UNIVERSIDAD DE LEÓN

Escuela de Ingenierías Industrial e Informática.

(School of Engineering, Computing and Aerospace.)

Doctorado en Ingeniería de la Computación.

(Ph. D. Engineering of Computation).

FEEDBACK CLASSIFICATION OF LINEAR SYSTEMS AND CONVOLUTIONAL CODES. APPLICATIONS IN CYBERNETICS, CODING THEORY AND CRYPTOGRAPHY.

by Noemí de Castro García.

Advisors: Dr. Miguel Carriegos Vieira.

Dr. Andrés Sáez Schwedt.

Research line: Linear algebra and its applications.

Dedicado a mi familia
y a Ángel.

Agradecimientos

Esta tesis ha sido realizada con la ayuda y apoyo de diferentes personas a las que quiero dedicar las siguientes líneas para expresar mi más profundo y sincero agradecimiento.

Las primeras personas a las que quiero dar las gracias son mi familia. Gracias a mis padres por los sacrificios realizados, por haberme inculcado el valor del esfuerzo y la humildad, por creer en mí. Gracias por todo el cariño, el cuidado, la ayuda y el aguante de todos estos años. Gracias por haberme soportado, levantado y apoyado, y haber estado siempre a mi lado, en cualquier momento y desde cualquier lugar. Nunca os lo agradeceré lo suficiente. Gracias abuel@s. Gracias a Jacobo y Esther por cuidarme, por vuestra preocupación, por hacerme reír cada día y por haberme ayudado cuando lo he necesitado. Gracias Iván, por enseñarme cada día, por recordarme a cada momento qué es lo importante, por hacer que quiera ser mejor y por sacarme una sonrisa en los momentos más duros. Gracias a todos, cada uno de vuestros abrazos fue significativo y la mejor fuente de energía para continuar.

En segundo lugar dar las gracias a mis amigos por aguantar mis ausencias durante largas temporadas. Gracias por venir a verme, por las charlas tras la pantalla del ordenador y por vuestro interés aunque mis historias matemáticas no fueran el tema más interesante del momento.

En tercer lugar me gustaría dar las gracias a aquellas personas que durante estos años me han ayudado a crecer personal y, sobre todo, profesionalmente. Gracias Andrés por las observaciones y correcciones realizadas, tus orientaciones me han sido muy útiles en la elaboración de la tesis. Gracias Maite por nuestras colaboraciones, por tu preocupación y tus consejos. Gracias Montse por tu ayuda cuando esta tesis no era más que un trabajo fin de Máster y, finalmente, dar las gracias a Adriana por ayudarme con el inglés.

Gracias Miguel. Tengo que agradecerte de manera especial que me hayas enseñado a

hacer matemáticas (aún lo intento) y toda la paciencia que has mostrado en el proceso . Gracias por tu tiempo (24 horas, 365 días), por ser un gran maestro y un gran Director de Tesis. Gracias por las discusiones matemáticas, por buscar mis límites y por nuestras charlas. Ante todo, gracias por tu confianza y por darme la oportunidad.

Mis últimos agradecimientos están dedicados a ti, Ángel. Tengo tantas gracias que darte que no se por dónde empezar. Gracias por tu ayuda constante, por enseñarme tantas matemáticas durante estos años, por tu apoyo incondicional, por los ánimos diarios y por tu infinita calma cuando la mía desaparecía. Esta tesis no hubiera sido posible sin ti a mi lado (aunque haya sido un lado un tanto lejos). Gracias por cruzarte en mi vida, por hacerme feliz y por demostrarme cada día que *somos globales* $\Leftrightarrow$ *somos en cualquier parte del mundo* $\forall$ *el rato.*

Gracias a todos.

Publications and Conferences.

We would like to remark that several items in our work have been submitted and published in different journals:

- M.V. Carriegos, Noemí DeCastro-García, M.M.Cb. López, Enumeration of locally Brunovsky linear systems over $\mathcal{C}(\mathbb{S}^1)$-modules. A procedure. *Cybernetics and Physics*,Vol. 2, (2013), pp. 72-76, [15].

- M. V. Carriegos, Noemí DeCastro-García, Partitions of elements in a monoid and its applications to systems theory, *Linear Algebra and Its Applications.In press.* doi:10.1016/j.laa.2015.05.03, [13].

- M.V Carriegos, Noemí DeCastro-García A.L. Muñoz Castañeda, A characterization of von Neumann regular rings in terms of linear systems, *Submitted to Linear Algebra and Its applications*, September (2015), [17].

- M.V Carriegos, Noemí DeCastro-García A.L. Muñoz Castañeda, Realizable rings and its applications to construct observable families of convolutional codes, *Work in Progress*, Date to submit to *Journal of algebra and its applications*: December, 2015.

Moreover, first results of the thesis were presented in some meetings and conferences by the author of the thesis:

- Join ALAMA-GAMM/ANLA Meeting celebrated at Universidad Politécnica de Catalunya, Barcelona, from 14 to 16 of June of 2014. Presented work: *First Order Representations of Convolutional Codes over Finite Rings. A proof.*

- 19th Conference of ILAS (International Linear Algebra Society) celebrated in Seoul, South Korea, from 6 to 9 of August of 2014, satellite conference of ICM of 2014. Presented work: *Enumeration of classes of feedback isomorphisms of Locally Brunovsky Linear Systems.*

Summary of Contents

Introduction

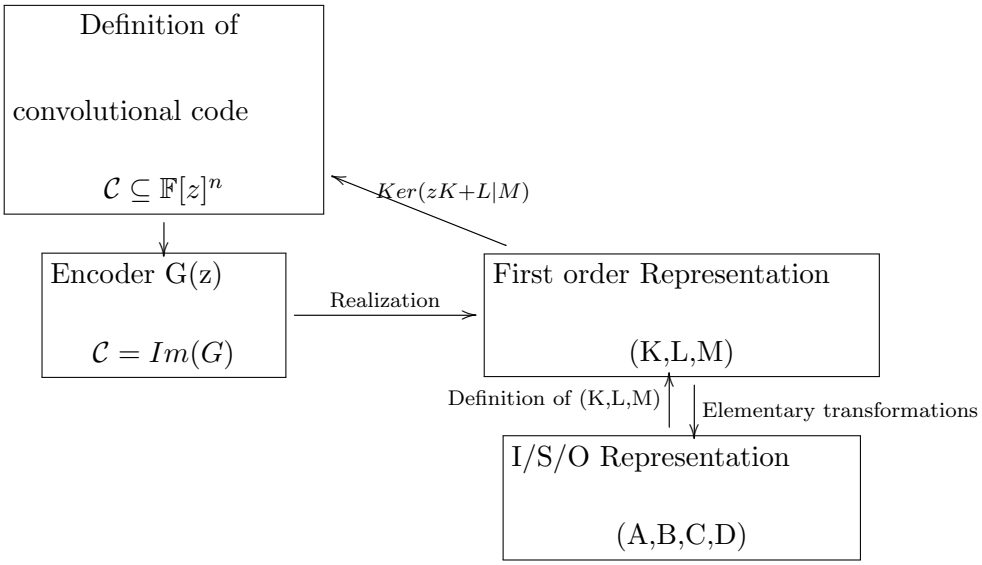
Several natural phenomena are mathematically modeled through linear systems of differential equations. The dynamical behaviour that we study in this work is feedback criterion. In order to decide when two physical systems have similar feedback behaviour we consider the matrices which define them. The classification problem of linear systems finishes, over finite vector spaces, building the Brunovsky canonical forms (see [8] and [44]). However, if we want a more realistic approach it is needed to extend the process to all possible algebraic structures. We study locally Brunovsky linear systems over commutative rings with identity and, in this context, known results about systems classification are not easily generalizable. Our first goal in this work is, applying results of [10], to give the number of classes of feedback isomorphisms of locally Brunovsky linear systems with state space X over different commutative rings by partitions in a monoid.

Another goal of this work is to give explicit interconnections between control theory and coding. This approach goes back to [70], [71] and [83], where a wide class of codes are shown to be linear systems. It should also be noticed that we are using algebraic tools in this work similar to the ones in [2], [5], [6], [7], [18], [39], [46], [50], [80] or [84].

Convolutional codes are a class of error-correcting codes used to detect and correct digital data transmission systems. Moreover, there exists a closed relation between linear systems over finite fields and convolutional codes that allows us to understand some properties of convolutional codes and to construct them. The link is given in terms of sets of matrices. First we get a first order representation (K, L, M) and finally we obtain the set of matrices (A, B, C, D) that gives us an I/S/O (input/state/output) representation from systems theory approach, where the inputs and outputs of a system are part of the codeword (the main results can be found in [47], [70], [71], and [83]). Decoder process of the code is given by the output controllability matrix; i.e., the matrix which solves the associated linear dynamical system, see [27], [28] and [29].

For the reader's convenience we gather the above results in a diagram where an arrow

means that a procedure is available to perform the path.



The natural question is whether we can generalize the above diagram to commutative rings with identity. We study this generalization (definition, properties, first order and I/S/O representations) for the family of convolutional codes over certain commutative rings with identity. Furthermore, we construct observable family of convolutional codes by reachable and observable I/S/O representations.

Finally, we study equivalence relations between certain families of convolutional codes and its I/S/O representations by their Kronecker Indices and their conjugate partitions. This final result is given by the correspondences between classes of feedback isomorphisms of locally Brunovsky linear system and classes of feedback isomorphisms of dynamical behaviours of I/S/O representations of certain families of convolutional codes.

The work is composed in four parts together with some appendices. Part I is devoted to gather some recent results in linear (control) systems in Chapter 1 and then, in Chapter 2, to write down our original results on linear systems over regular rings and Dedekind domains. Part II deals with convolutional codes, which are a remarkable class of linear systems. This approach is highlighted in Chapter 3 where we survey the main results in the topic. Chapter 4 collects our original new results. Part III is devoted to feedback actions and equivalence. We introduce the notion of feedback equivalence of a family of convolutional codes as a new original research topic. Finally our conclusions are listed in Part IV and a spanish summary in Part V. Along this work, R always denotes a commutative ring with identity.

Part I

Linear Systems.

‘

'Existence implies feedback and is prior to understanding. That is, things exist, like cells, children, massive computer programs using inductive loops, ecological systems with complex feedback, etc, but we may not or do not understand them. Understanding comes later in the form of introducing coordinates', [63].

Systems theory and feedback equivalence is currently one of the main holistic matters in science and engineering, see [62] and [76]. Feedback equivalence of linear systems over commutative rings has been largely studied using commutative algebra, see [5],[6],[7], [38] and [78] for details.

It is well known that Brunovsky's Theorem states that every reachable linear system over a field $\mathbb{K}$ is feedback equivalent to a Brunovsky Canonical Form ([8] and [44]). It has also been proven in [11] that the class of rings where every reachable system is Brunovsky is exactly the class of fields. Feedback invariants of linear systems are extended to the general case of commutative rings and it is shown that these invariants are complete for locally Brunovsky systems; i.e., for linear systems having locally a Brunovsky Canonical Form, see [40] .

Moreover, by [8] and [44], the number of feedback equivalence classes of reachable control systems over an n-dimensional $\mathbb{K}$-vector space equals the number $p_{\mathbb{N}}(n)$ of Euler's partitions of integer n. This result is generalized in [10] to the general framework of regular (locally Brunovsky) linear systems over a commutative ring. In fact the number of feedback equivalence classes of regular systems with (finitely generated projective) state space X equals the number of solutions of the linear equation

$$X \simeq Z_1 \oplus Z_2^2 \oplus \cdots \oplus Z_n^n \tag{1}$$

in the monoid $(\mathbf{P}(R), \oplus)$ of finitely generated projective R-modules. This result translates the matter to combinatoric topics.

The goal of this part is to answer the following question: How many different multi-input linear control systems are there with a fixed state space X over different classes of commutative rings?

First, we compute the above number when R is a finite product of rings $R \simeq R_1 \times \ldots \times R_t$ in terms of each direct factor R_i and, in particular, over a finite product of

projectively trivial rings. Furthermore, we study von Neumann regular rings and we show that, over a commutative von Neumann regular ring, every reachable system is locally of Brunovsky type and that this property characterizes the class of commutative von Neumann regular rings. In the Noetherian case, a von Neumann regular ring R decomposes in a finite direct product of projectively trivial rings and computations about the number of locally Brunovsky linear systems over R may be performed. This case is a generalization of $R = \mathbb{Z}/l\mathbb{Z}$, the ring of modular integers. Finally, we perform the above computation in the case where R is a Dedekind domain. In these rings a combinatorial approach is given and combinatorial numbers $\nu(n, k)$ are introduced.

This part is organized as follows: In Chapter 1 we give elementary theory of linear systems over commutative rings studying properties as observability or reachability and feedback equivalence between linear systems over a commutative ring R. In Chapter 2 we compute the number of classes of feedback isomorphisms of locally Brunovsky linear systems over finite product of rings, finite product of projectively trivial rings, von Neumann regular noetherian rings and Dedekind domains.

Chapter 1

Linear systems over commutative rings. A survey.

This Chapter deals with an overview of feedback classification of linear systems over commutative rings with identity. In all chapter R is a commutative ring with $1 \neq 0$.

1.1. Basic Definitions.

A n-dimensional linear dynamical system over $\mathbb{R}$ with m inputs is a system of differential equations with the form

$$\begin{cases} \overrightarrow{x}'(t) = A\overrightarrow{x}(t) + B\overrightarrow{u}(t) \\ \overrightarrow{y}(t) = C\overrightarrow{x}(t) + D\overrightarrow{u}(t) \end{cases} \tag{1.1}$$

where $\overrightarrow{x}(t)$ is the n-state vector, $\overrightarrow{y}(t)$ is the p-vector output, $\overrightarrow{u}(t)$ is the m-vector control, and A, B, C, D are the matrices that characterize the system. We also give an initial state $\overrightarrow{x}(t_0) = \overrightarrow{x}_0$ in time t_0. A system of above type is designed by the set (A, B, C, D). Because the dynamical behaviour of the linear system is determined by the matrices A and B we understand a dynamical system as a pair (A, B), see [5], [6], [7] and [38] for details.

The generalization of the definition of dynamical linear systems over commutative rings was given in [38] and it is as follows:

Definition 1.1.1 (cf. Definition 4, [38]). *Let X be a projective R-module. A system over a ring R is a triple $\Sigma = (X, f, B)$ where $f : X \to X$ is an endomorphism of a projective module X (whose associated matrix is A if $X \simeq R^n$) and B is a (finitely generated)*

submodule of X. The state-space of the system is X, and n is the rank of X. Usually B is specified in terms of generators giving a linear map $B : R^m \to X$ whose image is B. Moreover, is considered the natural inclusion map $i : B \to X$.

From above definition we can understand a system over R as a triple $\Sigma = (X, f, B)$ where X is the state-space R-module, f is an endomorphism of modules and B is the submodule of controls. We shall feel free use both point of view (matrices or modules) when it is convenient. To clarify the notation we say dynamical linear system when we deal with $\Sigma = (A, B)$ and we refer to $\Sigma = (X, f, B)$ as a linear system.

Parameters Linear Systems

Let $[a, b]$ be a compact interval of the real line. A pair of matrices $A = (a_{ij}(x))$, $B = (b_{ik}(x))$ where $1 \leq i, j \leq n$, $1 \leq k \leq m$ gives a family of linear systems over the ring $\mathcal{C}([a, b])$ of continuous functions $[a, b] \to \mathbb{R}$ by $\Sigma = ((\mathcal{C}([a, b]))^n, A, Im(B))$. Pointwise properties of Σ are given by those properties holding on every $\Sigma(x)$. For example, let $[a, b]$ be the interval $[0, 2\pi]$ and

$$\Sigma = \left[A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, B = \begin{pmatrix} cos(x) - 1 & -sin(x) \\ sin(x) & cos(x) + 1 \end{pmatrix} \right]$$

Then

$$\Sigma(0) = \left[\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right].$$

whereas

$$\Sigma(\pi/2) = \left[\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \right].$$

In general, if R is a commutative ring, $Spec(R)$ is its spectrum given by all prime ideals of R together with Zariski topology. $Spec(R)$ is quasi-compact and any linear system over R can be viewed as a family of linear systems over $Spec(R)$.

Example 1.1.2. *Let $R = \mathbb{Z}$ be the ring of rational integers and*

$$(A, B) = \left[\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 3 & 4 \end{pmatrix} \right].$$

If $\mathfrak{p} = 2\mathbb{Z}$ then

$$\Sigma(\mathfrak{p}) = \Sigma(mod\ 2) = \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right].$$

whereas if $\mathfrak{p}' = 3\mathbb{Z}$*, then*

$$\Sigma(\mathfrak{p}') = \Sigma(mod\ 3) = \left[\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right].$$

and so on.

1.2. Reachability, Controllability and Observability.

State controllability refers to the ability to manipulate the state applying specific inputs. 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. Since it is difficult to measure the state of a system directly it is important to describe such states observing the inputs and outputs of the system over some finite time interval (further study of this topic has been developed in [1]) .

We begin with the study of above properties of systems over the field of real numbers $\mathbb{R}$ and finally we recall the generalization over a commutative ring R with identity.

Let $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times m}$ be matrices such that we can consider the following time-invariant systems:

1. If it is continuous-time system, state equations are $x' = Ax + Bu$

2. If it is a discrete-time system, state equations are $x_{k+1} = Ax_k + Bu_k$ where $k \geq k_0 = 0$.

Definition 1.2.1 (cf. Section 5, [1])**.** *In the case of time-invariant systems, a state* x_1 *is called* reachable *(or controllable from the origin) if there exists an input that transfers the state of the system,* $x(t)$*, from the zero state to* x_1 *in some finite time* T *.*

The reachability of a system (in the cases discrete and continuous-time) refers to the ability of the system to reach x_1 *from the origin in some finite time.*

We recall the characterization of reachable systems in terms of the matrices of the dynamical system $\Sigma = (A, B)$.

Definition 1.2.2 (cf. Section 5, [1]). *In the time-invariant case, a system is reachable (or controllable from the origin) if and only if its controllability matrix* $\Phi_n = [B, AB, ..., A^{n-1}B] \in \mathbb{R}^{n \times mn}$ *has full row rank n; that is, rank* $\Phi_n = n$. *In this case we say that* $\Sigma = (A, B)$ *is reachable.*

Note that the matrix Φ_n should be called the *reachability matrix* or the *controllability-from-the-origin matrix*. Matrix Φ_n is sometimes denoted by A^*B.

Theorem 1.2.3 (cf. Theorem 5.23.,[1]). *Let* $\Sigma = (A, B)$ *be the dynamical part of a time-invariant linear system over* $\mathbb{R}$. *Then the following statements are equivalent:*

i) The system is reachable (controllable from the origin).

ii) Controllability matrix $\Phi_n = [B, A, B, ..., A^{n-1}B]$ *has full rank n.*

iii) The n rows of the matrix $(zI - A)^{-1}B$ *are linearly independent over the field of complex numbers.*

iv) Rank $(z_0 I - A, B) = n$ *for all complex number* z_0.

Above condition *iv*), $rank(z_0 I - A, B) = n$ for all z_0 in $\mathbb{C}$ (the algebraic clausure of $\mathbb{R}$), is equivalent to saying that the map

$$(zI - A \mid B) : \mathbb{R}[z]^{n+m} \longrightarrow \mathbb{R}[z]^n$$

is surjective, see Theorem B.2.7 of Appendix B. On the other hand, above Theorem holds both in discrete and continous case.

Definition 1.2.4 (cf. Section 5, [1]). *A state* x_0 *is called* controllable *(or controllable to the origin) if there exists an input that transfers the state from* x_0 *to the zero state in some finite time T.*

A system $\Sigma = (A, B)$ *is controllable, or controllable to the origin, when any state* x_0 *can be driven to the zero state in a finite number of steps. This definition is completely analogous for continous or discrete time-invariant systems.*

We also can study the controllability to the origin of a linear system by matrices:

Lemma 1.2.5 (cf. Section 5, [1]). *A system* $\Sigma = (A, B)$ *in* $\mathbb{R}$ *is controllable when* $A^n x_0 \in Im(\Phi_n)$ *for any* x_0. *If rank* $A = n$, *a system is controllable when rank* $\Phi_n = n$,

i.e., when the reachability condition is satisfied. In this case, the $n \times mn$ *matrix* $A^{-n}\Phi_n = [A^{-n}B, ..., A^{-1}B]$ *is of interest and the system is controllable if and only if rank* $(A^{-n}\Phi_n) = rank\ \Phi_n = n$.

Note that reachability always implies controllability because if the system is state reachable then there exists an input that transfers any state x_0 to any other state x_1 in finite time. Controllability implies reachability only when the state transition matrix Φ_n of the system is nonsingular. This is always true for continuous-time systems, but is true for discrete-time systems only when the matrix A of the system is non singular because if $rank\ A < n$ then controllability does not imply reachability (see Section 5.3. [1] for details).

Now we recall the characterization of reachability and observability of linear systems over commutative rings. Let $\Sigma = (A, B, C, D)$ be a n-dimensional linear system over the commutative ring with identity R. Further study of this topic has been developed in [7].

Definition 1.2.6 (cf. pp.54, [7]). *The reachability map is defined as:*

$$\rho : \oplus_{i=0}^{\infty} R^m \to R^n$$

such that for each nonnegative integer $i \geq 0$ *then* A^iB *is a* R*-linear map from* R^m *to* R^n. *The system is reachable if and only if* ρ *es surjective.*

Systems reachability is characterized by its matrix representation by the following theorem.

Theorem 1.2.7 (cf. Theorem 2.3., [7]). *Let* $\Sigma = (A, B, C, D)$ *be a* n*-dimensional linear system over a commutative ring* R. *The following statements are equivalent:*

1. *The system* Σ *is reachable.*
2. *The columns of* $[B, AB, \ldots]$*generate* R^n.
3. *The columns of* $\Phi_n = [B, AB, \ldots, A^{n-1}B]$ *generate* R^n.
4. *If* ϕ *denotes the map* $R^{mn} \to R^n$ *given by the multiplication of* Φ_n *then* ϕ *is residually surjective in each maximal of* R.
5. *The ideal* $\mathcal{I}_n(\Phi_n)$ *generated by the* $n \times n$ *minors of* Φ_n *is equal to* R.

Note that the characterization of reachability (controllability from the origin) only depends on the state matrix A and the input matrix B, see [7].

Reachability map of linear systems $\Sigma = (A, B)$ maps a finite sequence of inputs $(u_k, u_{k-1}, \ldots, u_1)$ to the state $(A^{k-1}Bu_1 + \ldots + ABu_{k-1} + Bu_k)$ reached from the origin after appying the sequence of inputs (u_i).

Finite sequences (of any lenght) of elements of R^m are given by the module $\prod_{i=0}^{\infty} R^m$. Therefore:

Definition 1.2.8 (cf. Section 2.2.[7]). *Let $\Sigma = (A, B, C, D)$ be a system over R. Consider the R-homomorphism*

$$\tau : R^n \to \prod_{i=0}^{\infty} R^p$$

$$x \mapsto \tau(x) = (Cx, CAx, CA^2x, ...)^t.$$

The system Σ is observable if and only if the map τ is inyective.

Theorem 1.2.9 (cf. Theorem 2.6, [7]). *Let $\Sigma = (A, B, C, D)$ be a linear system over R. The following are equivalent:*

1. *Σ is observable.*

2. *The following R-homomorphism is injective*

$$\tau_n : R^n \to \prod_{i=0}^{n} R^p$$

$$x \mapsto \tau(x) = (Cx, CAx, CA^2x, ..., CA^{n-1}x)^t$$

3. *Let $\Omega_n = [C, CA, ..., CA^{n-1}]^t$ be the observability matrix. If $\mathcal{I}_n(\Omega_n)$ is the ideal of R generated by the $n \times n$ minors of Ω_n, then the annhilator of $\mathcal{I}_n(\Omega_n)$ is zero.*

4. *The rank $\Omega_n(A, C)$ equals n.*

On the other hand, in coding literature, reachability is usually called controllability because it is referred to controllability from the origin. Moreover, difference between controllability from the origin (reachability) and output controllabillity has been researched and associated output controllability matrix of a dynamical linear system over a finite field is computed and its application to the decoding process of a convolutional code is given in [27], [28] and [29], among others.

1.3. Feedback equivalence of linear systems.

Two linear systems are feedback equivalent if one can transform one into the another by means of feedack actions. These feedback actions are changes of coordinates together with feedback loops. This kind of procedures are basic tools in Control Engineering and, in particular, are at the very heart of disciplines such as Control Automation and Servosystems. Note also that first feedback loop is the celebrated Maxwell's flyball Governor for steam engines [J.C. Maxwell, *On governors*, Proc. Royal Soc, 1868].

The goal is to describe feedback equivalence in the set of linear systems; to find out invariants, and to give canonical representations of each feedback class when it is possible. We review the main results about the topic.

Definition 1.3.1. *Let $\Sigma = (A, B)$ and $\Sigma' = (A', B')$ be n-dimensional linear systems over $\mathbb{R}$. These systems are feedback equivalent if there exists an element of the feedback group (P, Q, F) (a feedback control F and basis changes P and Q in the $\mathbb{R}$-modules of states and impulses) transforming each other, namely,*

$$(A, B) \overset{f.e}{\simeq} (A', B') \Leftrightarrow \exists (P, Q, F) \text{ such that } (P \cdot (A + B \cdot F) \cdot P^{-1}, P \cdot B \cdot Q) = (A', B')$$

where $P \in \mathcal{M}_{n\times n}(\mathbb{R})$ is invertible, $Q \in \mathcal{M}_{m\times m}(\mathbb{R})$ and $F \in \mathcal{M}_{m\times n}(\mathbb{R})$ and denoting by $f.e$ the feedback equivalence. The set of triples (P, Q, F) is called feedback group. The reader can see the feedback action In Figure 1.1.

