pmatrix} -\mathrm{Id}\\ 0\end{pmatrix},\ L:=\begin{pmatrix} A\\ C\end{pmatrix},\ M:=\begin{pmatrix} 0 & B\\ -\mathrm{Id} & D\end{pmatrix}, \tag{3}$$

we can state:

(i) $\mathcal{C}=\{v(z)\in R[z]^n : \exists x(z)\in R[z]^{\delta}$ such that $zKx(z)+Lx(z)+Mv(z)=0\}$.
(ii) K is injective.
(iii) (K,M) is surjective.

Definition 10 ([27]). *A triple (K,L,M) satisfying properties (i), (ii) and (iii) is called a* first-order representation *of the code $\mathcal{C}$. If (K,L,M) also satisfy the property (iv) $(zK+L,M)$ is surjective, then it is said that it is minimal.*

Remark 2. *There are some comments regarding first-order and I/S/O representations for convolutional codes, in the case the base ring is a finite field, that need to be pointed out.*

1. *Let $\mathcal{C}\subset R[z]^{n\times k}$ be a (k,n) convolutional code. When the base ring R is a field, there always exists a permutation $\sigma\in\mathfrak{S}_n$ of n elements such that $\mathcal{C}':=\sigma(\mathcal{C})$ admits an I/S/O representation ([32]). The way to find an I/S/O representation is as follows: first, one computes a first-order representation (K,L,M) (the proof of the existence theorem is constructive) and then, one makes elementary operations over the matrices (K,L,M) to obtain a triple of matrices $(\mathcal{K},\mathcal{L},\mathcal{M})$ such that*

$$\mathcal{K}=\begin{pmatrix} -I_\delta\\ O\end{pmatrix},\mathcal{L}=\begin{pmatrix} A\\ C\end{pmatrix} \textit{ and } \mathcal{M}=\begin{pmatrix} O & B\\ -I_{(n-k)} & D\end{pmatrix}. \tag{4}$$

   The system $\Sigma=(A,B,C,D)$ is an I/S/O representation of the convolutional code $\mathcal{C}'=\sigma(\mathcal{C})$ for the permutation σ.
2. *If we consider a (k,n) convolutional code $\mathcal{C}\subset\mathbb{F}[z]^n$ of complexity δ admitting a minimal first-order representation, then the convolutional code $\mathcal{C}$ is described by a minimal I/S/O representation, Σ, that is a reachable linear system. From this point of view, if we consider*

a reachable and observable linear system Σ over a finite field, we can obtain an observable convolutional code, that is usually denoted by $\mathcal{C}(A, B, C, D) = \mathcal{C}(\Sigma)$ [3,6,32].

3. *The first-order representations for convolutional codes over finite fields are constructed from the fact that G_h is injective. The matrix G_h is defined as follows: regarding $G(z) \in \mathbb{F}[z]^{n\times k}$ as a polynomial with coefficients in the vector space of matrices of size $n \times k$ with coefficients in $\mathbb{F}$, G_h is the coefficient of higher order in $G(z)$. The above condition that G_h is injective implies that $G(z)$ is minimal in the case where the base ring is a field (Theorem 2.22, Theorem 2.28, [33]), but this is no longer true for a general ring.*
4. *Given a linear dynamical system as in Equation (2), we define its transfer function matrix as $T(z) = C(z^{-1} \cdot I - A)^{-1} \cdot B + D$, $T(z)_{ij} \in R_r(z)$. The importance of the transfer function matrix is that it determines the input–output relation of the linear dynamical system. Observe that the existence of an I/S/O representation for a given convolutional code implies that codewords can be represented as*

$$v(z) = \begin{pmatrix} y(z) \\ u(z) \end{pmatrix},$$

with $u(z)$ being an information word. In fact, if a convolutional code admits an I/S/O representation, then it admits a convolutional encoder $G(z)$ that has a full-size minor which is invertible in the ring of total fractions $Q(R[z])$, so that $G(z)$ is equivalent (in the sense of Definition 3 for $\mathcal{A} = Q(R[z])$) to

$$\begin{pmatrix} T(z^{-1}) \\ I \end{pmatrix}.$$

Any convolutional code admitting an encoder of the above type is called systematic. Note that the above remark concludes that the systematicity of the encoder of a convolutional code is a necessary condition for the code to admit an I/S/O representation. In the case of finite fields, every convolutional code is systematic (Appendix II, Theorem 9, [28]).

In order to obtain a minimal first-order representation for convolutional codes over rings, we have to take into account that, for a general ring R, not every convolutional code admits either a minimal–basic convolutional encoder nor a systematic convolutional encoder. These two properties are analyzed in the following sections.

3. On the Predictable Degree Property of Polynomial Encoders

The predictable degree (PDP) of a polynomial matrix $G(z) \in R[z]^{n\times k}$ was introduced by G. D. Forney in [34]. In general, $\deg(G(z)u(z)) \leq \max\{\deg(u_i(z)) + \deg(G_i(z))\}$. Here, the degree of a polynomial vector means the maximum degree of its components, and $G_i(z)$ denotes the i-th column of $G(z)$. Saying that $G(z)$ has the PDP means that the above inequality is an equality for any $u(z)$. In terms of convolutional coding theory, this means that the degree of a code word $G(z)u(z)$ can be predicted from the degrees of the components of the information word $u(z)$ and the constraint lengths of $G(z)$.

Remark 3. *If $G(z)$ is a polynomial convolutional encoder over a finite field, then the following statements are equivalent (Theorem 2.22, Theorem 2.28, [33]):*

1. *$G(z)$ has the PDP; that is,*
$$\theta = max\{deg(u_i(z)) + \nu_i\}$$
for every information word $u(z)$ with finite-support (Section 2.5, [33]).
2. *It is minimal–basic, i.e., it is minimal and it is also basic.*
3. *G_h is injective.*
4. *$\delta_{G(z)}$ = the maximum degree of the full-size minors of $G(z)$.*

When we work over a general base ring, the above characterization of the PDP is not true. One can find easy examples of convolutional encoders with PDP which are not minimal–basic and vice versa.

Example 1.

1. *In the case where R is not a field, we can find easy examples of minimal–basic convolutional encoders that do not have PDP. For instance, consider the convolutional encoder $G(z) = \begin{pmatrix} 2z \\ 1 \end{pmatrix}$ over $R = \mathbb{Z}_4$. It is clearly basic, since $r = (2,1) : R[z]^2 \to R[z]$ is a retract for $G(z)$, and it is obviously minimal. However, $G_h = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$ is not injective.*
2. *We can also find easy examples of convolutional encoders with PDP that are not basic. Consider the following: over $R = \mathbb{Z}_4$ the convolutional encoder with PDP given by $G(z) = \begin{pmatrix} 2 \\ 2+z \end{pmatrix}$. If $G(z)$ were basic, then we could find a matrix $H(z) = (s(z), t(z)) : R[z]^2 \to R[z]$ such that $H(z)G(z) = 1$. This would mean, in particular, that $2 \cdot s_0 + 2 \cdot t_0 = 1$, and this would imply that $2 \in R$ is invertible, which is not true. Thus, $G(z)$ is not basic.*

Although the property of being minimal–basic does not imply the PDP when R is a general ring, we can prove an equivalence between this last property and the injectivity of G_h.