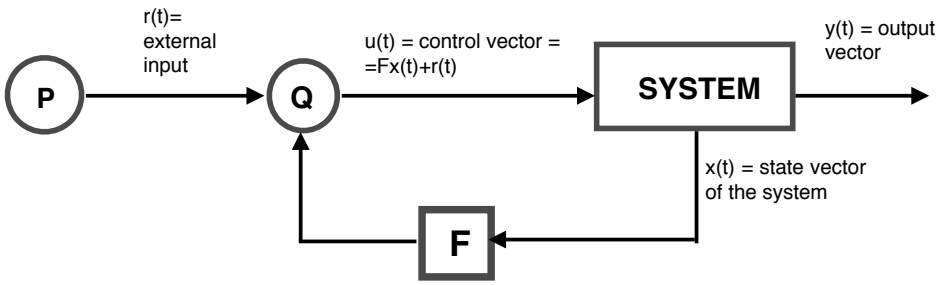


Figure 1.1: *State Diagram of Feedback Equivalence*

Example 1.3.2. *As a basic example of classification by the action of a group we have the similarity the classification of square matrices over $\mathbb{K}$. Let A and A' be matrices over $\mathbb{K}$. Then*

$A \simeq A'$, if and only if, $\exists P$ invertible where $A = P \cdot A' \cdot P^{-1}$.

Note that this case is analogous to study feedback equivalence between the systems (A, O) and (A', O) if we consider $Q = I_m$ and $F = (0)_{m\times n}$. Then, the group of invertible matrices $Gl_n(\overline{\mathbb{K}})$ of dimension n over the algebraic clausure of $\mathbb{K}$ performs over the group of square matrices $\mathcal{M}_{n,n}(\mathbb{K})$ by the action $P * D = P \cdot D \cdot P^{-1}$.

The problem of feedback classification of dynamical linear systems concludes with the construction of canonical forms by invariants, in Example 1.3.2 the problem of classification over $\mathbb{C}$ concludes with the definition of the Jordan Canonical form.

If $\Sigma = (A, B)$ is a dynamical linear system over a finite dimensional $\mathbb{K}$-vector space, by Brunovsky's Theorem ([8]) and the Kalman's Decomposition ([44]) the system Σ splits in a reachable system Σ_r and a zero control system Σ_0. We can compute the Brunovsky Canonical Form of Σ_r and the Jordan Canonical Form of Σ_0. This result implies that feedback classification of linear systems over $\mathbb{K}^n$ becomes in the classification of Reachable Systems.

1.3.1. Feedback isomorphisms of linear systems.

The study of canonical forms of linear systems over a commutative ring is a very wild problem, see [5] and [6] . In order to construct canonical forms and complete families of invariants for linear systems over commutative rings, feedback equivalence was generalized in [10].

Definition 1.3.3 (cf. Definition 4, [38]). *A linear system over R is a triple $\Sigma = (X, f, B)$ where X is a R-module, $f : X \to X$ is a linear map and $B \subseteq X$ is the R-submodule of controls.*

We recall the definition of feedback isomorphia of linear systems over a commutative ring R.

Definition 1.3.4 (cf. Definition 2.2, [10]). *Let Σ and Σ' be the linear systems $\Sigma = (X, f, B)$ and $\Sigma' = (X', f', B')$ over R. These systems are feedback isomorphic $\Sigma \overset{f.i}{\simeq} \Sigma'$ if and only if there exists an isomorphism $\phi : X \to X'$ such that:*

1. *$\phi(B) = B'$.*
2. *$Im(\phi f - f'\phi) \subset B'$.*

In this case we say that Σ is feedback equivalence to Σ' via ϕ.

Remark 1.3.5. *The above relation of feedback isomorphisms verifies that if a pair of dynamical linear systems $\Sigma = (A, B)$ and $\Sigma' = (A', B')$ are feeback equivalent then the associated linear systems $\Sigma = (X, f, B)$ and $\Sigma' = (X', f', B')$ are feedback isomorphic.*

Note that the above remark is equivalent to the fact that if the associated linear systems are not feedback isomorphic then the pair of matrices are not feedback equivalent. So, if we determine invariants of $\Sigma = (X, f, B)$ then we will find invariants of $\Sigma = (A, B)$, but this is not a complete family of invariants. For specific class of linear systems (locally Brunovsky linear systems) this complete family of invariants is available.

Feedback invariants of locally Brunovsky linear systems.

The invariants that describe a canonical form respect to feedback isomorphia for linear systems over commutative rings with identity are obtained from the canonical form for pairs of matrices via feedback equivalence. Feedback invariants for a linear system Σ are obtained as follows:

Definition 1.3.6 (cf. Definition 3.1, [10])**.** *Let $\Sigma = (X, f, B)$ be a linear system over R.*

1. *Invariants N_i^Σ are defined as $N_0^\Sigma = 0$ and $N_i^\Sigma = B + f(N_{i-1}^\Sigma)$ for $i \geq 1$*
2. *Invariants M_i^Σ are described as $M_i^\Sigma = X/N_i^\Sigma$*
3. *Invariants I_i^Σ are R-modules which are defined as $I_i^\Sigma = N_i^\Sigma/N_{i-1}^\Sigma$*
4. *We have the exact sequence: $0 \to I_i^\Sigma \hookrightarrow M_{i-1}^\Sigma \to M_i^\Sigma \to 0$ where $f(x + N_{i-1}^\Sigma) = f(x) + N_i^\Sigma$.*
5. *Let us denote as $Z_i^\Sigma = Ker(I_i^\Sigma \to I_{i+1}^\Sigma)$.*

Remark 1.3.7. *Invariants Z_i associated to Σ is given in [10] by the modules*

$$Z_i^\Sigma = Ker\left(\frac{B + fB + \ldots + f^{i-1}B}{B + fB + \ldots + f^{i-2}B} \xrightarrow{\overline{f}} \frac{B + fB + \ldots + f^{i}B}{B + fB + \ldots + f^{i-1}B}\right)$$

These invariants generalize the set of invariants M_i^Σ, given in [41], that are related to invariants Z_i^Σ by

$$Z_i^\Sigma = Ker\left(Ker(M_{i-1} \xrightarrow{I} M_i) \xrightarrow{\overline{f}} Ker(M_i \xrightarrow{I} M_{i+1})\right).$$

In order to prove that two linear systems are feedback isomorphic if and only if their invariant submodules are isomorphic we recall the following results

Theorem 1.3.8 (cf. Theorem 3.4, [10]). *Let $\Sigma = (X, f, B)$ and $\Sigma' = (X', f', B')$ be linear systems over R that are feedback isomorphic by $\phi : X \to X'$. Then the following statements are verified.*

1. *N_i^Σ is isomorphic to $N_i^{\Sigma'}$ via restriction of ϕ.*
2. *M_i^Σ is isomorphic to $M_i^{\Sigma'}$ via quotient of ϕ.*
3. *I_i^Σ is isomorphic to $I_i^{\Sigma'}$ via restriction of the quotient of ϕ.*
4. *The isomorphism ϕ commutes with the linear maps f and f'.*
5. *Z_i^Σ is isomorphic to $Z_i^{\Sigma'}$ via restriction of $\phi : I_i^\Sigma \to I_i^\Sigma$.*

Remark 1.3.9. *If two invariant submodules are equal, $N_i^\Sigma = N_{i+1}^\Sigma$, then*

$$N_{i+2}^\Sigma = B + f(N_{i+1}^\Sigma) = B + f(N_i^\Sigma) = N_{i+1}^\Sigma = N_i^\Sigma,$$

namely, there exists a natural number s from which the chain of invariants stabilizes

$$N_0^\Sigma \subsetneq N_1^\Sigma \subsetneq N_2^\Sigma \subsetneq ... \subsetneq N_s^\Sigma = N_{s+1}^\Sigma = ...$$

In the same way

$$M_s^\Sigma = M_{s+1}^\Sigma = ...$$
$$I_{s+1}^\Sigma = I_{s+2}^\Sigma = ... = 0$$
$$Z_s^\Sigma = Z_{s+1}^\Sigma = ... = 0.$$

We denote the above natural number s, in the case that it exists, as $s = s(\Sigma)$ and if it does not exist we denote it $s(\Sigma) = \infty$. The modules N_i^Σ represent, in the sequencial case, the subset of state spaces that is reachable by the system Σ at time i.

The main point of the classification by above invariants is that two linear systems are feedback isomorphic if and only if the family of invariants Z_i^Σ are isomorphic (see [10]). The direct way is proved in Theorem 1.3.8 but sequence (Z_i^Σ) characterizes the feedback class of the system Σ for a specific family of systems known as *locally Brunovsky*.

Definition 1.3.10 (cf. 3.1, [38]). *A linear system $\Sigma = (X, f, B)$ is reachable if and only if $N_{s(\Sigma)}^\Sigma = X$.*

Definition 1.3.11 (cf. Definition 2, [9]). *A linear system $\Sigma = (X, f, B)$ over R is locally Brunovsky if and only if the system Σ is reachable and its localizations $\Sigma_{\mathfrak{p}} = (X_{\mathfrak{p}}, f_{\mathfrak{p}}, B_{\mathfrak{p}})$ are of Brunovsky type for all prime ideal $\mathfrak{p}$ of R. Note that in this case modules $M_i^{\Sigma_{\mathfrak{p}}}$ and $Z_i^{\Sigma_{\mathfrak{p}}}$ are free for all i.*

As a matter of example of a ring that is not localy Brunovsky let us consider the following reachable system over $\mathbb{Z}$

$$\Sigma = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right]$$

System $\Sigma_{\mathfrak{p}}$ is of Brunovsky type if $\mathfrak{p} \neq 2\mathbb{Z}$ and $\Sigma_{2\mathbb{Z}}$ is not Brunovsky.

Note that there are locally Brunovsky systems that are not Brunovsky ones, see [12]. Since the Brunovsky Canonical Form of a system Σ is constructed from an adequate choice of bases of its invariants, these invariants need to be based free modules. Hence locally Brunovsky systems suggest locally free modules and in fact, local Brunovsky character is equivalent to saying that invariants are projective (see [9]).

Definition 1.3.12 (c.f. [14].). *A system is regular if all invariants of Definition 1.3.6 happen to be projective. If all invariants are free and the system is reachable then the system is called of Brunovsky.*

We recall the following characterization of locally Brunovsky type in terms of projective modules.

Theorem 1.3.13 (cf. Theorem 6.1, [10]). *Let $\Sigma = (X, f, B)$ be a reachable linear system over R. Then the following statements are equivalent*

1. *All M_i^{Σ} are projective.*
2. *All I_i^{Σ} are projective.*
3. *All Z_i^{Σ} are projective.*

If the invariants submodules of a system Σ satisfy the above result, then the linear system is called a locally Brunovsky linear system or regular system.

A complete set of feedback invariants is available for the class of locally Brunovsky linear systems. Invariants of locally Brunovsky linear systems verify the following properties:

Theorem 1.3.14 (cf.Theorem 6.3, [10]). *Let $\Sigma = (X, f, B)$ be a locally Brunovsky linear system over R. Then for all $i = 1, ...s(\Sigma)$ we have:*

1. *The invariant module M_i^Σ is direct summand of M_{i-1}^Σ.*
2. *The invariant module M_{i-1}^Σ decomposes as $M_{i-1}^\Sigma \cong I_i^\Sigma \oplus M_i^\Sigma$.*
3. *The state space decomposes as direct sum decomposition of the invariants: $X \cong I_1^\Sigma \oplus I_2^\Sigma \oplus .... \oplus I_{s(\Sigma)}^\Sigma$*
4. *The invariant modules I_{i+1}^Σ are direct summand of I_i^Σ for each i.*
5. *The invariant modules I_i^Σ decompose as $I_i^\Sigma \cong Z_i^\Sigma \oplus I_{i+1}^\Sigma$*
6. *The invariant modules M_i^Σ decompose as $M_i^\Sigma \cong Z_{i+1}^\Sigma \oplus ... \oplus Z_{s(\Sigma)}^\Sigma$.*
7. *The state space $X \cong Z_1^\Sigma \oplus (Z_2^\Sigma)^2 \oplus ... \oplus (Z_{s(\Sigma)}^\Sigma)^{s(\Sigma)}$ decomposes in a direct summand of invariants. Z_i^Σ.*

The above invariant submodules are projective finitely generated modules so the relation between the set of feedback isomorphisms classes of locally Brunovsky linear systems and the set of isomorphism classes of finitely generated projective modules is clear.

We consider $\mathbf{P}(R)$ the set of isomorphism classes $[P]$ of finitely generated projectives R-modules. Let us review some elementary properties of $\mathbf{P}(R)$ which will be applied in the sequel. Further study of this topic has been developed in [82].

Proposition 1.3.15. *Let $\mathbf{P}(R)$ be the set of isomorphism classes of finitely generated projective R-modules. Then the following properties hold:*

(i) *$\mathbf{P}(R)$ is a monoid partially ordered under operation $[P] \oplus [Q] = [P \oplus Q]$. Identity element is the zero R-module.*

We denote by P the finitely generated projective R-module and its isomorphism class.

(ii) *$\mathbf{P}(R)$ is a commutative monoid (i.e. $P \oplus Q = Q \oplus P$)*

(iii) *$\mathbf{P}(R)$ is a zero-sum-free monoid (i.e. $P \oplus Q = 0 \Rightarrow P = Q = 0$)*

(iv) *The mapping $\varphi : (\mathbb{N}, +) \to (\mathbf{P}(R), \oplus)$ sending $0 \mapsto 0$ and $n \mapsto R^n$ is an injective morphism of monoids.*

(v) If every finitely generated projective R-module is free (i.e. R is projectively trivial) then above morphism φ is an isomorphism.

If R is a domain with field of fractions $\mathbb{K}_R$ then every finitely generated projective R-module P has constant rank $\mathrm{rk}(P) = \dim(P \otimes_R \mathbb{K}_R)$.

(vi) Mapping $\mathrm{rk} : (\mathbf{P}(R), \oplus) \to (\mathbb{N}, +)$ *is a monoid morphism*

(vii) rk *is left inverse of φ; that is,* $\mathrm{rk} \circ \varphi = I_{\mathbb{N}}$

Now, we follow with the classification of linear systems. Denoting by $\mathbf{P}(R)^\infty$ the set of almost-zero sequences with entries in $\mathbf{P}(R)$.

Definition 1.3.16 (cf. Notation 6.5, [10])**.** *The map σ is defined by*

$$\begin{aligned} \sigma : \mathbf{P}(R)^\infty &\to DS(\mathbf{P}(R)) \\ (P_1, P_2, ...) &\mapsto (\oplus_{i\geq 1} P_i, \oplus_{i \geq 2} P_i, ...) \end{aligned}$$

In the rings such that the monoid $\mathbf{P}(R)$ is cancellative; that is, $a \oplus b = a \oplus c \Rightarrow b = c$ for each $a, b, c \in \mathbf{P}(R)$, the map σ is bijective.

Definition 1.3.17 (cf. Section 6.2, [10])**.** *The map γ is defined by*

$$\begin{aligned} \gamma : (B_r/\cong) &\to DS(\mathbf{P}(R)) \\ [\Sigma] &\mapsto (I_1^\Sigma, I_2^\Sigma, ...I_{s(\Sigma)}^\Sigma, 0, 0, ...) \end{aligned}$$

Definition 1.3.18 (cf. Section 6.2, [10])**.** *The map* Z *is described by*

$$\begin{aligned} \mathrm{Z} : (B_r/\cong) &\to \mathbf{P}(R)^\infty \\ [\Sigma] &\mapsto (Z_1^\Sigma, Z_2^\Sigma, ..., Z_{s(\Sigma)}^\Sigma, 0, 0, ...) \end{aligned}$$

Theorem 1.3.19 (c.f. Theorem 6.6., [10])**.** *Let X be a finitely generated projective R-module and let $X \cong X_1 \oplus X_2 \oplus ... \oplus X_q$ be a decomposition of X in direct sum such that X_{i+1} is direct sum of X_i for all $i = 1, ..., q-1$. Then there exists a linear system $\Sigma = (X, f, B)$ such that $I_i^\Sigma = X_i$ for all $i = 1, ...q$.*

Theorem 1.3.20 (c.f. Theorem 6.8, [10])**.** *Let $\Sigma = (X, f, B)$ and $\Sigma' = (X', f', B')$ be locally Brunovsky linear systems over R. If $Z_i^\Sigma \cong Z_i^{\Sigma'}$ are isomorphic for each $i = 1, ..., s$, then Σ and Σ' feedback isomorphic.*

Corollary 1.3.21 (c.f. Corollary 6.9,[10]). *The map Z is bijective. Then the invariants Z_i^{Σ} characterize the feedback classes of locally Brunovsky linear systems.*

Corollary 1.3.22 (c.f. Lemma 7.2, [10]). *If R is such that $\mathbf{P}(R)$ is cancellative, then the following diagram is commutative*

$$\begin{array}{ccc} (B_r/\cong) & \xrightarrow{\quad\gamma\quad} & DS(\mathbf{P}(R)) \\ & {\scriptstyle Z}\searrow \quad \nearrow{\scriptstyle \sigma} & \\ & \mathbf{P}(R))^{\infty} & \end{array}$$

and since all the above defined maps are bijective hence the invariant modules I_i^{Σ} classify the class of feedback isomorphisms of Σ.

1.4. Enumeration of linear systems via partitions.

It is well known that feedback classification of linear systems over $\mathbb{K}^n$ becomes in the classification of reachable systems. The number of feedback classes of reachable systems over $\mathbb{K}^n$ may be performed by using Kronecker invariants indices of the associated pencil $(zI - A, B)$ to n-dimensional dynamical linear system $\Sigma = (A, B)$ over $\mathbb{K}^n$. These indices could be algorythmic computed, see [79]. Moreover, the set of Kronecker indices $(\kappa_1 \geq \kappa_2 \geq \cdots \geq \kappa_p)$ is an ordered partition of the integer n (the dimension of state space); that is, $n = \kappa_1 + \ldots + \kappa_p$.

Remark 1.4.1. *The combinatorial approach of feedback equivalence of linear systems $\mathbb{K}^n$ is based on a bijective correspondence between a (reachable) linear system into the conjugate partition or onto the partition. Kronecker's conjugate partition is given by $(\xi_1, \xi_2, \ldots, \xi_p)$ where $\xi_1 = rk(B)$ and $\xi_i = rk(B, AB, ..., A^{i-1}B) - rk(B, AB, ..., A^{i-2}B)$ and classify too.*

The generalization of above computation over a commutative ring R with identity is given in [10]. Let Σ be a locally Brunovsky linear system over R being X, a projective finitely generated R-module of constant rank n, the state space.

Notation. *We denote by*

1. *m as the class of isomorphisms of X in $\mathbf{P}(R)$, $[X]$.*
2. *$fe_R(m)$ as the number of feedback isomorphisms classes of locally Brunovsky linear systems Σ with state-space X over R.*

Theorem 1.4.2 (cf. Corollary 8.1, [10]). *The set of feedback isomorphisms classes of locally Brunovsky Linear System with state-space X is in bijective correspondence with the set of solutions of the following linear equation in the monoid $(\mathbf{P}(R), \oplus)$ of isomorphism classes of finitely generated projective R-modules.*

$$X \simeq Z_1 \oplus (Z_2)^2 \oplus \ldots \oplus (Z_s)^s \oplus \cdots , \tag{1.2}$$

namely,

$$fe_R(m) = \#\ \{\textit{Solutions of the equation (1.2) in the abelian monoid } (\mathbf{P}(R), \oplus)\}\ .$$

Remark 1.4.3. *If the monoid is cancellative the invariant modules I_i^Σ classify.*

Since $I_i^\Sigma \cong Z_i^\Sigma \oplus I_{i+1}^\Sigma$ then $I_1 \oplus I_2 \oplus .... \oplus I_s = Z_1 \oplus (Z_2)^2 \oplus ... \oplus (Z_s)^s$ and hence

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

Chapter 2

On linear systems over regular rings and Dedekind domains.

This chapter is devoted to compute $fe_R(m)$, the number of feedback equivalence classes of locally Brunovsky linear systems with state space X, a projective finitely generated, over certain commutative rings. It equals the number of solutions of the following linear equation

$$X \simeq Z_1 \oplus Z_2^2 \oplus \cdots \oplus Z_s^s \tag{2.1}$$

in the monoid $(\mathbf{P}(R), \oplus)$ of isomorphism classes of finitely generated projective R-modules. In the case that $\mathbf{P}(R) \simeq \mathbb{N}$, since the monoid is cancellative, the equation (2.1) becomes $n = x_1 + \ldots + x_n$ and the above number equals $p_{\mathbb{N}}(n)$, the partitions of n.

Our goal in this section is, applying the results of [10], to perform the computation of feedback equivalence classes of locally Brunovsky linear system over projectively trivial rings, finite product of rings and Dedekind domains. Moreover, we give a characterization of von Neumann regular rings by properties of regular linear systems. Recall that R always denotes a commutative ring with identity.

2.1. Projectively trivial rings

Along the section Σ is considered as locally Brunovsky linear system over a commutative ring R.

Definition 2.1.1. *R is projectively trivial ring if all finitely generated projective R-modules are free.*

Note that if R is connected the above definition equals to the definition of projectively trivial ring given in Theorem IV. 49 of [56]. Examples of projectively trivial rings are: fields $\mathbb{K}$; local rings like $\mathbb{K}[[x_1, ..., x_s]]$ or $\mathbb{Z}/p^r\mathbb{Z}$ where p is prime; principal ideal domains like $\mathbb{Z}$ or $\mathbb{K}[x]$; polynomial rings like $\mathbb{K}[x_1, ..., x_s]$ or $\mathbb{Z}[x_1, ..., x_s]$; and the ring of continuous real-valued functions $\mathcal{C}(K)$ over compact contractible topological space K, i.e. if K retracts to a point.

Remark 2.1.2. *Let R be a projectively trivial ring. By Definition 2.1.1, the set $\mathbf{P}(R)$ of classes of isomorphisms of finitely generated projective R-modules is isomorphic to the semigroup of natural numbers, namely, $\mathbf{P}(R) \simeq \mathbb{N}$.*

Lemma 2.1.3. *If R is a projectively trivial ring then the number of feedback classes of locally Brunovsky linear systems with state space X (a projective finitely generated of R-module) of rank n equals*

$$fe_R(m) = \text{the number of solutions of the equation (2.1) in the abelian monoid } (\mathbf{P}(R), \oplus) = \text{Euler's partitions of the integer } n.$$

Proof. Because R is a projectively trivial ring, if $rank\ X = n$ hence $X \simeq R^n$. So, $m = n$ and the rank-map

$$\text{rank} : (\mathbf{P}(R), \oplus) \longrightarrow (\mathbb{N}, +) \tag{2.2}$$

is an isomorphism of monoids. Hence the solutions of equation (2.1) are exactly the solutions of $n = x_1 + \ldots + x_n$ that is equal to the partitions of integer $\text{rk}(X) = p_{\mathbb{N}}(n)$. □

A survey over Euler's partitions is provided in Appendix A.

Remark 2.1.4. *Note that over projectively trivial rings we really do not have more regular systems than in the case of fields, see [12].*

2.2. Finite product of rings.

Let R be such that $R \simeq R_1 \times \cdots \times R_t$ where R_i are rings for $i = 1, \ldots, t$. Along the section Σ is considered as locally Brunovsky linear system over a commutative ring R. In

order to compute the number of solutions of the equation (2.1) over R, finite product of rings, first we study some results describing the structure of $\mathbf{P}(R)$.

Remark 2.2.1 (§2. 2.1.2., c.f. [82]). *Let P be a R-module. If $e \in R$ is idempotent ($e^2 = e$), then $P = eR$ is projective because $R = eR \oplus (1-e)R$ and direct summands of free modules are projective. Conversely, if we have any decomposition $R = P \oplus Q$ then there exist unique elements $e \in P$ and $f \in Q$ such that $1 = e + f$ in R. The elements e and $f = 1 - e$ are idempotents and verify $ef = fe = 0$. Moreover, idempotent elements of R are in biunivocal correspondence with the descompositions with the form $R \simeq P \oplus Q$.*

Finally, each finitely generated projective R-module corresponds to an idempotent element in the ring $\mathcal{M}_{n\times n}(R)$. We must realize that if $P \oplus Q = R^n$ then from the composition $R^n \to P \to R^n$ we obtain an idempotent element $e \in \mathcal{M}_{n\times n}(R)$. In the same way, the image $e(R^n)$ of e is P.

Notation (cf. Definition 1.2.2, [64]). *Let R be a ring. Denote by $\mathcal{M}(n, R)$ the ring of $n \times n$ matrices over R and by $GL(n, R)$ the group of $n \times n$ invertible matrices over R. We embed $\mathcal{M}(n, R)$ in $\mathcal{M}(n + 1, R)$ by*

$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

(this is a nonunital ring homomorphism) and $GL(n, R)$ in $GL(n + 1, R)$ by the group homomorphism

$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

We denote by $\mathcal{M}(R)$ and $GL(R)$ the infinite unions of the $\mathcal{M}(n, R)$, resp. $GL(n, R)$. Note that $\mathcal{M}(R)$ is a ring without unit and $GL(R)$ is a group. It is important to remember that each matrix in $\mathcal{M}(R)$ has finite size.