Theorem 1. *Let $k \leq n \in \mathbb{N}$, $G(z) \in R[z]^{n \times k}$ a polynomial matrix and G_h the matrix of column-wise maximum degree coefficients. Then, $G(z)$ has PDP if and only if G_h is injective.*

Proof. The direct implication can be proved as in the case of fields (see (Theorem 2.22, Theorem 2.28, [33])). Let us prove the inverse implication. Suppose that $G(z)$ does not have the PDP, i.e., there is $u(z) \in R[z]^k$ such that

$$(\deg(v_i(z)) \leq) \deg(v(z)) < \max_i\{\theta_i + \nu_i\} \tag{5}$$

where $\theta_i := \deg(u_i(z))$. Let $\nu_1, \ldots, \nu_k$ be the constraint lengths of $G(z)$. Then,

$$\begin{aligned} v_i(z) =& g_{i1}(z)u_1(z) + \ldots + g_{ik}(z)u_k(z) \\ =& (g_{i1}^{\nu_1} u_1^{\theta_1}) z^{\nu_1+\theta_1} + \{\text{lower degree terms}\} + \\ & \vdots \\ & + (g_{ik}^{\nu_k} u_k^{\theta_k}) z^{\nu_k+\theta_k} + \{\text{lower degree terms}\}, \end{aligned} \tag{6}$$

where the $g_{it}^{\nu_t}$ may be zero or not. Suppose that

$$\nu_{j_1}\theta_{j_1} = \ldots = \nu_{j_l}\theta_{j_l} = \max_i\{\theta_i + \nu_i\}$$

Then, from Equations (5) and (6), we deduce that

$$g_{ij_1}^{\nu_{j_1}} u_{j_1}^{\theta_{j_1}} + \ldots + g_{ij_l}^{\nu_{j_l}} u_{j_l}^{\theta_{j_l}} = 0, \forall i = 1, \ldots, n \tag{7}$$

Let $u = (0, \ldots, u_{j_1}^{\theta_{j_1}}, \ldots, 0, \ldots, u_{j_l}^{\theta_{j_l}}, \ldots, 0) \in R^k$, which is non zero. Then, by Equation (7), we find that $G_h u = 0$, that is, G_h is not injective. □

Corollary 1. *Let $k \leq n \in \mathbb{N}$, and $G(z) = (g_{ij}(z)) \in R[z]^{k \times n}$ be a polynomial matrix with PDP. Then, $G(z)$ is injective, that is, it is a convolutional encoder.*

Proof. Suppose $G(z)$ is not injective. Then, there is a non-zero polynomial vector $u(z) \in R[z]^k$ such that $0 = G(z)u(z)$. Let $1 \leq t_1, \ldots, t_l \leq k$ be those subindices such that $\deg(u_{t_j}(z)) + \nu_{t_j} = \max\{\deg(u_i(z)) + \nu_i\}$ for all $j = 1, \ldots, l$. Denote $d_i = \deg(u_i(z))$, and let $u = (0, \ldots, u_{d_{t_1}}, \ldots, 0, \ldots, u_{d_{t_l}}, \ldots, 0) \in R[z]^k \setminus 0$, where $u_{d_{t_j}}$ is the maximum degree

coefficient of $u_{t_j}(z)$. Then, we have $G_h u = 0$, which implies that $u = 0$ by Theorem 1, and this is not possible. □

4. On the Existence of Representations over Principal Ideal Artinian Rings

In this section, we prove that convolutional codes over principal ideal artinian rings admit minimal first-order representations, such as those defined in Section 2.

Before this, we need to recall some algebraic properties of this class of rings.

A commutative ring, R, is an artinian ring if it is a noetherian ring with Krull dimension zero. As a consequence, it has finitely many prime ideals, all of them being maximal. By the Structure Theorem of artinian rings, we know that

$$R = \prod_{i=1}^{t} R_{\mathfrak{m}_i} \tag{8}$$

where $R_{\mathfrak{m}_i}$ are local artinian rings. Observe that local artinian rings are noetherian rings with only one prime (therefore maximal) ideal. The rings $\mathbb{Z}_{p^r}$, with p being a prime number, are typical examples of local artinian rings.

Artinian local rings can be easily characterized in terms of their nilradicals. More precisely, if R is a commutative ring with nilradical $\mathfrak{N}$, the following statements are equivalent:

1. R only has one prime ideal.
2. $\mathfrak{N}$ is a maximal ideal.
3. Every element of R is either invertible or nilpotent.

This follows directly from the equality $\mathfrak{N} = \bigcap_{\substack{\mathfrak{p} \subset R \\ \text{minimal}}} \mathfrak{p}$.

This characterization shows that artinian local rings are those noetherian rings in which every element is either invertible or nilpotent.

Proposition 1. *Let R be an artinian ring. The following statements hold:*

C1 *If P is a finitely generated projective module of constant rank n, then it is free.*

C2 *If R is a principal ideal ring and $G : R^k \to R^n$ is an injective matrix, then* $\mathrm{Coker}(G)$ *is flat.*

Proof.

1. By Equation (8), we know that $P = P_{\mathfrak{m}_1} \times \ldots \times P_{\mathfrak{m}_t}$. Now, the result follows from (Theorem 2, [35]).
2. Since flatness is a local property, we may assume that R is local. Let $G = (g_{ij}) : R^k \hookrightarrow R^n$ be an injective matrix. Injectivity implies that $\mathrm{Ann}_R(< M_1, \ldots, M_t >) = (0)$, where $M_1, \ldots, M_t$ are the full-size minors of G. Since every ideal of R is principal, we deduce that $\mathrm{Ann}_R(< M >) = (0)$, where $< M_1, \ldots, M_t >=< M >$, and $M \in R$. This implies that M is not a zero divisor and, therefore, is invertible in R, so $< M_1, \ldots, M_t >= R$. By Proposition 1.1, [36], this implies that $\mathrm{Coker}(G)$ is flat of rank $n - k$.