Lemma 2.2.2 (cf. Theorem 1.2.3, [64]). *For any ring R, $\mathbf{P}(R)$ may be identified with the set of conjugation orbits of $GL(R)$ on $Idem(R)$ where $Idem(R) = \{$set of idempotent matrices in $\mathcal{M}(R)\}$. The semigroup operation is induced by $(p, q) \mapsto \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$.*

Theorem 2.2.3. *If $R \simeq R_1 \times \cdots \times R_t$ is a finite product of rings then we have a decomposition over idempotent $Idem(R) \simeq Idem(R_1) \times \ldots \times Idem(R_t)$ and then $\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times ... \times \mathbf{P}(R_t)$.*

Proof. Let $\mathbf{P}(R)$ be the set of classes of isomorphisms of finitely generated projective modules over R. Let M be a finitely generated projective R- module. By Lemma 2.2.2 we have the following biunivocal correspondence

$$\left\{ \begin{array}{c} R-\text{finitely generated} \\ \text{projective modules} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{idempotent elements} \\ \text{of } \mathcal{M}_{n\times n}(R) \end{array} \right\}$$

That is, for every M there exists an unique associated idempotent element $\alpha \in \mathcal{M}_{n\times n}(R)$ to M such that $\alpha = (a_{ij})$ with $a_{ij} \in R$. Since $R \simeq R_1 \times \ldots \times R_t$ and $R = e_1R \oplus \cdots \oplus e_tR$ then $Idem(R) \simeq Idem(R_1) \times \ldots \times Idem(R_t)$ and so, each element $a_{ij} \in \alpha$ corresponds to a t-uple $(a_{ij}^1, ..., a_{ij}^t) \in R_1 \times \cdots \times R_t$. Namely, for each matrix α there exist idempotent matrices $\alpha_1, \cdots, \alpha_t$ in $R_1 \times \cdots \times R_t$. By Lemma 2.2.2, for each R_i is verified that

$$\left\{ \begin{array}{c} \text{idempotent elements} \\ \text{of } \mathcal{M}_{n\times n}(R_i) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} R_i-\text{finitely generated} \\ \text{projectives modules} \end{array} \right\}$$

Let M_i be a projective finitely generated R_i-modules for $i = 1, \ldots, t$. Because the class of M_i is an element of $\mathbf{P}(R_i)$ and all correspondences are isomorphisms then $\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times ... \times \mathbf{P}(R_t)$. □

Corollary 2.2.4. *If R_i is a projectively trivial ring over R for $i = 1, \ldots, t$, then*

$$\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times ... \times \mathbf{P}(R_t) \simeq \mathbb{N}^t.$$

Proof. Since $R_1, \ldots, R_t$ are projectively trivial rings then all finitely generated projective modules over R_i are free and then $\mathbf{P}(R_i) \simeq \mathbb{N}$ for $i = 1, ..., t$. By Theorem 2.2.3 we conclude the proof because $\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times ... \times \mathbf{P}(R_t) \simeq \mathbb{N} \times \overset{t)}{\ldots} \times \mathbb{N} = \mathbb{N}^t$. □

Example of finite products of projectively trivial rings are rings of modular integers and their rings of polinomials $(\mathbb{Z}/l\mathbb{Z})[x_1, \ldots, x_s]$.

Now we give our main results over the feedback classification of locally Brunovsky linear systems over finite product of rings.

Theorem 2.2.5. *Let $R \simeq R_1 \times \ldots \times R_t$ be a finite product of rings. Let $\Sigma = (X, f, B)$ be a linear system over R where X is a projective finitely generated R-module. Then*

$$fe_R(m) = fe_{R_1}(m_1) \cdot \ldots \cdot fe_{R_t}(m_t)$$

where m denotes the class of isomorphisms of X in $\mathbf{P}(R)$ and m_i denotes the class of isomorphisms of $X \otimes_R R_i$ in the $\mathbf{P}(R_i)$ for each $i = 1 \ldots, t$.

Proof. By Theorem 1.4.2

$$fe_R(m) = \# \left\{ \begin{array}{c} \textit{feedback isomorphism classes of locally Brunovsky} \\ \\ \textit{linear systems over } R \textit{ with state space } X \end{array} \right\} =$$

$$= \# \left\{ \textit{ Solutions of } X = Z_1 \oplus Z_2^2 \oplus \ldots \oplus Z_s^s \textit{ in } \mathbf{P}(R) \right\}$$

Since $\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times \ldots \times \mathbf{P}(R_t)$ we look for the number of solutions of the equation $m = z_1 + 2z_2 + 3z_3 + ... + sz_s$ where m and z_i are t-uples, namely, we compute the number of solutions of the following system of equations

$$\left\{ \begin{array}{l} m_1 = a_1 + 2a_2 + 3a_3 + ... + sa_s \\ m_2 = b_1 + 2b_2 + 3b_3 + ... + sb_s \\ \vdots \\ m_t = t_1 + 2t_2 + 3t_3 + ... + st_s \end{array} \right. \tag{2.3}$$

Because the number of solutions of the i-th equation is equal to $fe_{R_i}(m_i)$ for each $i = 1, ...t$, therefore the number of solutions of the system is equal to the number of possible combinations between the solutions of all equations, that is,

$$fe_R(m) = fe_{R_1}(m_1) \cdot \ldots \cdot fe_{R_t}(m_t) \ .$$

□

Corollary 2.2.6. *Let $R \simeq R_1 \times \ldots \times R_t$ be a finite product of projectively trivial rings. Let $\Sigma = (X, f, B)$ be a locally Brunovsky linear system over R with state space X a projective finitely generated R-module of rank n. Then $fe_R(m) = fe_R(n) = (p_{\mathbb{N}}(n))^t$ where $p_{\mathbb{N}}(n)$ is the number of partitions of natural number n.*

Proof. By Corollary 2.2.4, $\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times ... \times \mathbf{P}(R_t) \simeq \mathbb{N} \times \overset{t)}{\ldots} \times \mathbb{N}$. Hence the number of classes of feedback isomorphisms of locally Brunovsky linear systems over R is the number of solutions of the equation (2.1) over $\mathbb{N}^t$; that is, the number of solutions of

$$m = x_1 + 2x_2 + 3x_3 + ... + sx_s \tag{2.4}$$

where m and x_i are t-uples of natural numbers. Since $m \in \mathbf{P}(X)$ hence $m = (m_1, \ldots, m_t)$ and because $rank\ X = n$ then $X \simeq R^n$ and so, $m = (m_1, \ldots, m_t) = (n, \overset{t)}{\ldots}, n)$. Therefore the equation (2.4) becomes in

$$(n, n, \overset{t)}{...}, n) = (a_1, b_1, ..., t_1) + 2(a_2, b_2, ..., t_2) + 3(a_3, b_3, ..., t_3) + ... + s(a_s, b_s, ..., t_s),$$

namely,

$$\begin{cases} n = a_1 + 2a_2 + 3a_3 + ... + sa_s \\ n = b_1 + 2b_2 + 3b_3 + ... + sb_s \\ \vdots \\ n = t_1 + 2t_2 + 3t_3 + ... + st_s \end{cases} \tag{2.5}$$

where $n, a_i, b_i, ..., t_i \in \mathbb{N}$ for $i = 1, ..., t$.

Since $\mathbb{N}$ is cancellative the number of solutions of i-th equation is equal to $p_{\mathbb{N}}(n)$, the partitions of n for each $i = 1, ...t$ and we conclude that $fe_R(m) = p_{\mathbb{N}}(n) \cdot p_{\mathbb{N}}(n) \cdot \overset{t)}{..} \cdot p_{\mathbb{N}}(n) = (p_{\mathbb{N}}(n))^t$. □

Corollary 2.2.7. *Let $R = \mathbb{Z}/l\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_t\mathbb{Z}$ be a ring where l a square free integer, and p_i prime ideals. Let Σ be a linear system with state space X of rank n. Then $fe_{\mathbb{Z}/l\mathbb{Z}}(m) = fe_{\mathbb{Z}/l\mathbb{Z}}(n) = p_{\mathbb{N}}(n)^t$.*

Proof. Since $\mathbb{Z}/p_i\mathbb{Z}$ is projectively trivial ring by Corollary 2.2.6 we conclude the proof. □

Corollary 2.2.8. *If $R = \mathbb{Z}/l\mathbb{Z} \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_t^{rt}\mathbb{Z}$ and let Σ be a linear system with state space X of rank n, then we have $fe_{\mathbb{Z}/l\mathbb{Z}}(m) = fe_{\mathbb{Z}/l\mathbb{Z}}(n) = p_{\mathbb{N}}(n)^t$.*

Proof. Since $\mathbf{P}(\mathbb{Z}/p_i^{r_i}\mathbb{Z}) \simeq \mathbb{N}$ for each i, we conclude the proof. □

Remark 2.2.9. *The feedback classification of regular systems over $\mathbb{Z}/l\mathbb{Z}$ where l is a square-free integers is now complete. In fact, it is the classification of all reachable linear systems.*

2.3. Regular systems over von Neumann regular rings.

The class of von Neumann regular rings has been studied in linear control systems framework, see [16], [72], [73], [74] and [75]. Maybe the first example of commutative von Neumann regular ring is $\mathbb{Z}/l\mathbb{Z}$ where $l = p_1 \ldots p_t$ is square free integer. Another examples of von Neumann regular ring are the Boolean rings, that is, rings $(\mathbb{B}, +, \cdot)$ such that $b^2 = b$ for all $b \in \mathbb{B}$. These rings are very useful by its applications, [20].

In this section we show that over a commutative von Neumann regular ring every reachable system is locally of Brunovsky type and that this property characterizes the

class of commutative von Neumann regular rings. Moreover we compute the number of classes of feedback isomorphism of locally Brunovsky linear systems over von Neumann noetherian rings.

2.3.1. Preliminaries of von Neumann regular rings.

Definition 2.3.1 (Definition I, cf.[36]). *A ring R is a von Neumann regular commutative ring provided that for every $x \in R$ there exists $y \in R$ such that $xyx = x$.*

Note that von Neumann regular rings R are called absolutely flat rings by Bourbaki (§2, Ex. 17, [4]) because every R-module is flat. Moreover a von Neumann regular ring R has Krull dimension equal to zero and it is reduced (c.f. Theorem 3.71, [51]) .

Next we collect some characterizations of commutative von Neumann regular rings we are using in the sequel. We refer to [36] as main reference in the topic.

Proposition 2.3.2 (cf. Theorems 1.1 & 1.6, [36]). *Let R be a commutative ring with identity. The following statementes are equivalent:*

1. *R is a von Neumann regular ring.*
2. *Every R-module is flat.*
3. *Every finitely generated ideal is principal generated by an idempotent*
4. *$R_{\mathfrak{m}}$ is a field for every maximal ideal $\mathfrak{m}$ of R.*
5. *Every prime ideal is maximal and R has no nonzero nilpotents.*
6. *All simple R-modules are injective.*

2.3.2. Characterization of von Neumann regular rings.

We need a previous result in order to prove the characterization of von Neumann regular rings by properties of linear systems.

Proposition 2.3.3 (cf. Proposition 3G, [55]). *Let $(R, \mathfrak{m}, k)$ be a local ring. Let M be a R-module. Suppose that either $\mathfrak{m}$ is nilpotent or M is finite over R. Then*

$$M \text{ is free} \Leftrightarrow M \text{ is projective} \Leftrightarrow M \text{ is flat.}$$

We give our main results:

Theorem 2.3.4. *(A Brunovsky's Local Theorem.) Let R be a von Neumann regular ring. Let $\Sigma = (X, f, B)$ be a linear system over R where X is a finitely generated R-module. The following statements are equivalent:*

1. *Σ is reachable.*

2. *Σ is a locally Brunovsky system.*

Proof. $(1 \Rightarrow 2)$ Let Σ be a reachable system over R. Let $\mathfrak{p}$ be a prime ideal of R. Let

$$\Sigma_{\mathfrak{p}} = (X \otimes_R R_{\mathfrak{p}}, f \otimes 1, B \otimes_R R_{\mathfrak{p}}) = (X_{\mathfrak{p}}, f_{\mathfrak{p}}, B_{\mathfrak{p}})$$

be the linear system Σ localized at $\mathfrak{p}$, prime ideal of R. Note that surjectivity of linear map is a local property. Hence reachability of linear systems is also a local property and consequently $\Sigma_{\mathfrak{p}}$ is a reachable linear system over local ring $R_{\mathfrak{p}}$ for all prime ideal $\mathfrak{p}$ of R.

Let $M_i^{\Sigma_{\mathfrak{p}}} = X_{\mathfrak{p}}/(B_{\mathfrak{p}} + f_{\mathfrak{p}}B_{\mathfrak{p}} + \ldots + f_{\mathfrak{p}}^{i-1}B_{\mathfrak{p}})$ be the $R_{\mathfrak{p}}$-finitely generated modules invariants of the system $\Sigma_{\mathfrak{p}}$ and note that the invariants of localized system are the localization of invariants. That is to say, $M_i^{\Sigma_{\mathfrak{p}}} \simeq M_i^{\Sigma} \otimes_R R_{\mathfrak{p}}$ where $M_i^{\Sigma} = X/(B + fB + \ldots + f^{i-1}B)$ being the invariants finitely generated R-modules of the system Σ.

Because R is a von Neumann regular ring, invariant modules M_i^{Σ} are flat R- modules. Since flatness is a local property, $M_i^{\Sigma_{\mathfrak{p}}}$ are flat $R_{\mathfrak{p}}$-modules and by Proposition 2.3.3 hence free (because they are finitely generated modules and $R_{\mathfrak{p}}$ is local). Since $M_i^{\Sigma_{\mathfrak{p}}}$ is free therefore M_i^{Σ} is locally free and then Σ is locally Brunovsky linear system.

$(2 \Rightarrow 1)$ If Σ is a locally Brunovsky linear system then all $\Sigma_{\mathfrak{p}}$ of Brunovksy type and hence reachable. But reachability is local, it follows that Σ is reachable. □

Theorem 2.3.5. *(Locally Brunovsky Rings.) Let Σ be a linear system over R. The following statements are equivalent:*

i) R is von Neumann regular ring.

ii) Σ is reachable if and only if it is locally Brunovsky where X is a finitely generated R-module.

Proof. 1) $\Rightarrow$ 2) Is above Theorem 2.3.4.

2) $\Rightarrow$ 1) In order to prove that R is a von Neumann regular ring we need to show that every finitely generated ideal is principal and generated by an idempotent element.

Let $I = (g_1, \ldots, g_m)$ be a finitely generated ideal. Consider the following reachable linear system Σ:

$$\Sigma = \left(R^2, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, B = R \oplus (g_1, \ldots, g_m) \right)$$

or, in matrix form,

$$\Sigma = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \ldots 0 \\ 0 & g_1 \ldots g_m \end{pmatrix} \right)$$

The first M_i^Σ invariant is $M_1^\Sigma = R/I$ which is finitely generated and finitely presented because we have the following trivial presentation

$$R^n \xrightarrow{I} R \longrightarrow R/(g_1 \ldots g_m) \longrightarrow 0$$

We know that Σ is locally Brunovsky and hence M_1^Σ is locally free. So, by ([82], §2, 2.4), invariant M_1^Σ is a finitely generated projective R-module and then the following exact sequence (where mappings are natural) splits

$$0 \to I \to R \to R/I \to 0$$

and hence $R \simeq I \oplus R/I$. Now, by ([82], §2. 2.1.2,), we can find idempotents $e \in I, f \in R/I$ such that $f = 1 - e$, $1 = e + f$ in R and $I = eR, R/I = fR$ from which it follows that $I = (e)$ is principal generated by an idempotent. □

2.3.3. Von Neumann regular noetherian rings.

In above sections the equation $X \simeq Z_1 \oplus Z_2^2 \oplus \ldots \oplus Z_s^s \oplus \ldots$ has been studied in the case of locally Brunovsky linear systems over projectively trivial rings and over finite product of projectively trivial rings. With these results we can compute how many locally Brunovsky linear systems under feedback isomorphia there are over a von Neumann regular noetherian ring if we fix the rank state space X, $rank(X) = n$.

We need an algebraic result that we use in the sequel.

Theorem 2.3.6. *Let R be a commutative ring with identity, then the following are equivalent:*

i) R is von Neumann regular noetherian ring.

ii) There exists a finite number of fields $\mathbb{K}_i$ such that $R \simeq \mathbb{K}_1 \times \ldots \times \mathbb{K}_t$.

Proof. $i) \Rightarrow ii)$

We recall that if R is a commutative ring such that $Spec(R) = x_1 \sqcup \ldots \sqcup x_t$ where x_i is a closed point then $R \simeq R_1 \times \ldots \times R_t$ where $x_i = Spec(R_i)$. In order to apply this result to our case we study the spectrum of R: Since R is a von Neumann noetherian ring by hypothesis, R is zero dimensional and noetherian and so, R is an artinian reduced ring and then $Spec(R) = X$ is a finite set of closed points $\{x_1, \ldots, x_t\}$ with the Zariski's topology, see [3]. We denote by $\#\ Spec(R) = t$ the cardinal of the spectrum of R. So, we have

$$Spec(R) = x_1 \sqcup \ldots \sqcup x_t = Spec(k(x_1)) \sqcup \ldots \sqcup Spec(k(x_t))$$

where $k(x_i)$ is the residue field of point x_i of the spectrum of R.

By 4) and 5) of Proposition 2.3.2 is verified that $Spec\ (k(x_i)) = Spec(R_{\mathfrak{p}_{x_i}}/\mathfrak{p}_{x_i}) = Spec(R_{\mathfrak{m}_{x_i}}/\mathfrak{m}_{x_i}) = Spec(\mathbb{K}_i/\mathfrak{m}_{x_i}) = Spec(\mathbb{K}_i/(0)) = Spec(\mathbb{K}_i)$ for $i = 1, \ldots, t$.

Since $Spec(R)$ verifies that is disjoint union of spectra then we conclude the proof and $R \simeq \mathbb{K}_1 \times \ldots \times \mathbb{K}_t$

$ii) \Leftarrow i)$ Any finitely generated R-module M satisfies that $M_{\mathfrak{p}_{x_i}}$ is a $\mathbb{K}_i$ vector space thus flat over $\mathbb{F}_i$. Since flatness is a local condition we deduce that all finitely generated R-modules are flat and therefore all R-modules are flat (direct limit preserves flatness, [3] and [52]). Then R is a von Neumann regular ring. Since finite product of noetherian rings is noetherian we conclude the proof. □

We compute the number of classes of feedback isomorphisms of locally Brunovsky linear systems with state space the projective finitely generated R-module X of rank n over commutative noetherian von Neumann regular rings.

Theorem 2.3.7. *If R is a von Neumann regular noetherian commutative ring then the number of classes of locally Brunovsky linear systems with state space X of rank n is*

$$fe_R(m) = fe_R(n) = [p_{\mathbb{N}}(n)]^{\#Spec(R)}$$

Proof. By Theorem 2.3.6, R decomposes in a finite product of fields that they are projectively rings and by Corollary 2.2.6 we conclude the proof. □

Lemma 2.3.8. *The rings $R = \mathbb{Z}/l\mathbb{Z}$ where $l = p_1 \cdots p_t$ is a square free integers and where p_i are different primes are von Neumann rings.*

Proof. Ideals of $\mathbb{Z}/l\mathbb{Z} = \mathbb{Z}/p_1 \cdot \ldots \cdot p_t\mathbb{Z}$ is in bijective correspondence to ideals (d) of $\mathbb{Z}$ that contain to $p_1 \cdot \ldots \cdot p_t$ where d is not an unit. But $(d) \supset (p_1 \cdot \ldots \cdot p_t)$ if and only if $d \mid p_i$ for some $i = 1, ...t$ and this is verified if and only if $d = p_i$ for some $i = 1, ...t$. Then the prime ideals of R are $(p_1), \ldots, (p_t), (0)$ and $\mathbb{Z}/(p_1 \cdot \ldots \cdot p_t)\mathbb{Z}$. Maximal ideals are $(p_1), \ldots, (p_k)$.

If we localize the ring at maximal ideals we get

$$(\mathbb{Z}/l\mathbb{Z})_{p_i} = (\mathbb{Z}/(p_1 \cdot \ldots \cdot p_t)\mathbb{Z})_{p_i} = (\mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_t\mathbb{Z})_{p_i} =$$

$$= (\mathbb{Z}/p_1\mathbb{Z})_{p_i} \times \ldots \times (\mathbb{Z}/p_i\mathbb{Z})_{p_i} \times \ldots \times (\mathbb{Z}/p_t\mathbb{Z})_{p_i} =$$

$$= 0 \times \ldots \times 0 \times \mathbb{Z}/p_i\mathbb{Z} \times 0 \ldots \times 0 = \mathbb{Z}/pi\mathbb{Z} \text{ for } i = 1...t.$$

Since the localization at every maximal ideal $\mathfrak{m}_i$ is a field, by Proposition 2.3.2 the ring is a von Neumann regular noetherian ring. □

Remark 2.3.9. *If $R = \mathbb{Z}/l\mathbb{Z}$ where $l = p_1 \cdots p_t$ is square free then is a von Neumann noetherian regular ring and hence each reachable system is locally Brunovsky, then $p_{\mathbb{N}}(n)^t$ is the number of classes of reachable and locally Brunovsky linear systems with state space $X \simeq R^n$.*

Remark 2.3.10. *If we drop off noetherian hypothesis then it might exist infinitely many different isomorphim classes of reachable (i.e. locally Brunovsky) linear systems over von Neumann ring R with fixed state space. For instance consider the ring $\mathbb{F}_2[x_1, x_2, \ldots, x_n, \ldots]$ of polynomials in the indeterminates $\{x_i\}_{i=1}^{\infty}$ over field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and the ideal generated by all $x_i^2 - x_i$. The ring $\mathbb{B} = \mathbb{F}_2[x_1, \ldots, x_n, \ldots]/(x_i^2 - x_i)$ is a boolean ring ($b^2 = b \ \forall \ b \in \mathbb{B}$) and thus von Neumann regular ring.*

Let Σ_i be the following systems over $\mathbb{B}$

$$\Sigma_1 = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & x_1 \end{pmatrix} \right], \Sigma_2 = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & x_1x_2 \end{pmatrix} \right], \ldots,$$

$$, \Sigma_n = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & x_1 \cdot \ldots \cdot x_n \end{pmatrix} \right], \ldots$$

We have $M_1^{\Sigma_n} \simeq R/(x_1 \cdot \ldots \cdot x_n)$ and we consider the following exact sequences

$$0 \longrightarrow (x_1 \ldots x_i) \longrightarrow R \longrightarrow M_1^{\Sigma_i} \simeq R/(x_1 \ldots x_i) \longrightarrow 0$$

$$0 \longrightarrow (x_1 \ldots x_j) \longrightarrow R \longrightarrow M_1^{\Sigma_j} \simeq R/(x_1 \ldots x_j) \longrightarrow 0$$

If $M_1^{\Sigma_i} \simeq M_1^{\Sigma_j}$ *then by Schanuel's Lemma*

$$R \oplus (x_1 \dots x_i) \simeq R \oplus (x_1 \dots x_j) \text{ for } i \neq j$$

Since the following surjective maps (assume $i < j$*)*

$$(x_1 \dots x_i)R \xrightarrow{\cdot x_{i+1} \dots x_j} (x_1 \dots x_j)R$$

have non trivial kernels, the ideals $(x_1 \dots x_i)R$ *and* $(x_1 \dots x_j)R$ *can not be isomorphic as* R*-modules for* $i \neq j$*. Therefore* $M_1^{\Sigma_i} \not\simeq M_1^{\Sigma_j}$ *and* $\Sigma_i \overset{f.i.}{\not\simeq} \Sigma_j$*.*

Example 2.3.11. *We will compute* $fe_R(m)$ *over* $R = \mathbb{Z}/30\mathbb{Z}$ *for a locally Brunovsky linear system over* R*.*

Since $\mathbf{P}(\mathbb{Z}/30\mathbb{Z}) \simeq \mathbf{P}(\mathbb{Z}/2\mathbb{Z}) \times \mathbf{P}(\mathbb{Z}/3\mathbb{Z}) \times \mathbf{P}(\mathbb{Z}/5\mathbb{Z}) \simeq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ *then we look for the number of solutions of* $m = x_1 + 2x_2 + 3x_3 + ... + sx_s$ *where* n, x_i *are triples of natural numbers.*

If the state space is determined by the triple $(1, 2, 3)$ *then the equation to solve is the following system*

$$\begin{cases} 1 = a_1 + 2a_2 + 3a_3 + ... + sa_s \\ 2 = b_1 + 2b_2 + 3b_3 + ... + sb_s \\ 3 = c_1 + 2c_2 + 3c_3 + ... + sc_s \end{cases}$$

Since $\mathbb{N}$ *is cancellative the number of solutions of the first equation is* $p_{\mathbb{N}}(1)$*, of the second equation is* $p_{\mathbb{N}}(2)$ *and of the third equation is* $p_{\mathbb{N}}(3)$*. So,* $fe_{\mathbb{Z}/30\mathbb{Z}}(n) = p_{\mathbb{N}}(1) \cdot p_{\mathbb{N}}(2) \cdot p_{\mathbb{N}}(3) = 1 \cdot 2 \cdot 3 = 6$*.*

The reader can see the number of solutions with associated Young's Diagrams in the Table 2.1.

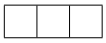
Partition	P(1)	P(2)	P(3)	Partition	P(1)	P(2)	P(3)
1= 1 2=1+1 3=1+1+1				1= 1 2=2 3=1+1+1			
1=1 2=1+1 3=2+1				1=1 2=2 3=2+1			
1=1 2=1+1 3=3				1=1 2=2 3=3			

Table 2.1: *Partitions in* $\mathbb{Z}/30\mathbb{Z}$

.

2.4. Locally Brunovsky linear systems over Dedekind domains.

Once the cases of projectively trivial rings and their finite products are solved, next step would be the study of Dedekind domains. Note that these rings are of interest both in linear algebra and in linear systems theory because they belong to the class of BCS rings, see [80], which are the largest class known of PA rings (i.e. commutative rings where reachability and asymptotic controllability are equivalent, see [7]).

In order to compute the number of solutions of the equation (2.1) for a locally Brunovsky linear system Σ over a Dedekind domain, first we give some preliminary results about Dedekind Domains.

In this section R denotes a Dedekind domain with field of fractions $\mathbb{K}(R)$; that it is to say, R is a commutative domain (no nonzero zero-divisors) which is noetherian, integrally

closed and 1-dimensional, and Σ is considered as locally Brunovsky linear system over R.

Proposition 2.4.1 (cf. I.3.4,[82]). *Let R be a commutative noetherian 1-dimensional ring. Then all finitely generated projective R-module P is completely classifed by its rank, $\mathrm{rk}(P) = \dim(P \otimes \mathbb{K}(R))$, and its determinant (a line bundle over R), $\wedge^{\mathrm{rk}(P)} P$. In particular, to be precise, every finitely generated projective R-module P of rank ≥ 1 is isomorphic to $R^{\mathrm{rk}(P)-1} \oplus \wedge^{\mathrm{rk}(P)} P$.*

We give some properties of the structure of line bundles in Appendix C to clarify the computation of the determinant of a finitely generated R-module P.

In order to study $\mathbf{P}(R)$ of a Dedekind domain we give a previous result of the Picard Group of the ring, $Pic(R)$.

Proposition 2.4.2 (cf. *I*§3 [82]). *Let $\mathrm{Pic}(R)$ be the set of isomorphism classes of line bundles over R (finitely generated projective R-modules of rank equals 1). Hence $(\mathrm{Pic}(R), \otimes_R)$ is an abelian group where $R = 1_{\mathrm{Pic}(R)}$ and $P^{-1} = \mathrm{Hom_R(P, R)}$.*

Proposition 2.4.3 (Chapter VII, §4.,10, Corollary, [4]). *Let R be a Dedekind domain. Let P be a finitely generated R-module of $rank(P) = n$. Then $P \simeq T(P) \oplus M$ where $T(P)$ is the torsion submodule of P and $M \simeq R^n$.*

Remark 2.4.4. *Let P be a projective finitely generated R-module. Note that above proposition implies that over a Dedekind domain, if $rank(P) = 0$ then $det(P) = R$.*

Proposition 2.4.5. *Let R be a Dedekind domain. Then $\mathbf{P}(R) \simeq [\mathbb{N}^+ \times Pic(R)] \cup \{0\}$.*

Proof. Since R is a Dedekind domain, R is a noetherian commutative ring with Krull dimension equals to 1. By Proposition 2.4.1 all finitely generated projective R-module, P, is completely determined by its rank and its determinant. Rank of P is a natural number and $det(P)$ is an algebraic line bundle so $\mathbf{P}(R) \to Pic(R) \oplus \mathbb{N}$ is injective.

By Proposition 2.4.3 and Remark 2.4.4 we have the isomorphism $\mathbf{P}(R) \simeq Pic(R) \oplus \mathbb{N} - \{(L, 0)\}$ where $L \ncong R$. Thus, $\mathbf{P}(R)$ equals $[\mathbb{N}^+ \times Pic(R)] \cup \{0\}$ as set.

□

Arithmetic in $(\mathbf{P}(R), \oplus)$ is given by

$$P \oplus Q \cong R^{\mathrm{rk}(P)+\mathrm{rk}(Q)-1} \oplus \left(\wedge^{\mathrm{rk}(P)} P \otimes_R \wedge^{\mathrm{rk}(Q)} Q \right) \tag{2.6}$$

where zero module 0 is the identity and internal law $\oplus$ is commutative.

Remark 2.4.6. *Let X be a finitely generated projective R-module. Looking for the number of classes of feedback isomorphisms of locally Brunovsky linear systems over X ($fe_R(m)$) is equivalent to computing the number of solutions of the following equation $X = Z_1 \oplus Z_2^2 \oplus \cdots \oplus Z_s^s$ in $\mathbf{P}(R)$. Since $\mathbf{P}(R) \simeq [\mathbb{N}^+ \times Pic(R)] \cup \{0\}$, the class of isomorphisms of X is a pair $m = (rk(X), det(X))$ and $fe_R(m)$ is determined by solutions of*

$$\mathrm{rk}(X) = \mathrm{rk}(Z_1) + 2\,\mathrm{rk}(Z_2) + \ldots + s\,\mathrm{rk}(Z_s) \text{ in } (\mathbb{N}, +) \tag{2.7}$$

together with a solution of

$$\det(X) = \det(Z_1) \otimes \det(Z_2)^{\otimes 2} \otimes \cdots \otimes \det(Z_s)^{\otimes s} \text{ in } Pic(R). \tag{2.8}$$

Note that the solutions of equation (2.8) in $Pic(R)$ are entangled with solutions of ranks equation in $\mathbb{N}$ (by Remark 2.4.4).

Remark 2.4.7. *Note that if we fix the rank of the state space, $rk(X) = n$, then $X \cong R^{n-1} \oplus L$ and*

$$\det(X) = \det(R^{n-1} \oplus L) = \wedge^n(R^{n-1} \oplus L) = \bigoplus_{i=0}^{n}[(\wedge^i R^{n-1}) \otimes (\wedge^{n-i} L)] =$$

$$= \bigoplus_{i=0}^{n-2}[R^{\binom{n-1}{i}} \otimes 0] \oplus [(\wedge^{n-1} R^{n-1}) \otimes (\wedge^1 L)] \oplus [\wedge^n R^{n-1} \otimes \wedge^0 L] = R \otimes L = L$$

and equation (2.8) turns to be $L = \det(Z_1) \otimes \det(Z_2)^{\otimes 2} \otimes \cdots \otimes \det(Z_s)^{\otimes s}$.

We recall that from the structure theorem for finite abelian groups for we can aproximate us to the solutions of the equation (2.8) over determinant line bundles in a easier way.

Theorem 2.4.8 (cf. Theorem 7 [21])**.** *Given any abelian group G, there exists a Dedekind domain R such that $Pic(R) \cong G$.*

Remark 2.4.9. *Let $\mid Pic(R) \mid = p$ be the order of $Pic(R)$ with p prime. By above proposition we will use the isomorphism*

$$(Pic(R), \otimes) \xrightarrow{\cong}{}^{\alpha} (\mathbb{Z}/p\mathbb{Z}, +)$$

$$L \quad \mapsto \quad \alpha(L)$$

where in particular $\alpha(R) = \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$.

In order to solve the equations (2.7) and (2.8) we introduce the following combinatorial numbers:

Definition 2.4.10. *Let n be a positive integer and $1 \leq k \leq n$. We denote by $\nu(n,k)$ the set of partitions of integer n into k different summands. We also denote by $\nu(n,k)$ its cardinal.*

Example 2.4.11. *As matter of example we study $\nu(5,1)$; that is, the number of partitions of integer 5 into 1 different summands and $\nu(5,2)$; that is, the number of partitions of integer 5 into 2 different summands.*

Case $n = 5$, $k = 1 \Rightarrow \nu(5,1) = 2$, *See Table 2.2.*

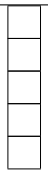
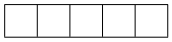
Partition	Young Diagram
5=1+1+1+1+1	
5=5	

Table 2.2: $\nu(5,1)$ *Partitions*

Case $n = 5$, $k = 2 \Rightarrow \nu(5,2) = 5$. *See Table 2.3.*

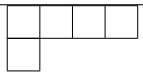
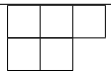
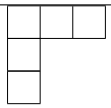
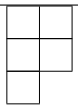
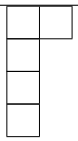
Partition	Young Diagram
5=4+1	
5=3+2	
5=3+ 1+1	
5=2+2 +1	
5=2+ 1+1+1	

Table 2.3: $\nu(5,2)$ *Partitions.*

Note that $\nu(5,1)+\nu(5,2)=p_{\mathbb{N}}(5)=7$.

Definition 2.4.12. *Let* p *be a prime number. We denote by* $\nu(n,k,p)$ *the set of partitions in* $\nu(n,k)$ *where all coefficientes of the summands are multiples of* p. *We also denote by* $\nu(n,k,p)$ *its cardinal. For convenience let's denote by* $\nu'(n,k,p)=\nu(n,k)-\nu(n,k,p)$.

Example 2.4.13. *As matter of example* $\nu(6,2)$ *is the number of partitions of integer* 6 *into* 2 *different summands and hence contains exactly partitions*

$$(51),(42),(411),(3111),(2211),(21111)$$

and therefore $\nu(6,2)=6$. *Now,* $\nu(6,2,2)=1$ *because the only partition in* $\nu(6,2)$ *with the property that all summands are multiple of* 2 *is* (42) .

Remark 2.4.14. *Combinatorial number* $\nu(n,k)$ *needs further study. We only point out two straightforward properties:*

(i) $\nu(n,1)=div(n)$*; that is* $\nu(n,1)$ *equals the number of divisors (including both* 1 *and* n*) of integer* n.

(ii) If $n<k(k+1)/2$ *then* $\nu(n,k)=0$ *because the least partition one can form with* k *different summands is* $(k,k-1,...,2,1)$ *and therefore an* $n\geq 1+2+\cdots+k=\frac{k(k+1)}{2}$ *is needed.*

(iii) $\nu(n,1)+\nu(n,2)+\ldots=p_{\mathbb{N}}(n)$

We remember some notations about the formula of the number of feedback classes of locally Brunovsky linear systems over R.

Notation. *1. We denote by* $fe_R(m)$ *the number of classes of feedback isomorphisms of locally Brunovsky linear systems over* R *with a state space a finitely projective* R*-module* X *denoting by* m *the class of isomrphisms of* X *in* $\mathbf{P}(R)$.

2. We denote by $fe_R(X)$ *the number of classes of feedback isomorphisms of locally Brunovsky linear systems over* R *with state space* X *of rank* n. *This notation is needed because over a Dedekind domain if rank* $X=n$ *then* X *could be* $X\simeq R^n$ *or* $X\simeq R^{n-1}\oplus L$.

We state our main result:

Theorem 2.4.15. *Let R be a Dedekind domain and let $Pic(R)$ be its Picard Group. Then, the number of feedback classes of locally Brunovsky linear systems $\Sigma = (X, f, B)$ over R is computed as follows:*

(i) $fe_R(m)$ is the number of solutions $(Z_1, Z_2, \ldots, Z_s)$ of the system of equations in $\mathbb{N}$ and $Pic(R)$.

$$\begin{cases} \operatorname{rk}(X) = \operatorname{rk}(Z_1) + 2\operatorname{rk}(Z_2) + \cdots + s\operatorname{rk}(Z_s) \\ \\ \det(X) = \det(Z_1) \otimes \det(Z_2)^{\otimes 2} \otimes \cdots \otimes \det(Z_s)^{\otimes s} \end{cases} \tag{2.9}$$

From following items we fix $\operatorname{rk}(X) = n$.

(ii) If $\mid Pic(R) \mid = \infty$ then $\operatorname{fe}_R(m) = \infty$.

(iii) If $\mid Pic(R) \mid = d < \infty$ then $fe_R(m) = \sum_{k=1}^{n} \nu(n,k) \cdot d^k$ where d is not prime.

(iv) If $\mid Pic(R) \mid = p$ is prime then $fe_R(R^n) = \sum_{k=1}^{n} \left[\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^{k-1}\right]$.

(v) If $\mid Pic(R) \mid = p$ is prime then $fe_R(R^{n-1} \oplus L) = \sum_{k=1}^{n} \nu'(n,k,p) \cdot p^{k-1}$

Proof. (i) Is clear by Remarks 2.4.6 and 2.4.7.

(ii) Suppose that $Pic(R)$ is of infinite order and L varies in $Pic(R)$. Then

$$(Z_1 = R^{n-1} \oplus L, Z_2 = 0, ...)$$

are infinitely many different solutions of first equation of (2.9).

(iii) $\nu(n,k)$ is the set of solutions $(\operatorname{rk}(Z_1), \operatorname{rk}(Z_2), \ldots, \operatorname{rk}(Z_n))$ of the equation (2.9) where k of the entries of above t-uple are non zero. Thus

$$(\operatorname{rk}(Z_1), \operatorname{rk}(Z_2), \ldots, \operatorname{rk}(Z_n)) = (0, \ldots, \operatorname{rk}(Z_{i_1}), \ldots, \operatorname{rk}(Z_{i_k}), \ldots, 0, \ldots)$$

In order to realize solutions $(Z_1, \ldots, Z_n)$ we are free to choose $L_1, \ldots, L_k$ in $Pic(R)$ to obtain solutions

$$(0, \ldots, 0, R^{rk(Z_{i_1})-1} \oplus L_1, 0, \ldots, 0, R^{rk(Z_{i_k})-1} \oplus L_k, 0, \ldots)$$

Since L_i varies in $Pic(R)$, then there are exactly d^k different choices and therefore

$$fe_R(m) = \sum_{k=1}^{n} \nu(n,k) \cdot d^k$$

(iv) If $\mid Pic(R) \mid = p$ is prime, then by Remark 6.1.9, $\mathrm{Pic}(R) \cong \mathbb{Z}/p\mathbb{Z}$, and equations giving $fe_R(R^n)$ are:

$$\begin{cases} n = \mathrm{rk}(Z_1) + 2\,\mathrm{rk}(Z_2) + \cdots + n\,\mathrm{rk}(Z_n) \text{ in } (\mathbb{N}, +) \\ \\ 0 = a_1 + 2a_2 + \cdots + na_n \text{ in } (\mathbb{Z}/p\mathbb{Z}, +). \end{cases} \tag{2.10}$$

where $a_i = \alpha(\det(Z_i))$

There are exactly $\nu(n,k)$ different solutions for the ranks equation with exactly k non zero $\mathrm{rk}(Z_i)'s$. Every solution of ranks equation gives some choices for the second equation. But is crucial to know how many coefficients are non zero modulo p.

The equation of the determinants (2.10) is on the form

$$0 = a_1 + 2a_2 + \ldots + pa_p + ... + (2p)a_{2p} + \ldots + na_n \ \textit{in}\ \mathbb{Z}/p\mathbb{Z} \tag{2.11}$$

Let us reorder the summands such that we have $l = \lfloor \frac{n}{p} \rfloor$ summands which coefficientes are multiple of p and $n - l$ summands whose coefficientes are prime with p.

$$0 = \overbrace{pa_p + 2pa_{2p} + \ldots + lpa_{lp}}^{l \text{ summands}} + \overbrace{a_1 + \ldots + (p-1)a_{p-1} + (p+1)a_{p+1} + ...}^{(n-l) \text{ summands}}$$

Since the group of l summands vanishes module p, then above equation in $\mathbb{Z}/p\mathbb{Z}$ is in fact

$$0 = a_1 + \ldots + (p-1)a_{p-1} + (p+1)a_{p+1} + ...$$

or even

$$0 = 0 \text{ if all non zero } (z_i)'s \text{ are on the form } i = \lambda p.$$

In the former case, corresponding to $\nu(n,k,p)$ in Definition 2.4.12, we have exactly $p^{(k-l-1)}$ choices of $a_1, ..., a_{p-1}, a_{p+1}, ...$ and p^l choices for $a_p, a_{2p}, ..., a_{lp}$. So, there are $p^{k-l-1} \cdot p^l = p^{k-1}$ different choices for every solution in $\nu(n,k)$.

In the latter case, corresponding to $\nu'(n,k,p)$ in Definition 2.4.12, p^k different solutions are freely chosen for $a_p, \ldots, a_{kp}$.

Therefore

$$fe_R(R^n) = \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^{k-1} \right)$$

(v) If $rk(X) = n$ but X is not free, then $X \cong R^{n-1} \oplus L$ and $\alpha(L) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. The equations to compute $fe_R(R^{n-1} \oplus L)$ are

$$\begin{cases} n = \mathrm{rk}(Z_1) + 2\,\mathrm{rk}(Z_2) + \cdots + n\,\mathrm{rk}(Z_n) \text{ in } (\mathbb{N}, +) \\ \\ 0 \neq \alpha(L) = a_1 + 2a_2 + \cdots + na_n \text{ in } (\mathbb{Z}/p\mathbb{Z}, +) \text{ } \textit{where } a_i = \alpha(\det(z_i)) \end{cases}$$

Analogous reasoning of (v) gives us

$$0 \neq \alpha(L) = a_1 + 2a_2 + \cdots + (p-1)a_{p-1} + (p+1)a_{p+1} + \ldots$$

or

$$0 \neq \alpha(K) = 0 \text{ having no solution.}$$

Therefore if X is not free of rank n we have

$$fe_R(R^{n-1} \oplus L) = \sum_{k=1}^{n} \nu'(n,k,p) \cdot p^{k-1}$$

□

Note that if we perform the sum of all computations over the different elements of $Pic(R)$, then we obtain coherent relationship between our formulae.

$$\sum_{L \in Pic(R)} fe_R(R^{n-1} \oplus L) = \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^{k-1} \right) + (p-1) \cdot \sum_{k=1}^{n} \nu'(n,k,p) \cdot p^{k-1} =$$

$$= \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + p \cdot \nu'(n,k,p) \cdot p^{k-1} \right) = \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^k \right) =$$

$$= \sum_{k=1}^{n} \left(\nu(n,k,p) + \nu'(n,k,p) \right) \cdot p^k = \sum_{k=1}^{n} \nu(n,k) \cdot p^k.$$

Remark 2.4.16. *The item iv) of above Theorem could be applied over $R = \mathcal{C}(\mathbb{S}^1)$, the ring of real continuous functions defined on the unit circle because it is a Dedekind domain whose $Pic(R) \simeq \mathbb{Z}/2\mathbb{Z}$.*

Furthermore, above computations of feedback isomorphisms of locally Brunovsky linear systems are invariant by homeomorphism of topological space and, so, the result holds in the case of all topological space in the class of homeomorphisms of unit circle. For example it is useful in the ring of real continuous functions defined over every figure in the plane that is homeomorphic to unit circle; namely, every closed curve.

Remark 2.4.17. *Note that we have computed the number of classes of feedback isomorphims of locally Brunovsky linear systems over all non singular differentiable connected and compact manifolds of dimension 1.*

2.4.1. Computational examples

1) Let $R = \mathcal{C}(\mathbb{S}^1)$ be the ring of real continuous functions defined on the unit circle. It is a Dedekind domain such that $Pic(R) \simeq \mathbb{Z}/2\mathbb{Z}$. We compute the $fe_R(X \simeq R^6)$.

In the first case, we have one $b_i \neq 0$. Note that $\nu(6,1) = 4$ such that $\nu(6,1,2) = 2$ and $\nu'(6,1,2) = 4 - 2 = 2$. So, for $k = 1$ we have $\nu(6,2,5) \cdot 2^1 + \nu'(6,2,5) \cdot 2^{1-1} = 6$. As we can see all solutions in Table 2.4.

In the second case, we have two $b_i \neq 0$. Note that $\nu(6,2) = 6$ such that $\nu(6,2,2) = 1$ and $\nu'(6,2,2) = 6 - 1 = 5$. So, for $k = 2$ we have $\nu(6,2,2) \cdot 2^2 + \nu'(6,2,2) \cdot 2^{2-1} = 14$. As we can see all solutions in Table 2.5.

In the third case, we have three $b_i \neq 0$. Note that $\nu(6,3) = 1$ such that $\nu(6,3,2) = 0$ and $\nu'(6,3,2) = 1 - 0 = 1$. So, for $k = 3$ we have $\nu(6,3,2) \cdot 2^3 + \nu'(6,3,2) \cdot 2^{3-1} = 4$. As we can see all solutions in Table 2.6.

There are not more cases because we can not make the number six with four or more summands. Then $fe_R(X \simeq R^6) = 6 + 14 + 4 = 24$. We can compute the solutions by the algorithm described in [15].

Sol. b_i	Eq. in a_i	Sol. a_i	Number of solutions a_i
$b_1 = 6$	$0{=}a_1$	$a_1 = 0$	$2^{1-1} = 1$
$b_2 = 3$	$0{=}\ 2a_2 \to 0 = 0$	$a_2 = 0, 1$	$2^1 = 2$
$b_3 = 2$	$0{=}3a_3$	$a_3 = 0$	$2^{1-1} = 1$
$b_6 = 1$	$0 = 6a_6 \to 0 = 0$	$a_6 = 0, 1$	$2^1 = 2$

Table 2.4: *Example 1: Solutions with one* $b_i \neq 0$

Sol. b_i	Eq. in a_i	Sol. a_i	Number of solutions a_i
$b_1 = 1$, $b_5 = 1$	$0{=}a_1 + 5a_5$	(0,0), (1,1)	$2^{2-1} = 2$
$b_1 = 2$, $b_4 = 1$	$0{=}\ a_1 + 4a_4$	(0,0), (0,1)	$2^{2-1} = 2$
$b_2 = 1$, $b_4 = 1$	$0{=}\ 2a_2 + 4a_4$	(0,0),(1,0) (0,1), (1,1)	$2^2 = 4$
$b_1 = 3$, $b_3 = 1$	$0{=}\ a_1 + 3a_3$	(0,0), (1,1)	$2^{2-1} = 2$
$b_1 = 4$, $b_2 = 1$	$0{=}\ a_1 + 2a_2$	(0,0), (0,1)	$2^{2-1} = 2$
$b_1 = 2$, $b_2 = 2$	$0{=}\ a_1 + 2a_2$	(0,0), (0,1)	$2^{2-1} = 2$

Table 2.5: *Example 1: Solutions with two* $b_i \neq 0$

Sol. b_i	Eq. in a_i	Sol. a_i	Number of solutions a_i
$b_1 = 1$,$b_2 = 1$, $b_3 = 1$	$0 = a_1 + 2a_2 + 3a_3$	$a_1 = a_2 = a_3 = 0$ $a_1 = a_3 = 0, a_2 = 1$ $a_1 = a_3 = 1, a_2 = 0$ $a_1 = a_2 = a_3 = 1$	$2^{3-1} = 4$

Table 2.6: *Example 1: Solutions with three* $b_i \neq 0$

2) Another example of feedback classification of locally Brunovsky linear systems over Dedekind domain allows us to classify systems over not trivial algebraic manifolds. Let R be a Dedekind domain whose $\mid Pic(R) \mid = 5$. Let $\Sigma = (X, f, B)$ be a linear system over R.

Let $X \simeq R^6$ be its state space. This is the case iv) of Theorem 2.4.15, then we look for the number of solutions of the foloowing system

$$\begin{cases} n = rk(z_1) + 2rk(z_2) + 3rk(z_3) + ... + srk(z_s) \\ det(X) = det(z_1) + 2det(z_2) + 3det(z_3) + ... + sdet(z_s) \end{cases} \tag{2.12}$$

The equation of the ranks is over $\mathbb{N}$ and the equation of the determinant line bundles is over $Pic(R) \overset{\alpha}{\simeq} \mathbb{Z}/p\mathbb{Z}$. Moreover $det(X) = det(R^n) = R$, the neutral element of $Pic(R)$ as abelian group, so $\alpha(R) = 0 \in \mathbb{Z}/p\mathbb{Z}$. In this case we have

$$\begin{cases} 6 = b_1 + 2b_2 + 3b_3 + ... + sb_s \\ 0 = a_1 + 2a_2 + 3a_3 + ... + sa_s \end{cases} \tag{2.13}$$

where $0, a_i \in \mathbb{Z}/5\mathbb{Z}$ and $b_i \in \mathbb{N}$.

We start from that the number of solutions of the equation $0 = a_1 + 2a_2 + 3a_3 + ... + sa_s$ *where* $a_i, 0 \in \mathbb{Z}/p\mathbb{Z}$ depends on how many summands are there and on how many coefficients of the summands of the equation are multiples of p. We suppose that we have k summands (not necessarily ordered), then we can find two cases (see the proof of Theorem 2.4.15)

1. If all coefficientes of the summands are multiples of p, then the equation to solve becomes in $0 = 0$, so we have as solutions all possible combinations of a_i in groups of k terms. Note the order is important and that we can repeat the choices for different a_i, then we have a variation with repetition, namely, p^k choices.

2. If not all coefficientes of the summands are multiple of p, we have p^{k-1} choices.

Moreover, the solutions of second equation depends on the solutions of the first equation because if some $b_i = 0 \rightarrow a_i = 0$. So, we study the number of solutions of the system by the quantity of terms different to zero in the second equation.

In the first case, we have one $b_i \neq 0$. Note that $\nu(6, 1) = 4$ such that $\nu(6, 1, 5) = 0$ and $\nu'(6, 1, 5) = 4 - 0 = 4$. So, for $k = 1$ we have $\nu(6, 1, 5) \cdot 5^1 + \nu'(6, 1, 5) \cdot 5^{1-1} = 4$. We can see all solutions in Table 2.7.

In the second case, we have two $b_i \neq 0$. Note that $\nu(6, 2) = 6$ such that $\nu(6, 2, 5) = 0$ and $\nu'(6, 2, 5) = 6 - 0 = 6$. So, for $k = 2$ we have $\nu(6, 2, 5) \cdot 5^2 + \nu'(6, 2, 5) \cdot 5^{2-1} = 30$. As we can see all solutions in Table 2.9.