□

Given a polynomial matrix $G(z) \in R[z]^{n \times k}$ and a prime ideal $\mathfrak{p} \subset R$, we denote by $G(\mathfrak{p})(z)$ the restriction of $G(z)$ to $\mathfrak{p}$, which is the matrix whose (i, j) entry is given by

$$G(\mathfrak{p})(z)_{ij} = \frac{g_{ij}(z)}{1} \bmod(\mathfrak{p}R_{\mathfrak{p}}) \in k(\mathfrak{p})[z],$$

where $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is the residue field of $\mathfrak{p}$.

The following result generalizes the Existence Theorem for first-order representations over finite fields (Theorem 5.1.1, [32]).

Theorem 2. *Let $k \leq n \in \mathbb{N}$, R a principal ideal artinian ring and $G(z) \in R[z]^{n\times k}$ a convolutional encoder with PDP. Then, the convolutional code $\mathcal{C} := \mathrm{Im}(G(z))$ admits a minimal first-order representation.*

Proof. For any polynomial $p(x) = a_0 + a_1 z + \ldots + a_l z^l \in R[z]$, we will use the following notation $[p(x)] = (a_0, a_1, \ldots, a_l) \in R^{1\times(l+1)}$. Consider the matrix $X(z) \in R[z]^{\delta\times k}$ given by

$$X(z) = \begin{pmatrix} e_1 & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & e_2 & \ldots & \mathbf{0} \\ \vdots & \vdots & \ldots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & e_k \end{pmatrix}, \text{ where } e_i = \begin{pmatrix} 1 \\ z \\ z^2 \\ \vdots \\ z^{\nu_i - 1} \end{pmatrix}, \tag{9}$$

and let $\Delta \in R^{(2\delta+n)\times(\delta+k)}$ be the matrix

$$\Delta = \begin{bmatrix} z \cdot X(z) \\ X(z) \\ G(z) \end{bmatrix} \in R^{(2\delta+n)\times(\delta+k)}.$$

The matrix Δ is surjective, so we can form the exact sequence

$$0 \longrightarrow \mathrm{Ker}(\cdot\Delta) \hookrightarrow R^{2\delta+n} \xrightarrow{\cdot\Delta} R^{\delta+k} \longrightarrow 0. \tag{10}$$

This exact sequence always splits, so $\mathrm{Ker}(\cdot\Delta)$ is a finitely generated projective R-module of constant rank $\delta + n - k$. By property **C1**, we deduce that $\mathrm{Ker}(\cdot\Delta)$ is in fact free, so we can construct a matrix

$$(KLM) \in R^{(\delta+n-k)\times(2\delta+n)}, \tag{11}$$

formed by the $(\delta + n - k)$ row vectors of a base of $\mathrm{Ker}(\cdot\Delta)$, which can be expressed in pencil form

$$(z \cdot K + L, M) \begin{pmatrix} X(z) \\ G(z) \end{pmatrix}. \tag{12}$$

We complete the proof in several steps.

Step 1: Let $\mathfrak{p} \subset R$ be a prime ideal and let $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ be its residue field. From Proposition 1, condition **C2**, the PDP and Remark 3, we deduce that $G(\mathfrak{p})(z) \in k(\mathfrak{p})^{k\times n}$ is a convolutional encoder with PDP.

Step 2: From Equations (10) and (11), we can form the exact sequence

$$0 \longrightarrow R^{\delta+n-k} \xrightarrow{\cdot(KLM)} R^{2\delta+n} \xrightarrow{\cdot\Delta} R^{\delta+k} \longrightarrow 0.$$

Since $R^{\delta+k}$ is free, and therefore flat, this exact sequence remains exact after extending scalars $- \otimes_R k(\mathfrak{p})$. This fact, together with the conclusion obtained in *Step 1* and Theorem 5.1.1, [32], shows that $(K(\mathfrak{p}), L(\mathfrak{p}), M(\mathfrak{p}))$ is a minimal first-order representation for $G(\mathfrak{p})(z)$. Therefore, K, L, M satisfy properties (ii) and (iii) and (iv) of Definition 10 over each residue field.

Step 3: Recall that a morphism of modules is surjective if and only if it is residually surjective, and that a residually injective morphism of modules is, in fact, injective. Therefore, K is injective because $K(\mathfrak{p})$is injective for all prime ideals, (K, M) is surjective because $(K(\mathfrak{p}), M(\mathfrak{p}))$ is surjective for all prime ideals, and $(zK + L, M)$ is surjective because, for every primer ideal $\mathfrak{p} \subset R$, its reduction modulo $\mathfrak{p}$ is surjective.

Step 4: To complete the proof, it only remains to show the property (i) of Definition 10. To do so, let us start by pointing out a simple but important observation. The matrix

$(X(z)|\mathbf{0}_{k\times n})$ is a retract for the matrix $\begin{pmatrix} X(z) \\ G(z) \end{pmatrix}$, that is, $S \cdot \begin{pmatrix} X(z) \\ G(z) \end{pmatrix} = \mathrm{Id}_k$. Since $(z \cdot K + L, M)$ is surjective, we can construct the diagram

$$0 \longrightarrow \mathrm{Ker}((z \cdot K + L, M)) \xrightarrow{\iota} R[z]^{\delta+n} \xrightarrow{(z\cdot K+L,M)} R[z]^{\delta+n-k} \longrightarrow 0 \qquad (13)$$

$$\Psi, \quad S, \quad \begin{pmatrix} X(z) \\ G(z) \end{pmatrix}, \quad R[z]^k$$

Now, because of Equation (12), $\begin{pmatrix} X(z) \\ G(z) \end{pmatrix}$ factorizes through $\mathrm{Ker}((z \cdot K + L, M))$, and we denote the resulting homomorphism by Ψ. Then,

$$(S \circ \iota) \circ \Psi = S \circ (\iota \circ \Psi) = S \cdot \begin{pmatrix} X(z) \\ G(z) \end{pmatrix} = \mathrm{Id}_k,$$

which means that $S \circ \iota : \mathrm{Ker}((z \cdot K + L, M)) \longrightarrow\!\!\!\!\!\rightarrow R[z]^k$ is a retract for Ψ. Observe now, that the exact sequence in (13) splits, so $\mathrm{Ker}((z \cdot K + L, M))$ is a finitely generated projective $R[z]$-module of constant rank k. Then, since $S \circ \iota$ is surjective, we know that $\mathrm{Ker}(S \circ \iota)$ is finitely generated and projective, and for each maximal ideal $\mathfrak{M} \subset R[z]$, $\mathrm{Ker}(S \circ \iota)/\mathfrak{M}\mathrm{Ker}(S \circ \iota) = 0$. By Nakayama's Lemma, $\mathrm{Ker}(S \circ \iota)_{\mathfrak{M}} = 0$ for all maximal ideals, so $\mathrm{Ker}(S \circ \iota) = 0$. We finally conclude that

$$\mathrm{Im}\begin{pmatrix} X(z) \\ G(z) \end{pmatrix} = \mathrm{Ker}(z \cdot K + L, M),$$

from which, we obtain property (i) of Definition 10. Thus, (K, L, M) is a minimal first-order representation for $G(z)$. □