In the third case, we have three $b_i \neq 0$. Note that $\nu(6,3) = 1$ such that $\nu(6,3,5) = 0$ and $\nu'(6,3,5) = 1 - 0 = 1$. So, for $k = 3$ we have $\nu(6,3,5) \cdot 5^3 + \nu'(6,3,5) \cdot 5^{3-1} = 25$. As we can see all solutions in Table 2.8.

There are not more cases because we can not make the number six with four or more summands. Then $fe_R(X \simeq R^6) = 4 + 30 + 25 = 59$.

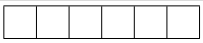
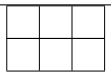
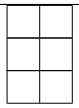
Sol. b_i	Partition	Young diagram	Eq. in a_i	Sol. a_i	Number of solutions a_i
$b_1 = 6$	6=6		$0=a_1$	$a_1 = 0$	$5^{1-1} = 1$
$b_2 = 3$	6= 3+3		$0= 2a_2$	$a_2 = 3$	$5^{1-1} = 1$
$b_3 = 2$	6=2+2+2		$0=3a_3$	$a_3 = 2$	$5^{1-1} = 1$
$b_6 = 1$	6= 1+1+1+1+1+1		$0 = 6a_6 \rightarrow 0 = a_6$	$a_6 = 0$	$5^{1-1} = 1$

Table 2.7: *Example 2: Solutions with one $b_i \neq 0$*

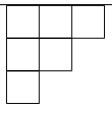
Sol. b_i	Partition	Young diagram	Eq. in a_i	Number of solutions a_i
$b_1 = 1$ $b_2 = 1$ $b_3 = 1$	6=3+2+1		$0 = a_1 + 2a_2 + 3a_3$	$5^{3-1} = 25$

Table 2.8: *Example 2: Solutions with three $b_i \neq 0$*

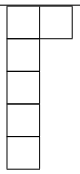
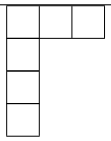
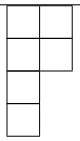
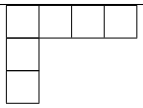
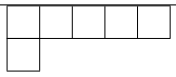
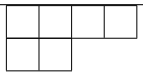
Sol. b_i	Partition	Young diagram	Eq. in a_i	Sol. a_i	Number of solutions a_i
$b_1 = 1$ $b_5 = 1$	6=2+1+1+1+1		$0=a_1 + 5a_5$	(0,0), (0,1), (0,3) (0,4), (0,5)	$5^{2-1} = 5$
$b_1 = 2$ $b_4 = 1$	6= 3+1+1+1		$0= a_1 + 4a_4$	(0,0), (1,1), (2,2) (3,3), (4,4)	$5^{2-1} = 5$
$b_2 = 1$ $b_4 = 1$	6= 2+2+1+1		$0= 2a_2 + 4a_4$	(0,0) (3,1) (1,2) (4,3) (2,4)	$5^{2-1} = 5$
$b_1 = 3$ $b_3 = 1$	6= 4+1+1		$0= a_1 + 3a_3$	(0,0), (1,4), (2,1) (3,4), (4,2)	$5^{2-1} = 5$
$b_1 = 4$ $b_2 = 1$	6= 5+1		$0= a_1 + 2a_2$	(0,0), (1,2), (2,4) (3,1), (4,3)	$5^{2-1} = 5$
$b_1 = 2$ $b_2 = 2$	6= 4+2		$0= a_1 + 2a_2$	(0,0), (1,2), (2,4) (3,1), (4,3)	$5^{2-1} = 5$

Table 2.9: *Example 2: Solutions with two* $b_i \neq 0$

Part II

Convolutional codes.

Coding theory is introduced to develop digital communications. Convolutional codes were introduced by Peter Elias in 1955 in [23] where a polynomial matrix $G(z)$ is used in the encoding procedure allowing to generate the code online without using a previous buffering. The first algebraic-theoric approach of convolutional codes was given by Forney in [25] where the relation between the $n \times k$ matrices over the field of rational functions over a field and the convolutional codes was shown. It was also explained that the term *convolutional* is used because the output sequences can be regarded as the convolution of the input sequence with the sequences in the encoder, [28].

Many properties of a convolutional code are studied by its parameters (rate, constraint length and complexity). In this sense, research in convolutional codes theory is often focused on constructing convolutional codes of a given rate and complexity with good free distance (Hamming distance). With this goal, convolutional codes are related with algebra, combinatorics or algebraic geometry, among others. Main relations between convolutional codes over finite fields and systems theory were given in [70], [71] and [83], where they proposed an algebraic decoding algorithm based on an input/state/output description of the code. More recently other authors have studied convolutional codes by using control theory and focusing on controllability/ observability problems (see [26], [27], [28],[29], [42], [59], [60] and [61]).

Other advances in coding theory are related with multidimensional codes and the tools of cotrollability are used in this field (see [31], [34], [45] and [84]).

However sometimes working over finite fields is too restrictive. This is the main motivation to study convolutional codes over rings. The first approach to convolutional codes over rings came by Massey and Mittelholzer in [53] and [54]. Extending convolutional codes to rings brings new difficulties, but gives some desirable behaviours. We give along Chapter 3 the main results about this topic.

In this part we base ourselves on the results of [19] over block codes In order to generalize the relation between convolutional codes and systems over commutative rings and we will answer the following questions:

1. Can we define a family of convolutional codes over R where R is a commutative ring

with identity?

2. Given a family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ where $\mathbb{F}_j$ is a finite field for $j = 1, \ldots, t$, are there triple of matrices (K, L, M) over R that we can consider a first order representation of the convolutional code ?

3. Moreover, are there matrices A, B, C and D that let us obtain a representation of controllability state spaces of the family of convolutional codes?

4. What are the properties of these families of convolutional codes and their first order and I/S/O representations?

This part is organized as follows: In Chapter 3 we give a review of elementary definitions and properties of convolutional codes over finite fields and over rings. Moreover, we focus on some sections on first order and I/S/O representations of convolutional codes. The answers to each of the above questions are given in Chapter 4.

Chapter 3

Convolutional Codes and linear systems. A survey.

The chapter is organized as follows: Preliminaries of convolutional codes over finite fields are given in Section 1. In Section 2, we review some results about first order representations of a convolutional code over a finite field. In Section 3 we recall the construction and properties of I/S/O representation of a convolutional code. Convolutional codes over rings are studied in Section 4 where we give main definitions and properties.

3.1. Preliminaries of convolutional codes over finite fields.

There is a considerable amount of literature on the theory of convolutional codes over finite fields, see [32], [35], [65], [66], [69] or [77], for example. In [67] we find an overview of the different approaches to the subject of convolutional code. In this work we use the definition of convolutional code as submodule of $\mathbb{F}[z]^n$ being interesting from associated first order and I/S/O representations following to [70], [71] and [83].

Definition 3.1.1 (c.f. Definition D', [67]). *A rate (n, k) convolutional code over a finite field $\mathbb{F}_q$ is a finitely generated $\mathbb{F}_q[z]^n$-submodule of rank k, $\mathcal{C} \subseteq \mathbb{F}_q^n[z]$.*

Finite field of $q = p^r$ elements, $\mathbb{F}_q$, is the field of the input alphabet channel. In the sequel we denote $\mathbb{F}_q \equiv \mathbb{F}$.

Note that since all $\mathbb{F}[z]$-module is a $\mathbb{F}$- vector space hence $\mathcal{C}$ is always a flat $\mathbb{F}$-submodule. Therefore there exist a flat quotient $\mathbb{F}[z]^n/\mathcal{C}$ over $\mathbb{F}$.

A convolutional code is presented by a matrix whose columns collect a set of generators of $\mathcal{C}$. Different approaches to generator matrix (polynomial matrix, scalar matrix and state space diagram) can be found in Appendix D. Now we give a review of fundamental definitions over generator matrices of convolutional codes.

Definition 3.1.2. *A generator matrix from a (n, k) convolutional code $\mathcal{C}$ over $\mathbb{F}$ is a matrix*

$$\begin{aligned} G(z) :&\mathbb{F}[z]^l \to \mathbb{F}[z]^n \\ &u(z) \mapsto v(z) = G(z)u(z) \end{aligned}$$

such that $Im\ G(z) = \mathcal{C}$.

Note that $\mathbb{F}[z]$ is a principal ideal domain and then a convolutional code $\mathcal{C}$ has a well-defined rank k and there exists a full-rank matrix $G(z)$ (of rank k) such that $\mathcal{C} = colsp_{\mathbb{F}[z]}G(z)$.

Definition 3.1.3 (cf. Definition 3.1.4, 3.1.5.,[83])**.** *An encoder to $\mathcal{C}$ is a matrix*

$$\begin{aligned} G(z) :&\mathbb{F}[z]^k \to \mathbb{F}[z]^n \\ &u(z) \mapsto v(z) = G(z)u(z) \end{aligned}$$

such that $Im\ G(z) = \mathcal{C}$ and $G(z)$ is injective: If we assume that $G(z)$ is an $n \times k$ matrix with entries in $\mathbb{F}[z]$, then $\mathcal{C} = \{v(z) \in \mathbb{F}^n[z] \mid \exists u(z) \in \mathbb{F}^k[z] \mid v(z) = G(z)u(z)\}$ defines a submodule of $\mathbb{F}^n[z]$. Namely, $\mathcal{C} = Im(G) \subseteq \mathbb{F}[z]^n$. Note that $Im(G)$ is a finitely generated sumodule.

The above definition implies that a $n \times k$ polynomial matrix is an encoder of $\mathcal{C}$ if its columns form a basis of the free module $\mathcal{C}$. In particular, an encoder is a generator matrix which $l = k$ and $G(z)$ is injective.

Moreover, there exists another parameter related with the convolutional codes and their generator matrices; that is, the complexity of both objects. The relation between these complexities is the key of the definition of a minimal encoder.

Definition 3.1.4. *Let $G \in \mathcal{M}_{n\times k}(\mathbb{F}[z]^k)$ be an encoder matrix of a convolutional code. The Forney's indices ν_i of $G(z)$ are the indices of columns $\nu_1, \nu_2, \ldots, \nu_k$ given by $\nu_i = max\{deg(g_{ij}) \mid 1 \leq i \leq n \text{ and } j = 1 \ldots, k\}$. We can assume that $\nu_1 \geq \nu_2 \geq ... \geq \nu_k$ up to reordenation.*

The memory of an encoder is ν_1 (a convolutional code with $\nu_1 = 0$ is a block code) and the complexity of the encoder is given by $c = \sum_{i=0}^{k} \nu_i$.

Definition 3.1.5 (cf. Definition 3.1.7.[83]). *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 $G(z)$.*

Definition 3.1.6 (cf. Definition 3.1.8, [83]). *Let $\mathcal{C} \subset \mathbb{F}[z]^n$ be a (n,k)-convolutional code. An encoder matrix $G(z)$ of $\mathcal{C}$ is minimal if and only if complexity $[G(z)]$ = complexity $(\mathcal{C})$; i.e, $c = \delta(\mathcal{C})$*

Note that the we have three sets of matrices associated to a convolutional code: generator matrices, encoders and minimal encoders such that

$$\{ \text{ minimal}\} \subset \{ \text{ encoders } \} \subset \{ \text{ generator matrices } \}$$

Moreover we have the following results between minimal encoders:

Lemma 3.1.7 (cf. Lemma 3.1.6 and Lemma 3.1.9, [83]). *Let $G(z)$ be an $n \times k$ polynomial matrix of rank k defining a convolutional code $\mathcal{C} = colsp_{\mathbb{F}[z]}G(z)$. Let $\widehat{G}(z)$ be an $n \times k$ polynomial matrix of rank k over $\mathbb{F}[z]$. The following statements are verified:*

1. *$G(z)$ and $\widehat{G}(z)$ define the same behaviour if and only if there exists a $k \times k$ unimodular matrix $U(z)$ such that $\widehat{G}(z) = G(z)U(z)$*

2. *There exists an unimodular matrix $U(z)$ such that $\widehat{G}(z) = G(z)U(z)$ is column-reduced, namely, $\widehat{G}(z)$ is a minimal encoder.*

3. *If $G(z)$ and $\widehat{G}(z)$ are minimal encoders of $\mathcal{C}$ then they have the same column degrees.*

Definition 3.1.8 (cf. 3.1.9 , [83]). *The column degrees $(\kappa_1, ..., \kappa_k)$ of any minimal encoder $\widehat{G}(z)$ of $\mathcal{C}$ are known as the Kronecker or controllability indices of the code. We can reorder them if it is necessary such that $\kappa_1 \geq \ldots \geq \kappa_k$. The invariant $\delta = \sum_{i=1}^{k} \kappa_i$ is the degree of the code $\mathcal{C}$.*

Note that the Kronecker's indices of a convolutional code are unique and invariants of the code and if we consider a minimal encoder of a convolutional code then the Kronecker's indices and Forney's indices are equal. In this case, $\kappa_1 = \nu_1$ is the memory of the encoder.

In systems Theory literature, the degree of the code δ is called theMcMillan degree of the system. In some coding literature, δ is called the complexity of the code.

We review the definition of the parameters of the code (further study of this topic has been developed in Section 10.1 in [57]). Parameters that are associated to a convolutional code from point of view of its generator matrix $G(z)$ are:

1. The memory $M = max_{i,j}[deg(g_{ij})] = \nu_1$. In the case that work with minimal encoders the memory equals to κ_1.

2. The lenght of restriction $K = M + 1$.

3. The rate $\frac{k}{n}$.

Example 3.1.9. *$G(z) = [z^2+1, z^2+z+1]$ is generator matrix of a $(2,1)$ convolutional code because $n = 2$ is the column number and $k = 1$ is the row number. We have $M = 2, K = 3$ and rate $\frac{1}{2}$.*

We give some notions about observable convolutional codes that are useful in the following Chapter.

Definition 3.1.10 (cf. Definition 3.3.1.[83])**.** *Let $G(z)$ be an encoder of a (n,k) convolutional code $\mathcal{C}$ over $\mathbb{F}$. A syndrome former for the code $\mathcal{C}$ is a homomorphism of modules given by*

$$\psi : \mathbb{F}[z]^n \to \mathbb{F}[z]^{n-k}$$

with the property that $Im\ G(z) \subseteq Ker\ \psi$.

Definition 3.1.11 (cf. Lemma 3.3.2. [83])**.** *Let $G(z)$ be an encoder of a (n,k) convolutional code $\mathcal{C}$ over $\mathbb{F}$. The convolutional code $\mathcal{C}$ is observable if and only if there exits an encoder $G(z)$ and a syndrome Former ψ such that the following sequence is exact*

$$0 \to \mathbb{F}[z]^k \xrightarrow{G(z)} \mathbb{F}[z]^n \xrightarrow{\psi} \mathbb{F}[z]^{n-k} \to 0$$

Note that above definition implies that $\mathcal{C}$ is observable if and only if $\mathbb{F}[z]^n/\mathcal{C}$ is $\mathbb{F}[z]$-flat module.

3.2. First order representations of convolutional codes.

The bridge between linear systems theory and convolutional codes is given by a duality between codes and sets of I/S/O (input/state/output) representations that are controllability state space systems. In order to obtain the I/S/O of the code first we compute a minimal first order representation (see [47], [70], [71] and [83] for details).

Let us recall some preliminaries of above duality over finite fields $\mathbb{F}$.

Theorem 3.2.1 (c.f. Theorem 3.1, [71]). *Let $\mathcal{C} \subseteq \mathbb{F}^n[z]$ be a (n,k) convolutional code of degree δ. Then there exists matrices $K, L \in \mathcal{M}_{(\delta+n-k)\times\delta}(\mathbb{F})$ and $M \in \mathcal{M}_{(\delta+n-k)\times n}(\mathbb{F})$ such that the code is described by*

$$\mathcal{C} = \Big\{ v(z) \in \mathbb{F}^n[z] \mid \exists x(z) \in \mathbb{F}^\delta[z] : \ (zK+L)x(z) + Mv(z) = 0 \Big\} \tag{3.1}$$

Moreover, the matrices satisfy minimality conditions:

1. *K has column full size range.*
2. *$[K \ M]$ has row full size range.*
3. *$[zK+L|M]$ is left prime $\equiv rg(z_0K+L \mid M) = \delta+n-k \ \forall z_0 \in \overline{\mathbb{F}}$*

Note that the minimality condition 3) is actually equivalent to saying that the matrix

$$(zK+L \mid M) : \mathbb{F}[z]^{\delta+n} \to \mathbb{F}[z]^{\delta+n-k}$$

is surjective. See Theorem B.2.7 of Appendix B.

Since $G(z)$ could be assumed minimal encoder of $\mathcal{C}$ (see proof of Theorem 5.1.1 of [83]), Kronecker's indices and Forney's indices are equal (this is the reason because we are using δ instead of c). Moreover, the triple of matrices $(K \mid L \mid M)$ has full rank and we have the following lemma:

Lemma 3.2.2 (c.f. Lemma 3.2, [71]). *Suppose that a code $\mathcal{C}$ over $\mathbb{F}$ with generator matrix $G(z)$ of full column rank is represented as in (3.1) by a minimal triple $[K,L,M]$. Then for all $z_0 \in \widehat{F}$, $G(z_0)$ has full-column rank if and only if z_0K+L has full-column rank.*

Furthermore, minimal first order representations of a given convolutional code are unique up to change of basis.

Theorem 3.2.3 (cf. Theorem 3.4., [71]). *Matrices K, L and M are unique in the following way: if $(\widehat{K}, \widehat{L}, \widehat{M})$ satisfies the minimality conditions of Theorem 3.2.1 and there exist unique invertible matrices T and S such that*

$$(\widehat{K}, \widehat{L}, \widehat{M}) = (TKS^{-1}, TLS^{-1}, TM)$$

Therefore, if a code $\mathcal{C}$ is described by a representation (K, L, M) that satisfies minimality conditions of Theorem 3.2.1 then we can consider an encoder $G(z)$ computing a minimal basis of

$$Ker[zK + L|M] = \big\{v(z) \in \mathbb{F}^n[z] \mid \exists x(z) \in \mathbb{F}^\delta[z] : \ (zK + L)x(z) + Mv(z) = 0\big\}.$$

The procedure to get the first order representation is given in [71] and [83] and it is as follows: We assume that $G(z)$ is a minimal encoder of $\mathcal{C}$ with column indices $\nu_1 \geq \nu_2 \geq ... \geq \nu_k$ and complexity $\delta = \sum_{i=0}^{k} \nu_i$.

Let $X(z) = \text{diag}(X_1(z), ..., X_k(z))$ be a $\delta \times k$ matrix where $X_i(z) = [1 \ z ... \ z^{\nu_i - 1}]^t$ with $i = 1, ..., k$, also $X(z)$ is left prime and it has the property that for each polinomyal vector $f(z) = (f_1(z), ..., f_k(z)) \in \mathbb{F}^k[z]$ where $deg f_i(z) \leq \nu_i - 1$ there exists an unique vector $\upsilon \in \mathbb{F}^\delta[z]$ such that $\upsilon X(z) = f(z)$. From this property, the matrix $X(z)$ is called basis matrix in [61] and [68], where an algoritmic approach is given by inspection.

Let $f(z) \in \mathbb{F}^k[z]$ be the polynomial vector with $deg f_i(z) \leq \nu_i$. Then $[f(z)]$ denotes the scalar vector of $\delta + k$ components that we get from $f(z)$ identifying each $f_i(z)$ with the row vector of $1 \times (\nu_i + 1)$ components with the coefficientes of $f_i(z)$. Hence we can consider $f(z)$ as a polynomial vector over $\mathbb{F}^{\delta+k}[z]$. Let ϕ be the map

$$\begin{aligned} \phi : \mathbb{F}^{2\delta+n} &\to \mathbb{F}^{\delta+k} \\ \upsilon &\mapsto \upsilon \begin{bmatrix} zX(z) \\ X(z) \\ G(z) \end{bmatrix} \end{aligned}$$

Since $X(z)$ has maximun rank then there exist $(\delta + n - k)$ free linearly independent constant vectors in the left Kernel of $X(z)$; namely, there exists a matrix of maximun rank $(K|L|M)$ of size $(\delta + n - k) \times (2\delta + n)$ such that $zKX(z) + LX(z) + MG(z) = 0$. This matrix is a minimal first order representation of $G(z)$.

Moreover, because $(K \mid L \mid M)$ is a full rank matrix, it has $(\delta + n - k)$ independent linear rows and columns and so there exists a minor of size $(\delta + n - k)$ that is invertible.

If we apply the inverse of this minor to the matrix $(K \mid L \mid M)$ then $[zK + L \mid M]$ is equivalent to the following pencil

$$\begin{bmatrix} zI - A & 0 & -B \\ -C & I & -D \end{bmatrix}$$

and we get a triple of matrices $(\mathcal{K} \mid \mathcal{L} \mid \mathcal{M})$ such that

$$\mathcal{K} = \begin{pmatrix} -I_{\delta\times\delta} \\ O \end{pmatrix}, \mathcal{L} = \begin{pmatrix} A_{\delta\times\delta} \\ C_{(n-k)\times\delta} \end{pmatrix} \text{ and } \mathcal{M} = \begin{pmatrix} O & B_{\delta\times k} \\ -I_{(n-k)\times(n-k)} & D_{(n-k)\times k} \end{pmatrix} \quad (3.2)$$

and both triple of matrices define the same convolutional code; that is,

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

The matrices (K, L, M) and $(\mathcal{K}, \mathcal{L}, \mathcal{M})$ are minimal first order representations of $\mathcal{C}$.

3.3. I/S/O Representations of a convolutional code over a finite field.

The above matrices A, B, C and D associated to convolutional code $\mathcal{C}$ over $\mathbb{F}$ and obtained from (3.2) allow us to get a representation of state spaces (see [47] and [83]):

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

By (3.2) we get

$$z \begin{pmatrix} I \\ 0 \end{pmatrix} x(z) - \begin{pmatrix} A \\ C \end{pmatrix} x(z) - \begin{pmatrix} 0 & B \\ -I & D \end{pmatrix} v(z) = 0$$

Therefore

$$\mathcal{C} = \{v(z) \in \mathbb{F}[z]^n \mid \exists x(z) \in \mathbb{F}[z]^\delta \mid \begin{pmatrix} zI - A & 0 & -B \\ -C & I & -D \end{pmatrix} \begin{pmatrix} x(z) \\ v(z) \end{pmatrix} = 0\} \quad (3.3)$$

If we divide the vector $v(z)$ into two parts $v(z) = (y(z), u(z))^t$, hence the equality (3.3) can be expressed by

$$\left.\begin{aligned} zx(z) &= Ax(z) + Bu(z) \\ y(z) &= Cx(z) + Du(z) \end{aligned}\right\} \quad (3.4)$$

If we consider

$$\left.\begin{aligned} x(z) &= x_0 z^\gamma + x_1 z^{\gamma-1} + \ldots + x_\gamma \\ y(z) &= y_0 z^\gamma + y_1 z^{\gamma-1} + \ldots + y_\gamma \\ u(z) &= u_0 z^\gamma + u_1 z^{\gamma-1} + \ldots + u_\gamma \end{aligned}\right\}$$

and replace in (3.4) we get the system

$$\begin{cases} x_{t+1} = Ax_t + Bu_t \\ y_t = Cx_t + Du_t \\ v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix},\ x_0 = 0,\ \exists \gamma : x_{\gamma+1} = 0. \end{cases} \tag{3.5}$$

where x_t is the n-state vector, y_t the p-vector output and u_t the m-vector control. We also give an initial state $x_{t_0} = x_0$ in time t_0. A time-invariant system of this class is characterized by the set (A, B, C, D) and inputs and outputs of system are part of the codeword.

Example 3.3.1. *Let $G_1(z)$ be an encoder over $\mathbb{Z}/2\mathbb{Z}$*

$$G_1(z) = \begin{pmatrix} z-1 & 1 \\ z^2+1 & 0 \\ z^2+1 & z+1 \end{pmatrix}.$$

Then, k = number of columns of $G_1(z) = 2$, n= number of rows of $G_1(z) = 3$, $\nu := [\nu_1 = 2, \nu_2 = 1]$ and $c = \delta = 2 + 1 = 3$. Now we compute the matrix $X(z) = \mathrm{diag}(X_1(z), X_2(z))$ that it will be $c \times k = 3 \times 2$.

For $i = 1 \to \nu_1 = 2 \to \nu_1 - 1 = 1 \to X_1(z) = (1\ z)^t$.

For $i = 2 \to \nu_2 = 1 \to \nu_2 - 1 = 0 \to X_2(z) = (1)^t$.

So

$$X(z) = \begin{pmatrix} 1 & 0 \\ z & 0 \\ 0 & 1 \end{pmatrix}.$$

In this case, $\phi : \mathbb{F}^9 \to \mathbb{F}^5$, the matrix $(zX(z)^t, X(z)^t, G(z)^t)$ by we get scalar matrix E_1^ϕ is

$$\begin{pmatrix} z & z^2 & 0 & 1 & z & 0 & z-1 & z^2+1 & z^2+1 \\ 0 & 0 & z & 0 & 0 & 1 & 1 & 0 & z+1 \end{pmatrix}$$

So, associated scalar matrix to ϕ is

$$E_1^{\phi} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We compute the $Ker(\phi)$ *and deduce* K_1, L_1 *and* M_1*, namely,*

$$Ker(\phi) = \{\overrightarrow{x} = (x_1, x_2, \ldots, x_9) \text{ such that } E_1^{\phi} \cdot \overrightarrow{x} = \overrightarrow{0}\} =$$

$$= \{x_1 = \beta + \alpha,\ x_2 = \mu + \lambda,\ x_3 = \lambda,\ x_4 = \mu + \alpha + \lambda,\ x_5 = \beta,\ x_6 = \lambda + \alpha,\ x_7 = \alpha,\ x_8 = \mu \text{ and } x_9 = \lambda\}$$

Then

$$(K_1|L_1|M_1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

From the above matrix we obtain $K_1, L_1 \in \mathcal{M}_{4\times 3}(\mathbb{Z}/2\mathbb{Z})$ *and* $M_1 \in \mathcal{M}_{4\times 3}(\mathbb{Z}/2\mathbb{Z})$*. Moreover, we can compute the matrices* $A_1 \in \mathcal{M}_{3\times 3}(\mathbb{Z}/2\mathbb{Z})$*,* $B_1 \in \mathcal{M}_{3\times 2}(\mathbb{Z}/2\mathbb{Z})$*,* $C_1 \in \mathcal{M}_{1\times 3}(\mathbb{Z}/2\mathbb{Z})$ *and* $D_1 \in \mathcal{M}_{1\times 2}(\mathbb{Z}/2\mathbb{Z})$*.*

$$A_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ B_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix},\ C_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},\ D_1 = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

3.3.1. Reachability of I/S/O representations.

We review the conditions about reachability (controllability from the origin) over the I/S/O representation of a convolutional code $\mathcal{C}$ over $\mathbb{F}$ that are given in [83] and implying that (A, B) is a reachable pair. First, we recall some results.

Definition 3.3.2. *Let* (A, B, C, D) *be scalar matrices over* $\mathbb{F}$ *as described in (3.2) and (3.5). The controllability (reachability) matrix was defined by*

$$\Phi_{\delta}(A, B) = \begin{pmatrix} B & AB & \ldots & A^{\delta-2}B & A^{\delta-1}B \end{pmatrix} \tag{3.6}$$

By Theorem 1.2.7, a linear system $\Sigma = (A, B)$ over a field $\mathbb{F}$ is reachable if its controllability matrix has maximun rank; that is, $rank\ \Phi_\delta(A, B) = \delta$. Moreover, the following reachability test is verified:

Lemma 3.3.3 (c.f. Hautus test, [37])**.**

$$rank\ \Phi_\delta(A, B) = \delta \text{ if and only if } rank\ (z_0 I + A \mid B) = \delta, \forall z_0 \in \overline{\mathbb{F}}$$

Remark 3.3.4 (cf. Lemma 5.3.5. [83])**.** *Note that the minimality condition iii) of Theoren 3.2.1 is equivalent to, by Hautus Test, the reachability (controllability from the origin) of the pair (A, B); namely, the condition of that (A, B) forms a reachable pair is translated to the controllability of the code $\mathcal{C}$ and so, an I/S/O representation of a convolutional code $\mathcal{C}$ is a reachable (controllable from the origin) dynamical linear system over $\mathbb{F}$: The equation (3.5) describes the dynamics of the following encoder*

$$G(z)U^{-1}(z) = \begin{bmatrix} Y(z)U(z)^{-1} \\ I_k \end{bmatrix}.$$

and then $u(z)$ must be in the column module of $U(z)$ in order that $y(z)$ and $x(z)$ have finite support. In terms of systems theory, it means that the state should start at zero and return to zero in finite time.

3.4. Construction of observable convolutional codes by I/S/O representations.

Duality between convolutional codes and reachable state space representations is useful to construct observable convolutional codes: an I/S/O representation is always a reachable dynamical linear system . If it is also observable, then the following results allow us to get an associated observable convolutional code.

First we review the result by which we relate minimal first order representations and observable convolutional codes by properties of the pencil $(zK + L)$.

Corollary 3.4.1 (c.f. Corollary 3.3., [71])**.** *A code $\mathcal{C}$ over $\mathbb{F}$ represented by the minimal triple (K, L, M) is observable if and only if the pencil $(zK + L)$ is right prime when considered as a matrix over $\mathbb{F}[z, z^{-1}]$*

Let $\Sigma = (A, B, C, D)$ be scalar matrices over $\mathbb{F}$ as described in (3.2) and (3.5). The observability matrix was defined by

$$\Omega_\delta(A, C) = \begin{pmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{\delta-1} \end{pmatrix} \tag{3.7}$$

Lemma 3.4.2 (c.f Lemma 5.3.2., [83]). *The system Σ is observable if and only rank $\Omega_\delta(A, C) = \delta$ or, by Hautus Test, equivalently $\forall\ z_0 \in \overline{\mathbb{F}}$,*

$$rank \begin{pmatrix} z_0 I + A \\ C \end{pmatrix} = \delta$$

Since all I/S/O representation of a (n, k) convolutional code $\mathcal{C}$ over $\mathbb{F}$ verifies that

$$rank\ \Omega_\delta(A, C) = rank\ \Omega_{\delta+1}(A, C) \leq \delta \ and \ \ rank\ \Phi_\delta(A, B) = rank\ \Phi_{\delta+1}(A, B) \leq \delta$$

(see Lemma 5.3.2., [83]), the following lemma allow us to we use a reachable and observable system $\Sigma = (A, B, C, D)$ to construct an observable convolutional code.

Lemma 3.4.3 (c.f. Lemma 5.3.5, [83]). *Let (A, B, C, D) be matrices such that verify (3.2) and (3.5) and suppose that rank $\Omega_\delta(A, C) = \delta$ and rank $\Phi_\delta(A, B) = \delta$. Then the triple $(\mathcal{K}, \mathcal{L}, \mathcal{M})$ defined by the matrices (A, B, C, D) and 3.2 satisfies the minimality conditions of Theorem 3.2.1. Moreover, the convolutional code $\mathcal{C}$ defined in this way is observable.*

3.5. Preliminaries over convolutional codes over rings.

The first approach to convolutional codes over rings was given by Massey and Mittelholzer in [53] and [54] where they extended the concept of convolutional code from fields to rings and more specifically to the ring $\mathbb{Z}/l\mathbb{Z}$. They also focused on the study of minimal and systematic encoders over rings showing that not all convolutional code over $\mathbb{Z}/l\mathbb{Z}$ admits a systematic or a minimal encoder.

From this point on there exists a considerable body of literature of convolutional codes over rings. In [24] and [43] the generator matrix and its properties have been studied for the case of convolutional codes over finite rings, finite groups and noetherian rings. Moreover,

in [48] and [49], properties and a trellis representation with a minimum number of states is developed over the finite ring case $G = \mathbb{Z}/p^r\mathbb{Z}$ where r is a positive integer and p is prime.

Notation. *Although the usual notation for convolutional codes over rings deals with submodules of $R(D)^n$ we use the indeterminated z instead of D in order to hold the notation of convolutional codes over finite fields and avoid mystakes. Therefore we denote the encoders by $G(z)$ instead of $G(D)$.*

In [53], Massey and Mittelholzer defined an (n, k) R-ary convolutional code $\mathcal{C}$ as a free submodule of $R(z)^n$ of rank k. The causal subcode $\mathcal{C}_c$ of $\mathcal{C}$ is the submodule of $\mathcal{C}$ consisting of all codewords having only causal components. The start module $\mathcal{C}_0$ of $\mathcal{C}$ is the R-module consisting of all R-ary n-tuples $[\alpha_1(0), \alpha_2(0), ..., \alpha_n(0)]$ for which $[\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)]$ is a codeword in the causal subcode $\mathcal{C}_c$. Further study of this topic has been developed in Section II of [54] where they gave the following properties:

Definition 3.5.1 (c.f. Section II, [54]). *A convolutional code $\mathcal{C} \subset R(z)^n$ is quasi-proper if $\mathcal{C}_0$ is a free submodule of R^n of rank k.*

Definition 3.5.2 (c.f. Section II, [54]). *A convolutional code $\mathcal{C} \subset R(z)^n$ is proper if one can select k components so that the n-tuples in $\mathcal{C}_0$ when restricted to these components form the free module R^k.*

Moreover, a definition and properties of generator matrix of a convolutional code over R were given.

Definition 3.5.3 (c.f. Section II, [54]). *A generator matrix $G(z)$ of $\mathcal{C}$ over R is any $n \times k$ matrix whose columns are a basis for $\mathcal{C}$.*

We have some properties about the generator matrix and the encoders of a convolutional code over R as submodule of $R(z)^n$.

Definition 3.5.4 (c.f. Section II, [54]). *An encoding matrix $G(z)$ of a convolutional code $\mathcal{C}$ over a ring is a generator matrix whose all entries are realizable.*

Definition 3.5.5 (c.f. Section II, [54]). *An encoding matrix $G(z)$ of a convolutional code $\mathcal{C}$ over a ring is systematic if each column of the identity matrix I_k is also a column of $G(z)$. The convolutional code $\mathcal{C} \subset R(z)^n$ is systematic if it has a systematic encoder matrix $G(z)$.*

Remark 3.5.6. *Note that above definition is equivalent to define an encoding matrix $G(z)$ as systematic if there exists a submatrix T of $G(z)$ such that $det(T) \in Units(R(z))$.*

Proposition 3.5.7 (c.f. Propositon 1,[54])**.** *A convolutional code is systematic if and only if it is proper.*

Remark 3.5.8 (c.f. Section II, [54])**.** *Let $\mathcal{C} \subset R(z)^n$ be a convolutional code.*

1. *If the ring R is a finite field, then every (n,k) convolutional code over R is proper. In particular, every (n,k) convolutional code $\mathcal{C}$ over $R = \mathbb{Z}/p\mathbb{Z}$, where p is a prime, is proper.*

2. *If $\mathcal{C}$ is over $\mathbb{Z}/l\mathbb{Z}$ where l is the product of two or more distinct primes, then an (n,k) convolutional code over $\mathbb{Z}/l\mathbb{Z}$ is thus isomorphic to a direct product of (n,k) convolutional codes over the corresponding fields $\mathbb{Z}/p\mathbb{Z}$.In this case, every (n,k) convolutional code over $\mathbb{Z}/l\mathbb{Z}$ is quasi-proper.*

3. *When $l = p^e$ where p is a prime and $e > 1$, then a quasi-proper (n,k) convolutional code over $R = \mathbb{Z}/l\mathbb{Z}$ is also proper.*

Another main contribution to convolutional code over rings was given by Johannesson, Wan and Wittenmark in [43]. The authors developed a more complete and systematic theory of convolutional codes over rings. They introduced the concepts of right invertible, noncatastrophic and basic encoders and analyzed the algebraic structure of these classes of matrices.

Definition 3.5.9 (c.f. Section II, [43])**.** *Let $R[z]$ be the polynomial ring over R. The trailling coefficient of a nonzero polynomial is the coefficient of the smallest power of z with a non zero coefficient.*

Let $R(z)$ be the following set

$$R(z) = \left\{ \begin{array}{c} \dfrac{f(z)}{q(z)} \text{ such that } f(z), q(z) \in R[z] \text{and the trailling} \\ \text{coefficient of } q(z) \text{ is a unit in } R \end{array} \right\}$$

modulo the equivalence relation

$$\frac{f(z)}{q(z)} \sim \frac{f'(z)}{q'(z)} \Leftrightarrow f(z)q'(z) = f'(z)q(z)$$

Note that $R(z) = S^{-1}R[z]$ being S the multiplicative system given by those polynomials with trailling coefficient equals an unit in R.

Definition 3.5.10 (c.f Definition 1, [43]). *Let $k < n$ be integers. A rate (n, k) convolutional transducer over the ring of rational functions $R(z)$ is an injective morphism of $R(z)$-modules*

$$R^k(z) \xrightarrow{\phi} R^n(z)$$

$$u(z) \mapsto v(z) = G(z) \cdot u(z)$$

where $G(z)$ is a $n \times k$ matrix with entries in $R(z)$ whose columns are linear independent over $R(z)$, namely, a matrix with entries in $R(z)$ whose columns are free over $R(z)$. This matrix is called the transfer function matrix.

Convolutional code over R is described as follows:

Definition 3.5.11 (Definition 2, c.f.[43]). *A rate (n, k) convolutional code over R is the image of a rate (n, k) convolutional transducer for $R(z)$.*

It follows inmediately from above definition that a rate (n, k) convolutional code over R with transfer function matrix $G(z)$ can be considered as the $R(z)$-column module of $G(z)$.

We recall some properties given in [43].

Definition 3.5.12 (c.f. Definition 4., [43]). *We say that two generator matrices are equivalent if they generate the same convolutional code.*

Theorem 3.5.13 (c.f. Theorem 1, [43]). *Let R be a noetherian ring and let $G(z) \in R(z)^{l\times q}$ and $G'(z) \in R(z)^{l'\times q}$ be generator matrices of convolutional codes over R. Then $G(z)$ and $G'(z)$ are equivalent generator matrices if and only if $l = l'$ and there exists an invertible matrix $T(z) \in R(z)^{l\times l}$ such that $G(z) = T(z)G'(z)$.*

Definition 3.5.14 (cf. Theorem 6, [43]). *A realizable generator matrix $G(z) \in R(z)^{l\times q}$ is said to be systematic if $I_{l\times l}$ is a submatrix of $G(z)$. A convolutional generator matrix is said to be systematic if it causes the information symbols to appear unchanged among the code symbols, i.e. if some of its columns form the indentity matrix. Here a symbol means an element of R.*

Finally, in [24], Fagnani and Zampieri presented a quite complete theory of convolutional codes over the ring $\mathbb{Z}/p^r\mathbb{Z}$ in the usual case where the input sequence space is a free module. In particular, some basic concepts about convolutional codes over $\mathbb{Z}/p^r\mathbb{Z}$ and their structural properties such as basicity, systematicity, non-catastrophicity and minimality were presented. Moreover, they describe how to construct convolutional codes over rings from linear block codes.

We review the main properties that are useful in this work.

Definition 3.5.15 (cf. Section 3.1,[24]). *A convolutional code $\mathcal{C} \subset R(z)^n$ is right invertible if there exists an encoder $G(z)$ which has right inverse over $R(z)$.*

Lemma 3.5.16 (cf. [24]). *$\mathcal{C}$ is systematic $\Leftrightarrow$ $\mathcal{C}$ is right invertible.*

Proof. It follows from Remark 3.5.6 and Definition 3.5.15, □

Definition 3.5.17 (cf. Section 3.1.[24]). *A polynomial generator matrix $G(z) \in R[z]^{l\times q}$ is said to be basic if there exists polynomial matrix $X(z) \in R[z]^{q\times l}$ such that $G(z)X(z) = I$ where I is the identity matrix of suitable dimension. Namely, a generator matrix $G(z)$ of a convolutional code $\mathcal{C} \subset R(z)^n$ is basic if is polynomial and has polynomial right inverse.*

Chapter 4

Families of convolutional codes over regular rings.

This chapter is organized as follows: In Section 1 we define a convolutional code over a commutative ring with identity R; that is, a family of convolutional codes that we denote by $\mathfrak{C}$. From this point we restrict us to the rings that decompose into a finite product of finite fields. An example of this class of rings is the ring of modular intergers $\mathbb{Z}/l\mathbb{Z}$ where $l = p_1 \dots p_t$ is square free. In Section 2, the properties of the family of convolutional codes are given. In Section 3 we construct a first order representations of $\mathfrak{C}$. In Section 4 we obtained a I/S/O description of the family of codes and we study some properties that we use to construct observable family of convolutional codes and that are useful in part III of this work. Along the chapter, R is a commutative ring with identity.

4.1. Family of convolutional codes.

First we give some aclarations of notation to avoid mystakes.

Notation. *1. We denote by $S = Spec(R)$, $\mathbb{A}^1_S = Spec(R[z])$ and $e : R \hookrightarrow R[z]$ the canonical inclusion. We also will use the notation e for the induced morphism between spectra, $e : \mathbb{A}^1_S \to S$.*

2. For any prime ideal $\mathfrak{p} \in R$ we denote $k(\mathfrak{p}) = R/\mathfrak{p}R$ the residue field.

3. Let M be a finitely generated $R[z]$-module. Let $\mathfrak{p}$ be a prime ideal of R. We denote $M(\mathfrak{p})$ the $k(\mathfrak{p})[z]$-module $M/(\mathfrak{p}M)$.

Definition 4.1.1. *A rate (n,k) convolutional code over R is a submodule $\mathfrak{C}_R \subset R[z]^n$ such that $R[z]^n/\mathfrak{C}_R$ is R-flat and $rk(\mathcal{C})(\mathfrak{p}) = k$ for any prime ideal.*

Note that the flatness condition ensures that for any prime ideal $\mathfrak{p} \subset R$ the $k(\mathfrak{p})[z]$-module $\mathcal{C}(\mathfrak{p})$ is still a submodule $\mathcal{C}(\mathfrak{p}) \subset k(\mathfrak{p})[z]^n$ and therefore a rate (n,k) convolutional code in the classical way. This point of view allows us to interpret a convolutional code over R as a family of convolutional codes one over each point $\mathfrak{p} \in S$.

Definition 4.1.2. *Let $\mathcal{C}(\mathfrak{p})$ be a convolutional code over $k(\mathfrak{p})[z]^n$ where $\mathfrak{p}$ is a prime ideal of R. We consider the degree of the convolutional code $\delta(\mathcal{C}(\mathfrak{p})) = \delta(\mathfrak{p})$. We say that $\mathfrak{C}_R$ has degree δ if $\delta(\mathfrak{p}) = \delta$ for all $\mathfrak{p}$.*

We will work in the sequel with families $\mathfrak{C}_R$ with degree $\delta(\mathfrak{C}_R) = \delta$.

Definition 4.1.3. *Generator matrix $G(z)$ of a (n,k) family of convolutional codes $\mathfrak{C}_R$ over R is given by a matrix where associated map*

$$G(z) : R[z]^l \longrightarrow R[z]^n$$

$$u(z) \mapsto v(z) = G(z) \cdot u(z)$$

verifies that $Im\ G(z) = \mathfrak{C}_R$.

Definition 4.1.4. *An encoder $G(z)$ of a (n,k) family of convolutional codes $\mathfrak{C}_R$ over R is a generator matrix with $l = k$ and $G(z)$ injective.*

From this point on we consider the ring $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ where $\mathbb{F}_j$ is a finite field for each $j = 1, \ldots, t$. Note that all results that are verified over finite product of fields hold over finite product over finite fields and so results of Appendix B could be applied.

Notation. *Since we fix the ring R along the sequel, we denote by $\mathfrak{C} \equiv \mathfrak{C}_R$ to simplify the notation.*

Note that a convolutional code $\mathfrak{C}$ over the ring $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ gives rise a family of convolutional codes over every residue field by means of $\{\mathfrak{C} \otimes_R R/\mathfrak{m}\}_{\mathfrak{m} \in max(R)}$. In the ring R the converse construction will be shown to be possible. That is given pointwise data $\mathcal{C}_\mathfrak{m}$ over $R/\mathfrak{m}\ \forall\ \mathfrak{m}$ there exist an (unique) convolutional code over R such that $\mathfrak{C} \otimes R/\mathfrak{m} = \mathcal{C}_\mathfrak{m}$.

Let $\mathfrak{C} \subset R[z]^n$ be a family of convolutional codes and let us denote by $\mathcal{C}_j$ the restriction of $\mathfrak{C}$ over each $\mathbb{F}_j$, namely, $\mathcal{C}_j = \mathfrak{C} \otimes_{R[z]} \mathbb{F}_j[z]$. For each j, we have the surjection

$$\varphi_j : R[z]^n \to \mathbb{F}_j[z]^n$$

such that $\varphi_j(\mathfrak{C}) = \mathcal{C}_j$. Then every $\mathcal{C}_j$ can be considered as $R[z]$-module via φ_j and we have $\mathfrak{C} = \bigoplus_{j=1}^{t} \mathcal{C}_j$.

4.1.1. Properties of families of convolutional codes.

Definition 4.1.5. *Let $\mathfrak{C} \subset R[z]^n$ be a family of convolutional codes over R. We say that $\mathfrak{C}$ is observable if $R[z]^n/\mathfrak{C}$ is flat over $R[z]$.*

Let R be the ring $R[z] \simeq \mathbb{F}_1[z] \times ... \times \mathbb{F}_t[z]$ where $\mathbb{F}_j$ is a finite field for $j = 1, \ldots, t$.

Proposition 4.1.6. *$\mathfrak{C}$ is observable $\Leftrightarrow$ $\mathcal{C}_j$ is observable $\forall\ j$.*

Proof. $\Rightarrow$) Since $\mathfrak{C}$ is observable, $R[z]^n/\mathfrak{C}$ is a $R[z]$- flat module and then the following sequence is exact

$$0 \longrightarrow \mathfrak{C} \hookrightarrow R[z]^n \longrightarrow R[z]^n/\mathfrak{C} \longrightarrow 0$$

If we twist by $\otimes_{R[z]}\mathbb{F}_j[z]$, the following sequence remains exact because $\mathbb{F}_j[z]$ is a $R[z]$-flat module (see B.2.9)

$$0 \longrightarrow \mathfrak{C} \otimes_{R[z]} \mathbb{F}_j[z] \hookrightarrow R[z]^n \otimes_{R[z]} \mathbb{F}_j[z] \longrightarrow (R[z]^n/\mathfrak{C}) \otimes_{R[z]} \mathbb{F}_j[z] \longrightarrow 0$$

Namely, the following sequence is exact

$$0 \longrightarrow \mathcal{C}_j \hookrightarrow \mathbb{F}_j[z]^n \longrightarrow \mathbb{F}_j[z]^n/\mathcal{C}_j \longrightarrow 0$$

and $\mathbb{F}_j[z]^n/\mathcal{C}_j$ is a $\mathbb{F}_j[z]$- flat module for every j, hence $\mathcal{C}_j$ is observable for $j = 1, \ldots, t$.

$\Leftarrow$) If $\mathcal{C}_j$ is observable, then $\mathbb{F}_j[z]^n/\mathcal{C}$ is a $\mathbb{F}_j[z]$- flat module for $j, 1 \ldots, t$. We consider the following exact sequence

$$0 \longrightarrow \mathcal{C}_j \overset{i_j}{\hookrightarrow} \mathbb{F}_j[z]^n \overset{q_j}{\longrightarrow} \mathbb{F}_j[z]^n/\mathcal{C}_j \longrightarrow 0$$

Since we can consider above equation for every j, we have the following exact sequence

$$0 \longrightarrow \mathcal{C}_1 \times \ldots \times \mathcal{C}_t \overset{i}{\hookrightarrow} \mathbb{F}_1[z]^n \times \ldots \times \mathbb{F}_t[z]^n \overset{q}{\longrightarrow} \mathbb{F}_1[z]^n/\mathcal{C}_1 \times \ldots \times \mathbb{F}_t[z]^n/\mathcal{C}_t \longrightarrow 0 \quad (4.1)$$

Note that the associated matrix of i and q are the Bass matrices

$$i = \begin{pmatrix} i_1 & 0 & \ldots & 0 \\ 0 & i_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & i_t \end{pmatrix} \text{ and } j = \begin{pmatrix} j_1 & 0 & \ldots & 0 \\ 0 & j_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & j_t \end{pmatrix}$$

From sequence (4.1) we obtain that the following sequence

$$0 \longrightarrow \mathfrak{C} \hookrightarrow R[z]^n \longrightarrow R[z]^n/\mathfrak{C} \longrightarrow 0$$

is exact, hence $R[z]^n/\mathfrak{C}$ is a $R[z]$- flat module and so $\mathfrak{C}$ is observable. □

Note that properties of proper, systematic and basic convolutional codes described in Definitions 3.5.2, 3.5.6 and 3.5.17 remain for families of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Moreover, Proposition 3.5.7 that relates systematic and proper codes holds too.

4.2. First order representation of a family of convolutional codes over finite rings

Let $\mathfrak{C}$ be a family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ where $\mathbb{F}_j$ is a finite field for all $j = 1, \ldots, t$.. We review some well known results that we will apply:

Remark 4.2.1. *(c.f. Chap.I, §2. 3. Remarks, [4])*

1. *A R-module, E, is flat if and only if for all ideal $\mathfrak{p}$ of R, of finite type, the canonical map $E \otimes_R \mathfrak{p} \to E$,with image $E\mathfrak{p}$, is injective.*

2. *Let E be a flat R-module. Let M be a R-module. If M' is a submodule of M, the canonical injection $E \otimes_R M' \to E \otimes_R M$ let us to identify $E \otimes_R M'$ with a subgroup of $E \otimes_R M$. Let N be a R-module and let $u : M \to N$ be homomorphism and we denote by $K = Ker\ u$ and $I = Im\ u$. If we consider following exact sequence $0 \to K \to M \xrightarrow{u} N$, by prop. 1 of [4] then $E \otimes_R (Ker\ u)$ is identified with $Ker\ (1_E \otimes u)$.*

Furthermore, if we denote by u' the surjective homomorphism $M \to I$ that has the same graph that u since the canonical injection $I \to N$ hence $1_E \otimes u'$ is surjective (number 1, lemma 1 of [4]) and $1_E \otimes i$ is injective because E is flat. So, since $1_E \otimes u = (1_E \times i) \circ (1_E \otimes u')$, then $E \otimes_R (Imu)$ is identified with $Im(1_E \otimes u)$

Lemma 4.2.2. *Let $R[z] \simeq \mathbb{F}_1[z] \times \ldots \times \mathbb{F}_t[z]$ be a commutative ring with $1 \neq 0$. Let M, N be $R[z]-$modules and let $M_j \simeq M \otimes_{R[z]} \mathbb{F}_j[z]$ and $N_j \simeq N \otimes_{R[z]} \mathbb{F}_j[z]$ be submodules. If $M_j \simeq N_j\ \forall j = 1, \ldots, t$ then $M \simeq N$.*

Proof. The proof is given in the B.2.11 of Appendix B. □

We need to give a previous algebraic result in order to construct a minimal first order representation of a family of convolutional codes $\mathfrak{C}$ over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$.