Remark 4. *Let $k \leq n \in \mathbb{N}$, R a principal ideal artinian ring and $G(z) \in R[z]^{k\times n}$ a convolutional encoder with PDP. If (K, L, M) is a first-order representation of $Im(G(z))$, then $(K(\mathfrak{p}), L(\mathfrak{p}), M(\mathfrak{p}))$ is a first-order representation of $Im(G(\mathfrak{p})(z))$ for each $\mathfrak{p} \in Spec(R)$*

Remark 5. *Observe that what we have proved is that the same construction method to find minimal first-order representations known in the case of fields ([32]) is also valid for commutative rings that satisfy the properties **C1** and **C2**. In particular, these properties are satisfied by any zero-dimensional ring, R, that satisfies one of the following conditions: (1) R is a noetherian, and therefore artinian, and principal ideal ring, or (2) R is a reduced ring, and hence von Neumann.*

Now, our aim is to prove the existence of I/S/O representations for convolutional codes over a principal ideal artinian ring. Recall from the classical theory of convolutional codes that I/S/O representations are not assigned to convolutional codes but to equivalence classes of them. That is, given a convolutional code $\mathcal{C} \subset \mathbb{F}[z]^n$, there is a permutation $\sigma \in \mathfrak{S}_n$ such that the (equivalent) convolutional code $\sigma(\mathcal{C})$ can be represented by an I/S/O representation. We show that the same result can be proved in the case that the principal ideal artinian ring R is local. If R is not local, the equivalence relation defined for codes (through permutations) has to be weakened in order to obtain an analogous result.

First, recall from Remark 2 that we have to show that every convolutional code over a principal ideal local ring is systematic.

Definition 11. *A systematic convolutional encoder is a convolutional encoder $G(z) \in R[z]^{k\times n}$ that has a full-size minor which is invertible in the total ring of fractions $Q(R[z])$. A systematic convolutional code $\mathcal{C} \subset R[z]^n$ is a convolutional code that admits a systematic convolutional encoder.*

Proposition 2. *Any polynomial convolutional encoder $G(z) \in R[z]^{n\times k}$ over a principal ideal artinian local ring R is systematic.*

Proof. Let $G(z) \in R[z]^{n\times k}$ be a (k,n) polynomial convolutional encoder. Since it is injective, we know that $\mathrm{Ann}_{R[z]}(< M_1(z),\dots,M_l(z) >) = 0$, where $M_1(z),\dots M_l(z) \in R[z]$ are the non-zero full-size minors of $G(z)$. Suppose that $M_i(z)$ is a zero divisor for every $i = 1,\dots,l$. Then, for every $i = 1,\dots,l$, there is an element $r_i \in R$ such that $r_i \cdot M_i(z) = 0$. Since R is a principal ideal artinian local ring, the nilradical is the unique prime ideal; it is generated by an element $\pi \in R$, and there is a natural number $\theta > 0$ such that $\pi^\theta = 0$. Then, $r_i \cdot M_i(z) = 0$ implies that

$$\begin{aligned} r_i &= \lambda_i \pi^{t_i},\ \lambda_i \in R^*,\ t_i > 0,\\ m_{ij} &= \mu_j \pi^{s_{ij}},\ \mu_j \in R^*,\ s_{ij} \geq 0,\\ t_i + s_{ij} &\geq \theta. \end{aligned}$$

Here m_{ij} is the jth order coefficient of $M_i(z)$. Let $r \in R$ be the element among the r_is with maximum exponent t_i. Then,

$$r \cdot M_i(z) = 0,\ \forall i = 1,\dots,l,$$

which, in turn, implies that $0 \neq r \in \mathrm{Ann}_{R[z]}(< M_1(z),\dots,M_l(z) >)$. Since this is not possible, we deduce that there exists a full-size minor, $M_i(z)$, which is not a zero divisor. □

Remark 6. *Note that Proposition 2 is not true if we drop the condition of being local. For instance, consider the ring $R = \mathbb{Z}_2 \times \mathbb{Z}_3$. This is a principal artinian non-local ring. Additionally, consider the matrix*

$$G(z) = \begin{pmatrix} 2z \\ 3z \end{pmatrix}.$$

It is clearly a convolutional encoder with PDP. However, both $2z$ and $3z$ are zero divisors and, therefore, not invertible in $Q(R[z])$, so $G(z)$ is not systematic.

Before proving the main results, we give some definitions about equivalence between convolutional codes over R.

Definition 12. *Let R be a commutative ring. Two (k,n) convolutional codes, $\mathcal{C}, \mathcal{C}' \subset R[z]^n$, are equivalent if there is a permutation $\sigma \in \mathfrak{S}_n$ of n elements such that $\sigma(\mathcal{C}) = \mathcal{C}'$.*

Definition 13. *Let R be a commutative ring. Two convolutional codes, $\mathcal{C}, \mathcal{C}' \subset R[z]^n$, are locally equivalent if for any prime ideal $\mathfrak{p} \in Spec(R)$, $\mathcal{C}_\mathfrak{p}$ and $\mathcal{C}'_\mathfrak{p}$ are equivalent.*

Definition 14. *Let R be a commutative ring. Two convolutional encoders, $G(z), G'(z) \in R[z]^{n\times k}$, are weakly (locally) equivalent if $\mathcal{C} := Im(G(z))$ is (locally) equivalent to $\mathcal{C}' := Im(G'(z))$.*

Accordingly, $G(z)$ and $G'(z)$ are weakly equivalent if and only if there is a permutation $\sigma \in \mathfrak{S}_n$ of n elements and an invertible matrix $P \in GL_k(R[z])$ such that $G(z) = \sigma \cdot G'(z) \cdot P$.

Now, we prove the existence of I/S/O representations for principal ideal artinian rings.

Theorem 3. *For any convolutional encoder $G(z) \in R[z]^{n\times k}$ with PDP over a principal ideal artinian local ring, there is a permutation $\sigma \in \mathfrak{S}_n$ such that $\sigma(Im(G(z)))$ admits an I/S/O representation.*

Proof. Let $G(z) \in R[z]^{n\times k}$ be a convolutional encoder with PDP and degree δ. By Theorem 2, we can find a minimal first-order representation (K, L, M) of $\mathrm{Im}(G(z))$. Moreover, we can assume that $(K(\mathfrak{m}), L(\mathfrak{m}), M(\mathfrak{m}))$ is a minimal first-order representation of the convolutional encoder $G(\mathfrak{m})(z) \in k(\mathfrak{m})[z]^{n\times k}$ (see proof Remark 4), where $\mathfrak{m}$ is the

unique prime ideal of R. From Section 5.2, [32], we know that, after a permutation of the code words of $G(z)$ (let us denote such a permutation by $\sigma \in \mathfrak{S}_n$), the full-size minor, $\det(F)$, of (K, M) consisting of the first $\delta + n - k$ columns, satisfies the condition that $F \bmod(\mathfrak{m}) \in k(\mathfrak{m})^{(\delta+n-k)\times(\delta+n-k)}$ is invertible, where $k(\mathfrak{m}) = R/\mathfrak{m}$ is the residue field. This implies that $\det(F) \notin \mathfrak{m}$, which means that $F \in R^{(\delta+n-k)\times(\delta+n-k)}$ is invertible because R is a principal ideal artinian ring. Then, the matrix $F^{-1}(K, L, M)$ takes the form

$$\begin{pmatrix} -\mathrm{Id}_\delta & A & \mathbf{0} & B \\ \mathbf{0} & C & -\mathrm{Id}_{n-k} & D \end{pmatrix},$$

and clearly, $A \in R^{\delta\times\delta}$, $B \in R^{\delta\times k}$, $C \in R^{n-k\times\delta}$, $D \in R^{n-k\times k}$ form an I/S/O representation of $\mathrm{Im}(\sigma(G(z))) = \sigma(\mathrm{Im}(G(z)))$. □

Remark 7. *Let $k \leq n \in \mathbb{N}$, R a principal ideal artinian ring and $G(z) \in R[z]^{k\times n}$ a convolutional encoder with PDP. If Σ is an I/S/O representation of $Im(G(z))$, then $\Sigma(\mathfrak{p}) = (A(\mathfrak{p}), B(\mathfrak{p}), C(\mathfrak{p}), D(\mathfrak{p}))$ is an I/S/O representation of $Im(G(\mathfrak{p})(z))$ for each $\mathfrak{p} \in SpecR$). This follows from Remark 4.*

Corollary 2. *For any convolutional encoder $G(z)$ with PDP over a principal ideal artinian ring, there is a locally weakly equivalent encoder $G'(z)$ such that $\mathcal{C}' := \mathrm{Im}(G'(z))$ admits I/S/O representation.*

Proof. Let $G(z)$ be a convolutional encoder with PDP and degree δ, and let $\mathrm{Spec}(R) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_q\}$ be the set of prime (in fact maximal) ideals. For each $i = 1, \ldots, q$, $R_i := R_{\mathfrak{m}_i}$ is a principal ideal local artinian ring, so, by Theorem 3, there are permutations $\sigma_{\mathfrak{m}_1}, \ldots, \sigma_{\mathfrak{m}_q} \in \mathfrak{S}_n$ such that the convolutional code over $R_{\mathfrak{m}_i}$ defined by the convolutional encoder

$$\frac{\sigma_{\mathfrak{m}_q}(G(z))}{1} \in R_{\mathfrak{m}_i}[z]^{n\times k}$$

admits an I/S/O representation. Now, let $\sigma \in \mathrm{GL}_n(R)$ be the unique invertible matrix such that $\sigma_{\mathfrak{m}_i} = \dfrac{\sigma}{1} \in \mathrm{GL}_n(R_{\mathfrak{m}_i})$. Then, $\mathrm{Im}(\sigma \cdot G(z))$ is locally equivalent to $\mathrm{Im}(G(z))$. □

The case of the ring of modular integers $\mathbb{Z}_M$ is of particular interest in convolutional coding theory over commutative rings. These rings are principal ideal artinian rings. Observe that Theorem 3 (respectively, Corollary 2) shows, in particular, that any convolutional code with PDP over a ring of modular integers $\mathbb{Z}_{p^r}$ with p a prime number (respectively, $\mathbb{Z}_M$ with M a natural number) is equivalent (respectively, locally equivalent) to a convolutional encoder with a I/S/O representation.

Example 2. *Let $G(z)$ be the following PDP encoder of a $(n = 3, k = 2, \delta = 4)-$ convolutional code $\mathcal{C}$ over $\mathbb{Z}_8$.*

$$G(z) = \begin{pmatrix} 1 + z^2 & 1 + z + 4z^2 \\ 5 + 4z & 3 + 6z + 3z^2 \\ 2z + z^2 & z \end{pmatrix}.$$

From $G(z)$ we obtain the triple of matrices $(K \mid L \mid M)$.

$$K = \begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 7 & 7 & 4 \\ 4 & 0 & 2 & 5 \\ 6 & 6 & 1 & 0 \end{pmatrix}, L = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 7 & 0 & 7 & 0 \\ 3 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Since

$$\begin{vmatrix} 7 & 0 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 \\ 0 & 7 & 7 & 4 & 1 \\ 4 & 0 & 2 & 5 & 0 \\ 6 & 6 & 1 & 0 & 0 \end{vmatrix} = 6$$

and $6 \notin \mathbb{Z}_8^*$*, we can not obtain the I/S/O representation. We perform the permutation* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *in* $G(z)$*,*

$$G'(z) = \begin{pmatrix} 2z + z^2 & z \\ 1 + z^2 & 1 + z + 4z^2 \\ 5 + 4z & 3 + 6z + 6z^2 \end{pmatrix}.$$

From $G(z)$*, we obtain the triple of matrices* $(K \mid L \mid M)$*.*

$$K = \begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 6 & 7 & 7 & 0 \\ 0 & 7 & 7 & 4 \\ 4 & 0 & 2 & 5 \end{pmatrix}, L = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 7 & 0 & 7 & 0 \\ 3 & 0 & 5 & 0 \end{pmatrix}, M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since

$$\begin{vmatrix} 7 & 0 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 \\ 7 & 7 & 7 & 0 & 1 \\ 0 & 7 & 7 & 4 & 0 \\ 4 & 0 & 2 & 5 & 0 \end{vmatrix} = 5,$$

and $5 \in \mathbb{Z}_8^*$*, we can obtain the I/S/O representation. In fact, we compute*

$$\mathcal{K} = \begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \mathcal{L} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 3 & 0 & 3 & 7 \\ 0 & 0 & 0 & 1 \\ 1 & 4 & 7 & 6 \\ 3 & 2 & 3 & 0 \end{pmatrix}, \mathcal{M} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \\ 7 & 1 & 4 \end{pmatrix}.$$

From the above first-order representation, we obtain

$$\Sigma = \left[A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 3 & 0 & 3 & 7 \\ 0 & 0 & 0 & 1 \\ 1 & 4 & 7 & 6 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 4 \\ 0 & 0 \\ 0 & 3 \end{pmatrix}, C = \begin{pmatrix} 3 & 2 & 3 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 4 \end{pmatrix} \right].$$