Theorem 4.2.3. *Let (K, L, M) be a triple of matrices such that $K, L \in \mathcal{M}_{(\delta+n-k)\times\delta}(R)$ and $M \in \mathcal{M}_{(\delta+n-k)\times n}(R)$. We consider the kernel of the pencil $(zK + L \mid M)$ defined as follows*

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

then the following sequence is exact

$$0 \longrightarrow Ker(zK + L) \longrightarrow Ker(zK + L, M) \longrightarrow Ker(zK + L \mid M) \longrightarrow 0$$

Proof. Let $(zK + L)$ be the morphism

$$zK + L : R^\delta[z] \to Im(zK + L)$$

$$x(z) \mapsto (zK + L) \cdot x(z)$$

Then $Ker(zK + L) = \{x(z) \in R^\delta[z] \text{ tal que } (zK + L)x(z) = 0\}$ and we have the following exact sequence

$$0 \to Ker(zK + L) \to R^\delta[z] \to Im(zK + L) \to 0 \tag{4.2}$$

Let $(zK + L, M)$ be the morphism

$$\begin{aligned}(zK + L, M) :& R^\delta[z] \times R^n[z] \to R[z]^{\delta+n-k} \\ & (x(z), v(z)) \mapsto (zK + L) \cdot x(z) + M \cdot v(z)\end{aligned}$$

Then $Ker(zK + L, M) = \{(x(z), v(z)) \in R^\delta[z] \times R^n[z] \text{ such that } (zK + L) \cdot x(z) + M \cdot v(z) = 0\}$ and we have the following exact sequence

$$0 \to Ker(zK + L, M) \to R^\delta[z] \times R^n[z] \to Im(zK + L, M) \to 0 \tag{4.3}$$

Let π_2 be the projection morphism

$$\pi_2 : Ker(zK + L, M) \longrightarrow Ker(zK + L \mid M)$$

$$(x(z), v(z)) \mapsto v(z)$$

where $(x(z), v(z))$ are such that $(zK+L)x(z)+Mv(z) = 0$. Since $Ker\pi_2 \simeq Ker(zK+L)$ and π_2 is surjective, we have the following exact sequence

$$0 \longrightarrow Ker(zK+L) \longrightarrow Ker(zK+L, M) \xrightarrow{\pi_2} Ker(zK+L \mid M) \longrightarrow 0 \qquad (4.4)$$

$$x \longrightarrow (x, 0)$$

$$(u, v) \longrightarrow v$$

which concludes that $Ker(zK+L \mid M)$ is the Cokernel of above sequence (4.4). □

If $R = \mathbb{F}$ then $Ker(zK+L \mid M)$ corresponds to with a convolutional code $\mathcal{C}$ as submodule of $\mathbb{F}[z]^n$ by a first order representations in the sense of [83].

We are going to construct the first order representation of $\mathfrak{C}$:

Consider the family $\mathfrak{C} = \bigoplus_{j=1}^{t} \mathcal{C}_j$ over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ where $\mathbb{F}_j$ is a finite field. Then every $\mathcal{C}_j$ over $\mathbb{F}_j$ has a first order representation.

Let μ be the map $\mu : R \longrightarrow \mathbb{F}_j$. For the convenience of the reader we denote by $\mu_j(R) = R \otimes_R \mathbb{F}_j$ and in terms of matrices we denote by $\mu_j(A) = A \otimes 1 = A_j$ the restriction of A module $\mathbb{F}_j$.

The matrices (K, L, M) are constructed by μ_j in the way $\mu_j(K) \simeq K_j$, $\mu_j(L) \simeq L_j$ and $\mu_j(M) \simeq M_j$ where (K_j, L_j, M_j) are a first order representation of $\mathcal{C}_j \subseteq \mathbb{F}_j[z]^n$ for each $\mathbb{F}_j$.

We give our main result: The matrices (K, L, M) that we get from the above described ones is a First Order Representation of a family of convolutional codes $\mathfrak{C}$ over R.

Theorem 4.2.4. *Realization Theorem I: Existence. We suppose $\mathfrak{C} \subseteq R^n[z]$ is a family of convolutional codes with rate $\frac{k}{n}$ and complexity δ. Then, the matrices $K, L \in \mathcal{M}_{(\delta+n-k)\times\delta}(R)$ and $M \in \mathcal{M}_{(\delta+n-k)\times n}(R)$ satisfy that the code is described by $\mathcal{C} = Ker(zK+L \mid M)$.*

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 $(zK+L \mid M) : R[z]^{\delta+n} \to R[z]^{\delta+n-k}$ is surjective.*

Proof. First of all we prove that $Ker[zK+L|M]\otimes_{R[z]}\mathbb{F}_j[z]\simeq Ker[zK_j+L_j|M_j]$ for each $j=1,\dots t$.

Let (K,L,M) be matrices that are constructed from (K_j,L_j,M_j), first order representation of $\mathcal{C}_j\subseteq\mathbb{F}_j[z]^n$. We show that since $\mathcal{C}_j=Ker(zK_j+L_j\mid M_j)$, it follows that $\mathcal{C}=Ker(zK+L\mid M)$.

Now we apply Theorem 4.2.3 to first order representation of each convolutional code $\mathcal{C}_j$ over each field $\mathbb{F}_j$ and get the following exact sequence

$$0\to Ker(zK_j+L_j)\overset{i_2^j}{\hookrightarrow}Ker(zK_j+L_j,M_j)\overset{\pi_2^j}{\to}Ker(zK_j+L_j\mid M_j)\to 0 \tag{4.5}$$

where π_2^j is the following morphism

$$\pi_2^j: Ker(zK_j+L_j,M_j)\longrightarrow Ker(zK_j+L_j\mid M_j)$$

with $\pi_2^j(x_j(z),v_j(z))=v_j(z)$ and $(x_j(z),v_j(z))$ are such that $(zK_j+L_j)x_j(z)+M_jv_j(z)=0$

Moreover, if we apply Theorem 4.2.3 to pencil $(zK+L\mid M)$ over the commutative ring R we get the following exact sequence

$$0\to Ker(zK+L)\overset{i_2}{\to}Ker(zK+L,M)\overset{\pi_2}{\to}Ker(zK+L\mid M)\to 0 \tag{4.6}$$

We define the surjective projection morphism $\overline{\pi_2}$ where $\otimes\mathbb{F}_j[z]$ denotes $\otimes_{R[z]}\mathbb{F}_j[z]$

$$\overline{\pi_2}: Ker(zK+L,M)\otimes\mathbb{F}_j[z]\longrightarrow Ker(zK+L\mid M)\otimes\mathbb{F}_j[z]$$

where $\overline{\pi_2}(\overline{x(z)},\overline{v(z)})=\overline{v(z)}$ and $(\overline{x(z)},\overline{v(z)})$ are such that $(zK+L)\overline{x(z)}+M\overline{v(z)}=0$.

If we tensor the sequence (4.6) by $\otimes\mathbb{F}_j[z]$, since $\mathbb{F}_j[z]$ is flat, the following sequence is also exact

$$0\to Ker(zK+L)\otimes\mathbb{F}_j[z]\overset{\overline{i_2}}{\hookrightarrow}Ker(zK+L,M)\otimes\mathbb{F}_j[z]\overset{\overline{\pi_2}}{\to}Ker(zK+L\mid M)\otimes\mathbb{F}_j[z]\to 0 \tag{4.7}$$

Applying Remark 4.2.1 and Lemma B.2.9 then we conclude that

$$\left.\begin{aligned} Ker(zK+L)\otimes_{R[z]}\mathbb{F}_j[z]&\simeq Ker(zK_j+L_j)\\ Ker(zK+L,M)\otimes\mathbb{F}_j[z]&\simeq Ker(zK_j+L_j,M_j)\end{aligned}\right\} \tag{4.8}$$

Therefore we have the following morphisms

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Ker(zK+L)\otimes\mathbb{F}_j[z] & \xrightarrow{\overline{i_2}} & Ker(zK+L,M)\otimes\mathbb{F}_j[z] & \xrightarrow{\overline{\pi_2}} & Ker(zK+L\mid M)\otimes\mathbb{F}_j[z] & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\alpha} & & \vdots{\scriptstyle\sigma} & & \\
0 & \longrightarrow & Ker(zK_j+L_j) & \xrightarrow{i_2^j} & Ker((zK_j+L_j,M_j)\otimes 1) & \xrightarrow{\pi_2^j} & Ker(zK_j+L_j\mid M_j) & \longrightarrow & 0
\end{array} \tag{4.9}$$

By (4.8), ϕ and α are isomorphisms and then we can show that there exists a morphism σ such that

$$\sigma : Ker(zK + L \mid M) \otimes \mathbb{F}_j[z] \to Ker(zK_j + L_j \mid M_j)$$

Since $\overline{\pi_2}$ is surjective, for each $x \in Ker(zK + L \mid M) \otimes \mathbb{F}_j[z]$, then there exists an $y \in Ker((zK + L, M)) \otimes \mathbb{F}_j[z]$ such that $\overline{\pi_2}(y) = x$. Then we define $\sigma(x) = (\pi_2^j \circ \alpha)(y)$.

Because of α and ϕ commute and by the definition of σ, the result follows from application of Short-Five-Lemma on the above commutative diagram with exact rows and we conclude that σ is an isomorphism. Therefore by Lemma 4.2.2 we are done.

Finally, the matrices (K, L, M) satisfy minimality conditions. Conditions 1) and 2) follow from Proposition B.2.5 and condition 3) is obvious since tha matrix $(zK + L \mid M)$ represents a surjective mapping on each connected component $\mathbb{A}^1_{\mathbb{F}_j}$ of $Spec(R[z])$. □

Corollary 4.2.5. *If (K, L, M) is any first order representation of $\mathcal{C}$ then (K_j, L_j, M_j) is a first order representation for the code $\mathcal{C}_j$.*

Proof. It follows straighforward from the above Theorem. □

Theorem 4.2.6. *Realization Theorem II: Uniqueness*

Matrices K, L and M over R are unique in the following sense: if $(\widehat{K}, \widehat{L}, \widehat{M})$ satisfies the minimality conditions of Theorem 4.2.4, then there exist unique invertible matrices T and S over R such that

$$(\widehat{K}, \widehat{L}, \widehat{M}) = (TKS^{-1}, TLS^{-1}, TM)$$

Proof. Let (K, L, M) and $(\widehat{K}, \widehat{L}, \widehat{M})$ be first order representations of the family of convolutional codes $\mathfrak{C} \subset R^n[z]$. We consider its restrictions to $\mathbb{F}_j$, (K_j, L_j, M_j) and $(\widehat{K}_j, \widehat{L}_j, \widehat{M}_j)$ for each $j = 1, \ldots, t$. Then there exist invertible matrices S_j and T_j such that

$$(\widehat{K}_j, \widehat{L}_j, \widehat{M}_j) = (T_j K_j S_j^{-1}, T_j L_j S_j^{-1}, T_j M_j) \tag{4.10}$$

Since $Gl_r(R) \simeq GL_r(\mathbb{F}_1) \times \ldots \times GL_r(\mathbb{F}_t)$ there are unique invertible matrices over R, S and T, such that its restrictions to the field $\mathbb{F}_j$ are precisely S_j and T_j. Obviously $\widehat{K} = TKS^{-1}$, $\widehat{L} = TLS^{-1}$ and $\widehat{M} = TM$. □

4.3. Representation I/S/O of a family of convolutional codes over finite rings.

Let $\mathfrak{C}$ be a convolutional code over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ such that $\mathfrak{C} \simeq \bigoplus_{j=1}^{t} \mathcal{C}_j$ where $\mathcal{C}_j$ are convolutional codes over $\mathbb{F}_j$.

Let (K_j, L_j, M_j) be first order representations of convolutional codes $\mathcal{C}_j$ over each $\mathbb{F}_j$ for $j = 1, \ldots, t$. By [83] we can make elementary transformations over matrices (K_j, L_j, M_j) and get the triple of matrices $(\mathcal{K}_j, \mathcal{L}_j, \mathcal{M}_j)$ verifying

$$\mathcal{K}_j = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, \mathcal{L}_j = \begin{pmatrix} A_j \\ C_j \end{pmatrix} \text{ and } \mathcal{M}_j = \begin{pmatrix} O & B_j \\ -I_{(n-k)} & D_j \end{pmatrix} \tag{4.11}$$

where the matrices $A_j \in \mathcal{M}_{\delta\times\delta}(\mathbb{F}_j)$, $B_j \in \mathcal{M}_{\delta\times k}(\mathbb{F}_j)$, $C_j \in \mathcal{M}_{(n-k)\times\delta}(\mathbb{F}_j)$ and $D_j \in \mathcal{M}_{(n-k)\times k}(\mathbb{F}_j)$ verifies that (A_j, B_j, C_j, D_j) are I/S/O representations of each convolutional code $\mathcal{C}_j$.

Remark 4.3.1. *Both triples of matrices (K_j, L_j, M_j) and $(\mathcal{K}_j, \mathcal{L}_j, \mathcal{M}_j)$ are first order representations of the same code $\mathcal{C}_j$ for each j and then $Ker(zK_j + L_j \mid M_j) \simeq Ker(z\mathcal{K}_j + \mathcal{L}_j \mid \mathcal{M}_j)$ for all j.*

By patching we can construct over R the triple of matrices (K, L, M) from (K_j, L_j, M_j). This triple (K, L, M) is a first order representation of $\mathfrak{C}$ and from this set of matrices we can obtain an I/S/O representation of $\mathfrak{C}$.

Theorem 4.3.2. *Let $\mathfrak{C}$ be a convolutional code over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Let (K, L, M) be a first order representation of $\mathfrak{C}$. Then*

i) We can make elementary transformations over (K, L, M) and obtain $(\mathcal{K}, \mathcal{L}, \mathcal{M})$ such that

$$\mathcal{K} = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, \mathcal{L} = \begin{pmatrix} A \\ C \end{pmatrix} \text{ and } \mathcal{M} = \begin{pmatrix} O & B \\ -I_{(n-k)} & D \end{pmatrix} \tag{4.12}$$

where $A \in \mathcal{M}_{\delta\times\delta}(R)$, $B \in \mathcal{M}_{\delta\times k}(R)$, $C \in \mathcal{M}_{(n-k)\times\delta}(R)$ and $D \in \mathcal{M}_{(n-k)\times k}(R)$.

ii) Moreover, the triple of matrices obtained in i) verifies that

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

Proof. *i*) Since $(K_j \mid L_j \mid M_j)$ is a full rank matrix, $(K \mid L \mid M)$ has linearly independent rows and so, there exists a square minor W of size $(\delta+n-k)$ such that $det(W) \in R-\{0\}$. If we multiply $W^{-1}(K \mid L \mid M)$ and we reorder, if it neccessary, we get a triple of matrices $(\mathcal{K} \mid \mathcal{L} \mid \mathcal{M})$ in the following way

$$\mathcal{K} = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, \mathcal{L} = \begin{pmatrix} A_{\delta\times\delta} \\ C_{(n-k)\times\delta} \end{pmatrix} \text{ and } \mathcal{M} = \begin{pmatrix} O & B_{\delta\times k} \\ -I_{(n-k)} & D_{(n-k)\times k} \end{pmatrix}$$

ii) We start with the fact that

$$\left.\begin{array}{l} Ker(zK+L \mid M) \otimes_{R[z]} \mathbb{F}_j[z] \simeq Ker(zK_j+L_j \mid M_j) \\ Ker(z\mathcal{K}+\mathcal{L} \mid \mathcal{M}) \otimes_{R[z]} \mathbb{F}_j[z] \simeq Ker(z\mathcal{K}_j+\mathcal{L}_j \mid \mathcal{M}_j) \end{array}\right\}$$

By Lemma 4.2.2, since $Ker(zK_j+L_j \mid M_j) \simeq Ker(z\mathcal{K}_j+\mathcal{L}_j \mid \mathcal{M}_j)$ for all j ,we conclude the proof. □

The matrices A, B, C and D over R obtained from (4.12) are an I/S/O representation of $\mathfrak{C}$, the family of convolutional codes over R, that is, they define a representation of controllability state spaces linear system from

$$\mathfrak{C} = \{v(z) \in R[z]^n \mid \exists x(z) \in R[z]^\delta \textit{ such that } (zK+L)x(z)+Mv(z)=0\} \tag{4.13}$$

to

$$\left\{\begin{array}{l} x_{t+1} = Ax_t + Bu_t \\ y_t = Cx_t + Du_t \\ v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix},\ x_0 = 0,\ \exists\gamma : x_{\gamma+1} = 0. \end{array}\right. \tag{4.14}$$

where x_t is the n-state vector, y_t the p-vector output and u_t the m-vector control. We also give an initial state $x_{t_0} = x_0$ in time t_0.

Remark 4.3.3. *The procedure developed in Section 3.3 for fields also holds for* $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. *This is the way to get (4.14) from (4.13).*

Proposition 4.3.4. *The matrices* (A, B, C, D) *over* R *obtained in (4.12) can be constructed from* (A_j, B_j, C_j, D_j) *over* $\mathbb{F}_j$, *the I/S/O representations of the convolutional codes* $\mathcal{C}_j$ *over each finite field.*

Proof. Let W be the square minor of size $(\delta+n-k)$ such that $det(W) \in Units(R)$ defined as in Proof of i) of Theorem 4.3.2. Let $\mu_j(W) \cong W_j$ be the square minor of size $(\delta+n-k)$ such that $det(W_j) \in \mathbb{F}_j - \{0\}$.

We know that

$$W^{-1}(K \mid L \mid M) = (\mathcal{K} \mid \mathcal{L} \mid \mathcal{M}) \tag{4.15}$$

where $(K \mid L \mid M)$ and $(\mathcal{K} \mid \mathcal{L} \mid \mathcal{M})$ are minimal first order representations of $\mathfrak{C}$.

If we apply μ_j to the equation (4.15) we get

$$\mu_j[W^{-1} \cdot (K \mid L \mid M)] = [\mu_j(W^{-1}) \cdot \mu_j(K \mid L \mid M)] = [W_j^{-1}(K_j \mid L_j \mid M_j)]$$

$$= (\mathcal{K}_j \mid \mathcal{L}_j \mid \mathcal{M}_j) = \begin{bmatrix} -I_j & A_j & O & B_j \\ O & C_j & -I_j & D_j \end{bmatrix} \tag{4.16}$$

On the other hand

$$\mu_j(\mathcal{K} \mid \mathcal{L} \mid \mathcal{M}) = \mu_j \begin{bmatrix} -I & A & O & B \\ O & C & -I & D \end{bmatrix} \tag{4.17}$$

and since (4.16)=(4.17) we conclude the proof. □

Example 4.3.5. *In this example, we will raise two convolutional codes with their encoders, each one generating a dynamical linear system. The first convolutional code $\mathcal{C}_1$ is over $\mathbb{Z}/2\mathbb{Z}$ and the second $\mathcal{C}_2$ is over $\mathbb{Z}/3\mathbb{Z}$. We compute their first order and I/S/O representations.*

Consider an encoder of $\mathcal{C}_1$ over $\mathbb{Z}/2\mathbb{Z}$

$$G_1(z) = \begin{pmatrix} z-1 & 1 \\ z^2+1 & 0 \\ z^2+1 & z+1 \end{pmatrix}$$

Then there exist matrices K_1, L_1 and M_1 that are a first order representation of $\mathcal{C}_1$. From these, we compute the I/S/O representation associated to the code by the matrices A_1, B_1, C_1 and D_1.

$$K_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, L_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \text{ and } M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Therefore

$$A_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, B_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, C_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \text{ and } D_1 = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Consider an encoder of $\mathcal{C}_2$ *over* $\mathbb{Z}/3\mathbb{Z}$

$$G_2(z) = \begin{pmatrix} z & -1 \\ 1 & z-1 \\ -z^2+z-1 & 0 \end{pmatrix}$$

The following matrices K_2, L_2 *and* M_2 *are a first order representation of* $\mathcal{C}_2$*:*

$$K_2 = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}, L_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Then

$$A_2 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}, B_2 = \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 1 & 0 \end{pmatrix}, C_2 = \begin{pmatrix} 0 & 1 & -1 \end{pmatrix}, \text{ and } D_2 = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Now, we obtain the corresponding I/S/O representation of a familiy of convolutional codes $\mathfrak{C}$ *over* $R \simeq \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ glueing *the matrices* (A_1, B_1, C_1, D_1) *and* (A_2, B_2, C_2, D_2)

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 5 & 4 & 0 \\ 2 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 3 & 2 \\ 1 & 3 \end{pmatrix}, C = \begin{pmatrix} 3 & 1 & 5 \end{pmatrix}, and D = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Therefore we perform matrices K, L *and* M *in* $\mathbb{Z}/6\mathbb{Z}$

$$K = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}, L = \begin{pmatrix} 0 & 1 & 0 \\ 5 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 1 & 5 \end{pmatrix} \text{ and } M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 1 & 3 \\ -1 & 0 & 0 \end{pmatrix} \tag{4.18}$$

Now if we compute $Ker(zK + L|M)$ *then we get an encoder of* $\mathfrak{C}$ *over* $\mathbb{Z}/6\mathbb{Z}$

$$G(z) = \begin{pmatrix} z+3 & 5 \\ 3z^2+1 & -2z+2 \\ -z^2+4z-1 & 3z-3 \end{pmatrix} \tag{4.19}$$

Note that encoder $G(z)$ *restricts to* $\mathbb{Z}/2\mathbb{Z}$ *obtaining* $G_1(z)$ *and to* $\mathbb{Z}/3\mathbb{Z}$ *getting* $G_2(z)$.

4.3.1. Properties of I/S/O representations of a family of convolutional codes.

Let $\Sigma = (A, B, C, D)$ be a system over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ that it is an I/S/O representation that we obtain by a first order representation of a family of convolutional codes over R, $\mathfrak{C}$. Since the pair (A, B) characterizes the dynamic of the system let us denote by $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ the dynamical part of the I/S/O.

From above section we can consider one I/S/O representations for each convolutional code $\mathcal{C}_j$ over each $\mathbb{F}_j$. Let us denote their dynamical part by $\Sigma_j^{\mathcal{C}_j} = (A_j, B_j)^{\mathcal{C}_j}$. Note that $\Sigma_j^{\mathcal{C}_j}$ is reachable (controllability from the origin) for all $j = 1, \ldots, t$, see Remark 3.3.4.

Proposition 4.3.6. *Let* $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ *be the dynamical part of an I/S/O representation of a family of convolutional codes,*$\mathfrak{C}$*, over* $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$*. Then* $\Sigma^{\mathfrak{C}}$ *is a reachable linear system over* R.

Proof. Let (A, B, C, D) be an I/S/O representation of a $\mathfrak{C}$ over R. By Proposition 4.3.4

$$\mu_j(A) \equiv A_j, \mu_j(B) \equiv B_j, \mu_j(C) \equiv C_j \text{ and } \mu_j(D) \equiv D_j.$$

and by [83] each I/S/O representation of each convolutional code over $\mathbb{F}_j[z]$ verifies that $rank\ \Phi_\delta(A_j, B_j) = \delta$ (because it verifies the minimaly condition of Theorem 3.2.1) and so, $\Sigma_j^{\mathcal{C}_j}$ is reachable. Then $rank\ \Phi_\delta(A, B) = \delta$ over the ring R and by Theorem 1.2.7 the dynamical linear system $\Sigma^{\mathfrak{C}}$ is reachable over R. □

Theorem 4.3.7. *Let* $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ *be the dynamical part of an I/S/O representation of a family of convolutional codes,* $\mathfrak{C}$*, over* R*. Then* $\Sigma^{\mathfrak{C}}$ *is a locally Brunovsky linear system over* R.

Proof. By Proposition 4.3.6 the system $\Sigma^{\mathfrak{C}}$ is reachable over R. Since $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ is a von Neuman noetherian ring, by Proposition 2.3.4 hence $\Sigma^{\mathfrak{C}}$ is a locally Brunovsky linear system over R. □

4.3.2. Construction of observable family of convolutional codes.

By Section 3.4 of Chapter 5, if we consider a reachable and observable I/S/O representation over a finite field then we get an observable convolutional code by minimal first order representation. In this section we prove that we can generalize this result to the case of I/S/O representations of family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$.

Proposition 4.3.8. *Let $(A, B, C, D)^{\mathfrak{C}}$ be a reachable linear system over R that we can consider an I/S/O representation of $\mathfrak{C}$. If $(A, B, C, D)^{\mathfrak{C}}$ is observable then $\mathfrak{C}$ is an observable family of convolutional codes over R.*

Proof. Let $\mathfrak{C}$ be a family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$.

By hypothesis $(A, B)^{\mathfrak{C}}$ is a reachable linear system over R and observable, so $rank\ \Omega_\delta(A, C) = rank\ \Phi_\delta(A, B) = \delta$. Let $(A_j, B_j, C_j, D_j)^{\mathcal{C}_j}$ be the linear systems over each $\mathbb{F}_j$. By μ_j we can consider them as I/S/O representations of each convolutional code $\mathcal{C}_j$ over $\mathbb{F}_j$ for $j = 1, \ldots, t$. Because R is a pointwise ring, $rank\ \Omega_\delta(A_j, C_j) = \delta$ and $rank\ \Phi_\delta(A_j, B_j) = \delta$ for $j = 1, \ldots, t$. Then $\mathcal{C}_j$ is an observable convolutional code over each $\mathbb{F}_j$. By Lemma 4.1.6 then $\mathfrak{C}$ is an observable family of convolutional codes over R. □

Part III

Feedback equivalence.