Example 3. *Let* $G(z)$ *be the following PDP encoder of a* $(n = 4, k = 2, \delta = 6)-$ *convolutional code* $\mathcal{C}$ *over* $\mathbb{Z}_4$*.*

$$G(z) = \begin{pmatrix} 1 + z + z^3 & 0 \\ 0 & 1 + z + z^3 \\ 1 + z^2 + z^3 & 1 + z + z^2 + z^3 \\ 1 + z^3 & 1 + z^2 \end{pmatrix}.$$

From $G(z)$, we obtain the triple of matrices $(K \mid L \mid M)$.

$$K = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 3 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 3 \\ 0 & 3 & 3 & 3 & 3 & 3 \\ 0 & 0 & 3 & 0 & 3 & 0 \end{pmatrix}, L = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 \end{pmatrix}, M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Since

$$\begin{vmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 & 3 & 0 & 1 \\ 0 & 3 & 3 & 3 & 3 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 & 3 & 0 & 0 & 0 \end{vmatrix} = 3$$

and $3 \in \mathbb{Z}_4^*$, we can obtain the I/S/O representation. In this case,

$$\mathcal{K} = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \mathcal{L} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 & 3 & 0 \\ 0 & 1 & 0 & 3 & 0 & 3 \\ 0 & 0 & 3 & 3 & 0 & 0 \end{pmatrix}, \mathcal{M} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 1 & 3 \end{pmatrix}.$$

From the above first-order representation, we obtain

$$\Sigma = \left[A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 & 3 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 3 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 & 0 & 3 & 0 & 3 \\ 0 & 0 & 3 & 3 & 0 & 0 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \right].$$

5. Minimal I/S/O Representations: Reachability and Observability

Minimality is one of the most important properties of an I/S/O representation of a convolutional code. An I/S/O representation is minimal when it has the smallest dimension among all I/S/O representations of the code. These representations require less memory space in their implementations, which provides more efficiency. The problem of the existence of minimal representations was initially highlighted in the case of quaternary convolutional codes over $\mathbb{Z}_4$ and their trellis representations ([29]). After this, the minimality problem of I/S/O representations over finite fields was solved in [3,6] through the reachability property (controllability in coding literature) of the associated linear system. In general, the minimality problem is hard to solve, and each case needs to be studied. In the case of convolutional codes over finite rings, the minimality of the I/S/O representation is achieved by the reachability of the system. For instance, the necessary and sufficient conditions for the minimality of the state-space model for basic 2D convolutional codes

over finite fields were found by a property of strongly modally reachability in [37], or by separable Roesser models for 2D periodic convolutional codes in [38].

We review a result about reachability properties of systems over commutative rings with identity that let us prove the minimality of I/S/O representations of convolutional codes over principal ideal artinian rings.

Proposition 3 (Theorem 2.3, [39] and Proposition 2.1, [26]). *Let $\Sigma = (A, B, C, D) \in R^{\delta\times\delta} \times R^{\delta\times k} \times R^{n\times\delta} \times R^{n\times k}$ be a linear system over R. The following statements are equivalent:*

(1) Σ is reachable.
(2) The columns of $\Phi_\delta = \begin{pmatrix} B & AB & \dots & A^{\delta-1}B \end{pmatrix}$ generate R^δ.
(3) The map ϕ: $R^{k\delta} \to R^\delta$ 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 $(zI - A, B) : R[z]^{\delta+k} \to R[z]^\delta$ is surjective.

Theorem 4. *Let $\mathcal{C}$ be a (k, n, δ) be a convolutional code over a principal ideal artinian ring R. Let $\Sigma = (A, B, C, D) \in R^{\delta\times\delta} \times R^{\delta\times k} \times R^{n-k\times\delta} \times R^{n-k\times k}$ be an I/S/O representation of $\mathcal{C}$. Then, Σ is a reachable linear system.*

Proof. Follows from Remark 4, Remark 7 and Proposition 3 (5). □

Example 4. *Let $G(z)$ be the PDP encoder*

$$G(z) = \begin{pmatrix} 1+z^2 & 1+z+4z^2 \\ 5+4z & 3+6z+3z^2 \\ 2z+z^2 & z \end{pmatrix}.$$

The encoder generates a $(n = 3, k = 2, \delta = 4)$ convolutional code, $\mathcal{C}$, over $\mathbb{Z}_8$, whose I/S/O representation was obtained in Example 2. Since

$$rank\begin{pmatrix} B & AB & A^2B & A^3B \end{pmatrix} = rank\begin{pmatrix} 0 & 0 & 1 & 4 & 0 & 5 & 7 & 3 \\ 1 & 4 & 0 & 5 & 7 & 3 & 3 & 4 \\ 0 & 0 & 0 & 3 & 4 & 2 & 1 & 1 \\ 0 & 3 & 4 & 2 & 1 & 1 & 6 & 5 \end{pmatrix}$$

is maximum because

$$|\Phi_4| = \begin{vmatrix} 0 & 0 & 1 & 4 \\ 1 & 4 & 0 & 5 \\ 0 & 0 & 0 & 3 \\ 0 & 3 & 4 & 2 \end{vmatrix} = 7$$

is invertible in $\mathbb{Z}_8$, we deduce that Σ is reachable and, hence, a minimal I/S/O representation of $\mathcal{C}$.

Example 5. *Consider now the encoder given in Example 3 and its I/S/O representation. Note that*

$$\begin{pmatrix} B & AB & A^2B & A^3B & A^4B & A^5B \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 3 & 1 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 1 & 3 & 0 & 1 & 0 \\ 0 & 1 & 3 & 1 & 0 & 1 & 3 & 0 & 1 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 & 1 & 3 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 3 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 \end{pmatrix}.$$

Since

$$|\Phi_6| = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 \\ 0 & 1 & 3 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 3 & 0 & 3 \\ 1 & 3 & 0 & 3 & 0 & 0 \end{vmatrix} = 1,$$

$rank\begin{pmatrix} B & AB & A^2B & A^3B & A^4B & A^5B \end{pmatrix}$ is maximum, so the I/S/O representation given in Example 3 is minimal.

Construction of Observable Convolutional Codes over R

We recall the following result regarding observability property.

Proposition 4 (Theorem 2.6, [39]). *Let $\Sigma = (A, B, C, D) \in R^{\delta\times\delta} \times R^{\delta\times k} \times R^{n\times\delta} \times R^{n\times k}$ be a linear system over R. The following statements are equivalent.*

(1) Σ is observable.
(2) Let $\Omega_\delta = [C, CA, ..., CA^{\delta-1}]^t$ (here, we mean the block transpose of the matrix $[C, CA, ..., CA^{\delta-1}]$) be the observability matrix. Then, rank $(\Omega_\delta) = \delta$.
(3) The map τ: $R^\delta \to R^{p\delta}$ 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.

Theorem 5. *Let R be a principal ideal artinian ring. Let $\Sigma = (A, B, C, D) \in R^{\delta\times\delta} \times R^{\delta\times k} \times R^{n-k\times\delta} \times R^{n-k\times k}$ be a reachable and observable linear system over R. We construct the triple of matrices (K, L, M) as follows:*

$$K = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, L = \begin{pmatrix} A \\ C \end{pmatrix} \text{ and } M = \begin{pmatrix} O & B \\ -I_{(n-k)} & D \end{pmatrix} \tag{14}$$

and we consider the associated convolutional code $\mathcal{C}$ obtained by $Ker(zK + L \mid M)$. Then, $\mathcal{C}$ is observable.

Proof. Follows from Remark 4, Remark 7, Proposition 1 (2), Proposition 4 (3) and Lemma 5.3.5 in [32]. □

Example 6. *Let Σ be the following linear systems over $\mathbb{Z}_8$*

$$\Sigma = \left[A = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 5 & 1 \\ 4 & 7 \end{pmatrix}, C = \begin{pmatrix} 1 & 5 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \end{pmatrix}\right].$$

Since the two first columns of Φ_2 generate $\mathbb{Z}_8^2$ because

$$\Phi_2 = \begin{pmatrix} B & AB \end{pmatrix} = \begin{pmatrix} 5 & 1 & 1 & 6 \\ 4 & 7 & 4 & 7 \end{pmatrix};$$

then, Σ is reachable. Furthermore, since

$$\Omega_2 = \begin{pmatrix} C & CA \end{pmatrix}^t = \begin{pmatrix} 1 & 1 \\ 5 & 0 \end{pmatrix},$$

then, Σ is observable because $\mid \Omega_2 \mid = 3 \in \mathbb{Z}_8^*$. From Σ, we compute the first-order representation

$$\mathcal{K} = \begin{pmatrix} 7 & 0 \\ 0 & 7 \\ 0 & 0 \end{pmatrix}, \mathcal{L} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \\ 1 & 5 \end{pmatrix}, \mathcal{M} = \begin{pmatrix} 0 & 5 & 1 \\ 0 & 4 & 7 \\ 7 & 0 & 1 \end{pmatrix}.$$

Finally, we obtain the associated $(3,2,2)$ *convolutional encoder by* $Ker(zK+L \mid M)$*:*

$$G(z) = \begin{pmatrix} 4z-1 & 3z+6 \\ z-1 & z+4 \\ 4z-4 & 3z+1 \end{pmatrix}.$$

This is an observable convolutional encoder since the full-size minors of $G(z)$*,* $\mathcal{U}_i$*, generate the ring; that is, there exist* λ_1, λ_2 *and* λ_3 *such that* $\lambda_1 \cdot \mathcal{U}_1 + \lambda_2 \cdot \mathcal{U}_2 + \lambda_3 \cdot \mathcal{U}_3 \in (\mathbb{Z}_8[z])^*$*:* $1 \cdot (z^2+2z+2) + 4 \cdot (-z+5) + 1 \cdot (7z^2+2z+7) = 5$*.*

6. Conclusions

In this work, we proved several results that let us extend the relation between convolutional codes and I/S/O representations known in classical convolutional coding theory to convolutional codes defined over a principal ideal artinian rings, such as $\mathbb{Z}_{p^r}$.

First of all, we demonstrated the existence of first-order representations for convolutional codes with the PDP over any principal ideal artinian ring. Secondly, this first-order representation allows us to obtain, when the base ring is local, an I/S/O representation Σ for the (equivalence class of the) code. The local property of the ring ensures that every polynomial convolutional encoder of the code is systematic, a necessary condition to obtain Σ. Since Σ determines a reachable linear system, we can conclude that the representation is minimal. Furthermore, we proved that we can weaken (in a natural way) the equivalence relation for codes in such a way that the same result obtained in the local case is also true in the non local case. Finally, we showed that we can construct observable convolutional codes over principal ideal artinian local rings from reachable and observable linear systems as is carried out in classical convolutional theory. All the results can be applied over $\mathbb{Z}_M$, where M is a positive integer.

There are two interesting applications of the existence of an I/S/O in classical convolutional coding theory. On the one hand, one can derive (algebraic) decoding algorithms for convolutional codes based on I/S/O representations. On the other hand, I/S/O representations have proven to be very useful in the study of the different notions of distances (free distances, column distances, etc.) in classical convolutional coding theory.

The results of this work suggest that these two problems, in the theory of convolutional codes over principal ideal artinian rings, could be tackled in the same way as has been done in classical theory.

Furthermore, it would be interesting to see if the results presented in this article can be used to design good component codes for Turbo codes.

Author Contributions: Conceptualization, A.L.M.C., N.D.-G. and M.V.C.; methodology, A.L.M.C., N.D.-G. and M.V.C.; investigation, A.L.M.C., N.D.-G. and M.V.C.; writing–original draft preparation, A.L.M.C., N.D.-G. and M.V.C.; writing–review and editing, A.L.M.C., N.D.-G. and M.V.C.; visualization, A.L.M.C., N.D.-G. and M.V.C.; supervision, A.L.M.C., N.D.-G. and M.V.C.; project administration, A.L.M.C., N.D.-G. and M.V.C.; funding acquisition, A.L.M.C., N.D.-G. and M.V.C.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. McEliece, R.L. The algebraic theory of convolutional codes. In *Handbook of Coding Theory I*; Springer: Berlin, Germany, 1998; pp. 1065–1138.
2. Massey, J.; Sain, M. Codes, automata, and continuous systems: Explicit interconnections. *IEEE Trans. Autom. Control* **1967**, *12*, 644–650. [CrossRef]
3. Rosenthal, J.; York, F. BCH convolutional codes. *IEEE Trans. Inf. Theory* **1999**, *45*, 1833–1844. [CrossRef]
4. Kuijper, M.; Polderman, J. Reed-Solomon list decoding from a system-theoretic perspective. *IEEE Trans. Inf. Theory* **2004**, *50*, 259–271. [CrossRef]
5. Rosenthal, J. Connections between Linear Systems and Convolutional Codes. In *Codes, Systems, and Graphical Models*; Marcus, B., Rosenthal, J., Eds.; Springer: New York, NY, USA, 2001; pp. 39–66.
6. Rosenthal, J.; Schumacher, J.; York, E. On behaviors and convolutional codes. *IEEE Trans. Inf. Theory* **1996**, *42*, 1881–1891. [CrossRef]
7. Kuijper, M. *First Order Representations of Linear Systems*; Systems & Control: Foundations & Applications; Birkhäuser: Basel, Switzerland, 1994.
8. Kuijper, M.; Schumacher, J. Realization of Autoregressive Equations in Pencil and Descriptor Form. *SIAM J. Control Optim.* **1990**, *28*, 1162–1189. [CrossRef]
9. Willems, J.C. From time series to linear systems Part I. Finite dimensional linear time invariant systems. *Automatica* **1986**, *22*, 561–580. [CrossRef]
10. Kitchens, B. Symbolic Dynamics and Convolutional Codes. In *Codes, Systems, and Graphical Models*; Marcus, B., Rosenthal, J., Eds.; Springer: New York, NY, USA, 2001; pp. 347–360.
11. Climent, J.; Herranz, V.; Perea, C. A first approximation of concatenated convolutional codes from linear systems theory viewpoint. *Linear Algebra Its Appl.* **2007**, *425*, 673–699. [CrossRef]
12. Climent, J.; Napp, D.; Pinto, R.; Simões, R. Series concatenation of 2D convolutional codes by means of input-state-output representations. *Int. J. Control* **2018**, *91*, 2682–2691. [CrossRef]
13. Napp, D.; Perea, C.; Pinto, R. Input-state-output representations and constructions of finite support 2D convolutional codes. *Adv. Math. Commun.* **2010**, *4*, 533–545. [CrossRef]
14. Napp, D.; Pereira, R.; Rocha, P. A State Space Approach to Periodic Convolutional Codes. In *Coding Theory and Applications*; Barbero, Á.I., Skachek, V., Ytrehus, Ø., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 238–247.
15. Climent, J.; Napp, D.; Pinto, R.; Requena, V. Minimal State-Space Representation of Convolutional Product Codes. *Mathematics* **2021**, *9*, 1410. [CrossRef]
16. Rosenthal, J. An Algebraic Decoding Algorithm for Convolutional Codes. In *Dynamical Systems, Control, Coding, Computer Vision*; Picci, G., Gilliam, D.S., Eds.; Birkhäuser Basel: Basel, Switzerland, 1999; pp. 343–360.
17. Muñoz Castañeda, A.L.; Muñoz Porras, J.M.; Plaza-Martín, F.J. Rosenthal's Decoding Algorithm for Certain 1-Dimensional Convolutional Codes. *IEEE Trans. Inf. Theory* **2019**, *65*, 7736–7741. [CrossRef]
18. Massey, J.; Mittelholzer, T. Convolutional codes over rings. In Proceedings of the Joint Swedish-Soviet International Workshop on Information Theory, Gotland, Sweeden, 27 August–1 September 1989; pp. 14–18.
19. Massey, J.; Mittelholzer, T. Systematicity Furthermore, Rotational Invariance Of Convolutional Codes Over Rings. In Proceedings of the International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk, Russia, 2–8 September 1990; pp. 154–158.
20. Johannesson, R.; Zhe-Xian, W.; Wittenmark, E. Some structural properties of convolutional codes over rings. *IEEE Trans. Inf. Theory* **1998**, *44*, 839–845. [CrossRef]
21. Fagnani, F.; Zampieri, S. System-theoretic properties of convolutional codes over rings. *IEEE Trans. Inf. Theory* **2001**, *47*, 2256–2274. [CrossRef]
22. El Oued, M.; Napp, D.; Pinto, R.; Toste, M. On duals and parity-checks of convolutional codes over Zpr. *Finite Fields Their Appl.* **2019**, *55*, 1–20. [CrossRef]
23. Kuijper, M.; Pinto, R. On Minimality of Convolutional Ring Encoders. *IEEE Trans. Inf. Theory* **2009**, *55*, 4890–4897. [CrossRef]
24. Napp, D.; Pinto, R.; Toste, M. Column Distances of Convolutional Codes Over $\mathbb{Z}_{p^r}$. *IEEE Trans. Inf. Theory* **2019**, *65*, 1063–1071. [CrossRef]
25. DeCastro-García, N. Feedback equivalence of convolutional codes over finite rings. *Open Math.* **2017**, *15*, 1495–1508. [CrossRef]
26. DeCastro-García, N.; García-Planas, M.I. Concatenated linear systems over rings and their application to construction of concatenated families of convolutional codes. *Linear Algebra Its Appl.* **2018**, *542*, 624–647. [CrossRef]
27. DeCastro-García, N. Feedback Classification of Linear Systems and Convolutional Codes. Applications in Cybernetics, Coding Theory and Cryptography. Ph.D. Thesis, Universidad de Len, León, Spain, 2016.
28. Forney, G. Convolutional codes I: Algebraic structure. *IEEE Trans. Inf. Theory* **1970**, *16*, 720–738. [CrossRef]
29. Sole, P.; Sison, V. Quaternary Convolutional Codes From Linear Block Codes Over Galois Rings. *IEEE Trans. Inf. Theory* **2007**, *53*, 2267–2270. [CrossRef]
30. Seshadri, C.S. Triviality of Vector Bundles over the Affine Space K2. *Proc. Natl. Acad. Sci. USA* **1958**, *44*, 456–458. [CrossRef] [PubMed]

31. Mittelholzer, T.; Honor, B.; Darnell, M.; Farell, P. Minimal encoders for convolutional codes over rings. In *Communications Theory and Applications*; HW Communications Ltd.: Lancaster, UK, 1993; pp. 30–36.
32. York, E. Algebraic Description and Construction of Error Correcting Codes, a Systems Theory Point of View. Ph.D. Thesis, University of Notre Dame, Notre Dame, IN, USA, 1997.
33. Johannesson, R.; Zigangirov, K.S. *Fundamentals of Convolutional Coding*, 2nd ed.; Wiley-IEEE Press: Hoboken, NJ, USA, 2015.
34. Forney, J.; David, G. Minimal Bases of Rational Vector Spaces, with Applications to Multivariable Linear Systems. *SIAM J. Control* **1975**, *13*, 493–520. [CrossRef]
35. Kaplansky, I. Projective Modules. *Ann. Math.* **1958**, *68*, 372–377. [CrossRef]
36. Campillo, A.; Sánchez Giralda, T. Finitely generated projective modules and Fitting ideals. *Collect. Math.* **1979**, *30*, 97–102.
37. Pinto, R.; Simões, R. On Minimality of ISO Representation of Basic 2D Convolutional Codes. In *Coding Theory and Applications*; Barbero, Á.I., Skachek, V., Ytrehus, Ø., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 257–271.
38. Napp, D.; Pereira, R.; Pinto, R.; Rocha, P. Realization of 2D (2,2)–Periodic Encoders by Means of 2D Periodic Separable Roesser Models. *Int. J. Appl. Math. Comput. Sci.* **2019**, *29*, 527–539. [CrossRef]
39. Brewer, J.W.; Bunce, J.W.; Van Vleck, F.S. *Linear Systems over Commutative Rings*; Dekker: New York, NY, USA, 1986.