Chapter 5

Feedback Equivalence of a family of convolutional codes.

It is well known that every dynamical part of an I/S/O representation of a convolutional code $\mathcal{C}$ over a finite field $\mathbb{F}$, in sense of [83], denoted by $\Sigma^{\mathcal{C}} = (A, B)^{\mathcal{C}}$, forms a reachable linear system over $\mathbb{F}$. Since a field is a Brunovsky ring (see [11]) then each $\Sigma^{\mathcal{C}}$ is a Brunovksy linear system over $\mathbb{F}$. The problem of feedback classification of Brunovsky linear systems over a finite vector spaces is solved by Brunovsky canonical forms. Moreover, the number of feedback isomorphisms of Brunovsky (or reachable) linear systems can be computed by Kronecker's indices $\kappa_1 \geq \ldots \geq \kappa_k$ being equal to partitions of dimension of matrix A (the rank of the state space of the system). Note that above results imply that there exists a clear relation between I/S/O representations of a convolutional codes and Brunovsky linear systems. The key of this relations are in the invariants of both systems under feedback equivalence defined by their Kronecker's (or controllabiliity) indices studied in [8], [44], [58] and [79].

On the other hand, more recently, feedback equivalence over convolutional codes has been used for its applications by the relation between convolutional codes and systems theory by first order representations by equivalence class of GL_δ (see [26], [28],[29], [30], [33] and [70], for example).

Our results in this part show that not only the dynamical part of an I/S/O representation is a Brunovsky linear system over $\mathbb{F}$, moreover, the number of feedback classes of convolutional codes, that is, the amount of feedback classes of dynamical parts of an

I/S/O equals the number of feedback isomorphisms of Brunovsky linear systems over $\mathbb{F}$.

In the case of family of convolutional codes the above results hold. The ring $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ is a von Neumann regular noetherian ring and we have shown in Chapter 2 that every reachable system over R is a locally Brunovsky linear system. Hence every I/S/O representation is a reachable system and also is a locally Brunovsky linear system over R. Furthermore, the number of feedback isomorphisms of locally Brunovsky linear systems can be computed and is equal to the number of feedback classes of dynamical parts os I/S/O representations of families of convolutional codes over R.

This chapter is organized as follows: In Section 1, an equivalence relation between convolutional codes and its Kronecker indices is given over finite fields. One can also perform the computation of feedback equivalence classes. Moreover, a relation between dynamics of I/S/O representations and Brunovsky linear systems is given in terms of feedback equivalence classes. In Section 2 we generalize the above results over families of convolutional codes over finite product of finite fields and locally Brunovsky linear systems..

5.1. Invariants of a convolutional code over finite fields.

Let $\mathcal{C}$ be a (n, k) convolutional code over $\mathbb{F}$. Recalling the Definition 3.1.8 we consider the Kronecker's indices $\kappa_1 \geq \ldots \geq \kappa_k$ of any minimal encoder of $\mathcal{C}$. We also have the degree of the code $\mathcal{C}$ defined by its Kronecker's indices by $\delta = \sum_{i=1}^{k} \kappa_i$ that is invariant of the code.

Note that we consider a minimal encoder of the convolutional code and then the Kronecker's indices and Forney's indices are equal and the degree of the code δ is equal to the complexity of its encoder c.

Definition 5.1.1. *Let us denote by $\mathfrak{K}^{\mathcal{C}}$ as the k-tuple of Kronecker Indices of a (n, k) convolutional code $\mathcal{C}$ over $\mathbb{F}$; namely, $\mathfrak{K}^{\mathcal{C}} = (\kappa_1, \ldots, \kappa_k)$.*

We define a feedback relation between convolutional codes in terms of their Kronecker's Indices.

Definition 5.1.2. *Let $\mathcal{C}$ and $\overline{\mathcal{C}}$ be convolutional codes over $\mathbb{F}$. The feedback convolutional codes relation, $\overset{f.c.e}{\sim}$, defined by*

$$\mathcal{C} \overset{f.c.e}{\sim} \overline{\mathcal{C}} \Leftrightarrow \mathfrak{K}^{\mathcal{C}} = \mathfrak{K}^{\overline{\mathcal{C}}}$$

is an equivalence relation.

Lemma 5.1.3. *The number of feedback equivalence classes of convolutional codes with the same degree δ under f.c.e relation is equal to the partitions of the degree of the code; that is,*

$$\#\{ \text{ feedback equivalence classes of } \mathcal{C} \ \} = p(\delta)$$

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

Proof. Feedback equivalent classes of convolutional codes with the same degree δ is defined as the different ways to get δ by sums of Kronecker's Indices, namely, the partition of integer δ. □

In systems theory over a finite vector space, Kronecker's indices are known as controllability (reachability) indices of pair $\Sigma = (A, B)$ and these indices are invariants of the system under feedback equivalence: If $\Sigma = (A, B)$ is a system that represents a dynamic over a finite dimensional $\mathbb{K}$-vector spaces, by the Kalman's Decomposition and Brunovsky's Theorem the feedback classification of linear systems over $\mathbb{K}^n$ reduces to the classification of reachable systems. The number of feedback equivalent dynamical linear systems is equal to the number of feedback equivalent reachable systems that may be performed by using Kronecker invariants indices $\kappa_1 \geq \kappa_2 \geq \cdots \geq \kappa_p$ of the pencil $(zI - A, B)$ associated to $\Sigma = (A, B)$.

Since by first order representation we can compute an I/S/O representation for a convolutional code $\mathcal{C}$ ([70], [71] and [83]), the relation between controllability indices of the code and controllability (reachability) indices of the I/S/O representation as dynamical linear system is clear and it is given in following theorem:

Theorem 5.1.4 (c.f. Theorem 2, [58].)**.** *If $\Sigma = (A, B)$ forms a controllable pair such that $A \in \mathcal{M}_{\delta\times\delta}(\mathbb{F})$ and $B \in \mathcal{M}_{\delta\times k}(\mathbb{F})$, then there exist positive integers $\kappa_1 \geq \ldots \geq \kappa_k$ (often referred to as the controllability indices of the pair (A, B)) only dependent on the GL_δ equivalence class of (A, B) having the following properties:*

1. *$\kappa_1 = \kappa$, the controllability index of (A, B).*
2. *$\sum_{i=1}^{k} \kappa_i = \delta$, the size of matrix A.*
3. *There exists polynomial matrices $X(z), Y(z), U(z)$ satisfying*

$$Ker \begin{bmatrix} zI - A & 0 & -B \\ -C & I & -D \end{bmatrix} = Im \begin{bmatrix} X(z) \\ Y(z) \\ U(z) \end{bmatrix}$$

and having the property that the i-th column degree of $G(z) = \begin{pmatrix} Y(z) \\ U(z) \end{pmatrix}$ *is equal to* κ_i*, and the ith column degree of* $X(z)$ *is equal to* $\kappa_i - 1$ *for* $i = 1, \ldots, k$.

Since I/S/O representations over a finite field allow us to understand a convolutional code by $\mathcal{C} = Ker(zK + L \mid M) = Ker \begin{pmatrix} zI - A & 0 & -B \\ -C & I & -D \end{pmatrix}$, Theorem 5.1.4 could be applied and then controllability indices of $\mathcal{C}$ equals the controllability indices of the pair $\Sigma^{\mathcal{C}} = (A, B)^{\mathcal{C}}$, dynamical part of I/S/O representation of the code $\mathcal{C}$ as linear system over $\mathbb{F}$.

We call Kronecker's Indices in both cases of controllability indices of codes and systems.

Remark 5.1.5 (cf. [10])**.** *Kronecker's indices of a dynamical linear system over* $\mathbb{F}$ *are in bijective correspondence with conjugate partitions of the Kronecker indices that are given by* $(\xi_1, \xi_2, \ldots, \xi_p)$ *where*

$$\xi_1 = rk(B) \text{ and}$$

$$\xi_i = rk(B, AB, ..., A^{i-1}B) - rk(B, AB, ..., A^{i-2}B).$$

These indices ξ *also classify the system too.*

Let us denote by $\xi^{\mathcal{C}}$ *as the k-tuple of Kronecker's indices conjugate partition of the I/S/O representations of a* (n, k) *convolutional code* $\mathcal{C}$ *over* $\mathbb{F}$*; that is,* $\xi^{\mathcal{C}} = (\xi_1, \ldots, \xi_k)$.

Proposition 5.1.6. *Let* $\mathcal{C}$ *and* $\overline{\mathcal{C}}$ *be convolutional codes over* $\mathbb{F}$*. The Kronecker Indices of* $\mathcal{C}$ *and* $\overline{\mathcal{C}}$ *are equal if and only if the dynamical parts of its I/S/O's are feedback isomorphic; namely,*

$$\mathfrak{K}^{\mathcal{C}} = \mathfrak{K}^{\overline{\mathcal{C}}} \Leftrightarrow \Sigma^{\mathcal{C}} \overset{f.i}{\simeq} \overline{\Sigma}^{\overline{\mathcal{C}}}$$

where we denote by f.i the feedback isomorphism between Brunovsky linear systems.

Proof. Let (A, B, C, D) and $(\overline{A}, \overline{B}, \overline{C}, \overline{D})$ be the corresponding I/S/O representations by first order representations of $\mathcal{C}$ and $\overline{\mathcal{C}}$. Let us denote the dynamical part of these I/S/O's by $\Sigma^{\mathcal{C}} = (A, B)^{\mathcal{C}}$ and $\overline{\Sigma}^{\overline{\mathcal{C}}} = (\overline{A}, \overline{B})^{\overline{\mathcal{C}}}$.

$\Rightarrow$) If $\mathfrak{K}^{\mathcal{C}} = \mathfrak{K}^{\overline{\mathcal{C}}}$, since the Kronecker's indices of a convolutional code are equal to the Kronecker's indices of its I/S/O representation, then $\mathfrak{K}^{\Sigma^{\mathcal{C}}} = \mathfrak{K}^{\Sigma^{\overline{\mathcal{C}}}}$. Because the Kronecker's indices are feedback equivalence invariants for Brunovsky linear systems (note that these indices are invariant of reachable systems and every I/S/O representation is reachable and Brunovsky), hence $\Sigma^{\mathcal{C}} \overset{f.i.}{\simeq} \Sigma^{\overline{\mathcal{C}}}$.

$\Leftarrow$) If $\Sigma^{\mathcal{C}} \overset{f.i.}{\simeq} \Sigma^{\overline{\mathcal{C}}}$, then Kronecker's indices of the systems are equal, $\mathfrak{K}^{\Sigma^{\mathcal{C}}} = \mathfrak{K}^{\Sigma^{\overline{\mathcal{C}}}}$ and then $\mathfrak{K}^{\mathcal{C}} = \mathfrak{K}^{\overline{\mathcal{C}}}$. □

Proposition 5.1.7. *Let $\mathbb{F}$ be a finite field. Then*

$$\left\{\begin{array}{c} \textit{Feedback classes of} \\ \textit{Dynamical parts of I/S/O's} \\ \textit{of convolutional codes} \\ \textit{over } \mathbb{F} \end{array}\right\} = \left\{\begin{array}{c} \textit{Feedback classes of} \\ \textit{Brunovsky Linear Systems} \\ \textit{over } \mathbb{F} \end{array}\right\}$$

Proof. Let us denote by $(A,B)^{\mathcal{C}}$ the set of dynamics of the I/S/O representations of a convolutional code over $\mathbb{F}$. Let denote by $Br(\mathbb{F})$ the set of Brunovsky Linear Systems over $\mathbb{F}$ with state space of rank δ. Let $[(A,B)^{\mathcal{C}}]$ be the classes of feedback equivalence of $(A,B)^{\mathcal{C}}$ under the feedback convolutional codes equivalence given in Definition 5.1.2, $f.c.e$, and let $[Br(\mathbb{F})]$ be the classes of feedback isomorphisms of $Br(\mathbb{F})$ under the feedback isomorphism of Brunovsky linear systems over fields.

Since every $(A,B)^{\mathcal{C}}$ representation of a convolutional code over a finite field $\mathbb{F}$ is a reachable system and fields are Brunovksy rings, every I/S/O representation is a Brunovsky linear system. We conclude the proof because $\#\,[Br(\mathbb{F})] = p_{\mathbb{N}}(\delta)$ and $\#\,\{\text{feedback classes of } \mathcal{C}\} = \#\,\{(A,B)^{\mathcal{C}}\} = p_{\mathbb{N}}(\delta)$. Then $[(A,B)^{\mathcal{C}}] = [Br(\mathbb{F})]$ □

5.2. Invariants of a family of convolutional codes.

Let $\mathfrak{C}$ be a (n,k) family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Let $\mathcal{C}_j$ be the j-th (n,k) convolutional code over $\mathbb{F}_j$ such that $\mathcal{C}_j \simeq \mathfrak{C} \otimes_{R[z]} \mathbb{F}_j[z]$.

Note that results of above section hold for the convolutional codes $\mathcal{C}_j$ for all $j = 1, \ldots, t$, and then $\xi^{\mathcal{C}_j} = \{(\xi_i^j)\}$ and $\mathfrak{K}^{\mathcal{C}_j} = \{(\kappa_i^j)\}$ are invariant indices of each code with $i = 1, \ldots, k$.

Definition 5.2.1. *We define the Kronecker indices of $\mathfrak{C}$,and we denote them by $\mathfrak{K}^{\mathfrak{C}}$, as the t-uple of vectors where each component are the Kronecker indices of each $\mathcal{C}_j$, namely*

$$\mathfrak{K}^{\mathfrak{C}} = [(\kappa_1^1, \ldots, \kappa_1^t), \ldots, (\kappa_k^1, \ldots, \kappa_k^t)]$$

where (κ_i^j) *is the* i*-th Kronecker index of the convolutional code* $\mathcal{C}_j$*.*

Definition 5.2.2. *We define the Kronecker′s indices conjugate partition of* $\mathfrak{C}$*, and we denote them by* $\xi^{\mathfrak{C}}$*, as the* t*-uple of vectors where each component are the conjugate partition of Kronecker indices of each* $\mathcal{C}_j$*, namely*

$$\xi^{\mathfrak{C}} = [(\xi_1^1, \ldots, \xi_1^t), \ldots, (\xi_k^1, \ldots, \xi_k^t)]$$

where (ξ_i^j) *is the* i*-th Kronecker's index conjugate partition of the convolutional code* $\mathcal{C}_j$*.*

Remark 5.2.3. *By definition of* $\mathfrak{C}$ *every convolutional code* $\mathcal{C}_j$ *has the same number of Kronecker indices,* k*, and* $\sum_{i=1}^{k} \kappa_i^j = \delta$*, the degree of the code, for all* $j = 1 \ldots t$*.*

Definition 5.2.4. *Let* $\mathfrak{C}$ *and* $\overline{\mathfrak{C}}$ *be convolutional codes over* R*. The feedback relation of families of convolutional codes,* $\overset{f.f.c.e.}{\sim}$*, defined as*

$$\mathfrak{C} \overset{f.f.c.e}{\sim} \overline{\mathfrak{C}} \Leftrightarrow \mathfrak{K}^{\mathfrak{C}} = \mathfrak{K}^{\overline{\mathfrak{C}}}$$

is an equivalence relation.

Lemma 5.2.5. *The number of feedback equivalence classes of family of convolutional codes with the same degree* δ *under feedback equivalence is* $p_{\mathbb{N}}(\delta)^t$ *where* $p_{\mathbb{N}}(\delta)$ *is the partition of the degree of the codes.*

Proof. Feedback equivalence classes of a family of convolutional codes $\mathfrak{C}$ such that the components of its Kronecker's indices verify $\sum_{j=1}^{k} \kappa_i^j = \delta$ for each $i = 1, \ldots, t$, are the possible ways to get δ, t times; that is, $p_{\mathbb{N}}(\delta)^t$. □

We give and recall some notations in order to clarify the following results.

Notation. *Let* $\mathfrak{C}$ *and* $\overline{\mathfrak{C}}$ *be families of* (n, k) *convolutional codes over* R*.*

1. *Let* $\Sigma = (A, B, C, D)$ *and* $\overline{\Sigma} = (\overline{A}, \overline{B}, \overline{C}, \overline{D})$ *be the corresponding I/S/O representations obtained of* $\mathfrak{C}$ *and* $\overline{\mathfrak{C}}$ *by Theorem 4.2.4 . We denote by* $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ *and* $\overline{\Sigma}^{\overline{\mathfrak{C}}} = (\overline{A}, \overline{B})^{\overline{\mathfrak{C}}}$ *the dynamical part of these systems where* $A, \overline{A} \in \mathcal{M}_{\delta\times\delta}(R)$ *and* $B, \overline{B} \in \mathcal{M}_{\delta\times k}(R)$*.*

2. *Let us denote by* $\mathfrak{K}^{\mathfrak{C}}$ *and* $\mathfrak{K}^{\overline{\mathfrak{C}}}$ *the set of Kronecker indices of the families of convolutional codes and* $\xi^{\mathfrak{C}}$ *and* $\xi^{\overline{\mathfrak{C}}}$ *the set of conjugate partition of the Kronecker indices of these families.*

3. *Let us denote by* $\mathfrak{K}^{\Sigma^{\mathfrak{C}}}$ *and* $\mathfrak{K}^{\Sigma^{\overline{\mathfrak{C}}}}$ *the set of Kronecker Indices of the associated pairs* $(A,B)^{\mathfrak{C}}$ *and* $(\overline{A},\overline{B})^{\overline{\mathfrak{C}}}$ *to the family of convolutional codes as linear systems over* R*. Moreover, let us denote by* $\xi^{\Sigma^{\mathfrak{C}}}$ *and* $\xi^{\Sigma^{\overline{\mathfrak{C}}}}$ *the set of conjugate partition of the Kronecker indices of these dynamical systems*

4. *Let us denote by* $\Sigma^{\mathcal{C}_j}=(A_j,B_j)^{\mathcal{C}_j}$ *and* $\overline{\Sigma}^{\overline{\mathcal{C}_j}}=(\overline{A}_j,\overline{B}_j)^{\overline{\mathcal{C}_j}}$ *be the corresponding dynamical parts of the I/S/O representations, computed by first order representations, of each* $\mathcal{C}_j$ *and* $\overline{\mathcal{C}}_j$*, the restrictions to each finite field* $\mathbb{F}_j$ *of* $\mathfrak{C}$ *and* $\overline{\mathfrak{C}}$*.*

5. *Let us denote by* $\mathfrak{K}^{\Sigma^{\mathcal{C}_j}}$ *and* $\mathfrak{K}^{\Sigma^{\overline{\mathcal{C}_j}}}$ *the set of Kronecker indices of the dynamical behaviour of its associated I/S/O representations to convolutional codes over finite fields as linear systems. Moreover, let us denote by* $\xi^{\Sigma^{\mathcal{C}_j}}$ *and* $\xi^{\Sigma^{\overline{\mathcal{C}_j}}}$ *the set of conjugate partition of Kronecker indices of these I/S/O representations.*

We give our main results:

Theorem 5.2.6. *Let* $\mathfrak{C}$ *and* $\overline{\mathfrak{C}}$ *be families of convolutional codes over* $R\simeq\mathbb{F}_1\times\ldots\times\mathbb{F}_t$*. Let* $\Sigma^{\mathfrak{C}}$ *and* $\overline{\Sigma}^{\overline{\mathfrak{C}}}$ *be the corresponding dynamical parts of their I/S/O representations. Then*

$$\mathfrak{K}^{\mathfrak{C}}=\mathfrak{K}^{\overline{\mathfrak{C}}}\Leftrightarrow\Sigma^{\mathfrak{C}}\overset{f.i}{\simeq}\overline{\Sigma}^{\overline{\mathfrak{C}}}$$

where $f.i$ *denoting the feedback isomorphism between locally Brunovsky linear systems with state space of rank* δ *given in Definition 1.3.4.*

Proof. $\Rightarrow$) If $\mathfrak{K}^{\mathfrak{C}}=\mathfrak{K}^{\overline{\mathfrak{C}}}$, then

$$[(\kappa_1^1,\ldots,\kappa_1^t),\ldots,(\kappa_k^1,\ldots,\kappa_k^t)]=[(\overline{\kappa}_1^1,\ldots,\overline{\kappa}_1^t),\ldots,(\overline{\kappa}_k^1,\ldots,\overline{\kappa}_k^t)]$$

The sets of $\{\kappa_i^j\}$ and $\{(\overline{\kappa}_i^j)\}$ are the controllability indices of the convolutional codes $\mathcal{C}_j$ and $\overline{\mathcal{C}}_j$ over finite fields and, by [58], these indices equal the controllability indices of the I/S/O representations of the codes, $\Sigma^{\mathcal{C}_j}$ and $\overline{\Sigma}^{\overline{\mathcal{C}_j}}$, namely, if $\mathfrak{K}^{\mathcal{C}_j}=\mathfrak{K}^{\overline{\mathcal{C}}_j}$ then $\mathfrak{K}^{\Sigma^{\mathcal{C}_j}}=\mathfrak{K}^{\Sigma^{\overline{\mathcal{C}}_j}}$. From systems theory point of view, these Kronecker's indices are invariant and classify the systems over vector spaces.

In the case of locally Brunovksy linear systems over commutative rings, the invariant indices that classify are the conjugate partition of Kronecker indices. Since there exists a bijective correspondence between Kronecker and Kronecker's indices of (locally) Brunovsky linear systems, if $\mathfrak{K}^{\Sigma^{\mathcal{C}_j}}=\mathfrak{K}^{\overline{\Sigma}^{\overline{\mathcal{C}}_j}}\Rightarrow\xi^{\Sigma^{\mathcal{C}_j}}=\xi^{\overline{\Sigma}^{\overline{\mathcal{C}}_j}}$. These Kronecker's conjugate partitions $\xi^{\Sigma^{\mathcal{C}_j}}$

are the class of feedback isomorphisms of the invariants I_i of the system $\Sigma^{\mathcal{C}_j}$ in the $\mathbf{P}(\mathbb{F}_j)$. Now, since $\mathbf{P}(R) \simeq \mathbf{P}(\mathbb{F}_1) \times \ldots \times \mathbf{P}(\mathbb{F}_t)$ for all j then if $\xi^{\Sigma^{\mathcal{C}_j}} = \xi^{\overline{\Sigma}^{\overline{\mathcal{C}}_j}}$ then $\xi^{\Sigma^{\mathfrak{C}}} = \xi^{\overline{\Sigma}^{\overline{\mathfrak{C}}}}$.

The partitions ξ are invariants from feedback classification in systems theory over R because the invariants $[I_i]$ of the system classify when $\mathbf{P}(R)$ is cancellative. So $\Sigma^{\mathfrak{C}} = (A,B)^{\mathfrak{C}} \overset{f.i}{\simeq} \overline{\Sigma}^{\overline{\mathfrak{C}}} = (\overline{A},\overline{B})^{\overline{\mathfrak{C}}}$.

$\Leftarrow$) If $\Sigma^{\mathfrak{C}} = (A,B)^{\mathfrak{C}} \overset{f.i}{\simeq} \overline{\Sigma}^{\overline{\mathfrak{C}}} = (\overline{A},\overline{B})^{\overline{\mathfrak{C}}}$ then the invariants $[Z_i]^{\Sigma^{\mathfrak{C}}} = [Z_i]^{\overline{\Sigma}^{\overline{\mathfrak{C}}}}$. Since R is a Von Neuman noetherian ring, $\mathbf{P}(R)$ is cancellative and then $[I_i]^{\Sigma^{\mathfrak{C}}} = [I_i]^{\overline{\Sigma}^{\overline{\mathfrak{C}}}}$. Now, by decomposition of $\mathbf{P}(R)$, if $\xi^{\Sigma^{\mathfrak{C}}} = \xi^{\overline{\Sigma}^{\overline{\mathfrak{C}}}} \Rightarrow \xi^{\Sigma^{\mathcal{C}_j}} = \xi^{\overline{\Sigma}^{\overline{\mathcal{C}}_j}}$.

Since over fields there exists a bijective correspondence between the partitions ξ and the Kronecker indices, hence $\mathfrak{K}^{\Sigma^{\mathcal{C}_j}} = \mathfrak{K}^{\overline{\Sigma}^{\overline{\mathcal{C}}_j}}$ and by duality between systems and codes then $\mathfrak{K}^{\mathcal{C}_j} = \mathfrak{K}^{\overline{\mathcal{C}_j}}$ and we conclude that $\mathfrak{K}^{\mathfrak{C}} = \mathfrak{K}^{\overline{\mathfrak{C}}}$. □

Theorem 5.2.7. *Let $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ be a ring such that $\mathbb{F}_j$ are finite fields. Then*

$$\left\{ \begin{array}{c} \textit{Feedback classes of} \\ \textit{Dynamical parts of I/S/O's} \\ \textit{of families of convolutional} \\ \textit{codes over } R \end{array} \right\} = \left\{ \begin{array}{c} \textit{Feedback classes of} \\ \textit{Locally Brunovsky Linear Systems} \\ \textit{over } R \end{array} \right\}$$

Proof. Let us denote by $\{(A,B)\}^{\mathfrak{C}}$ the set of dynamics behaviours of I/S/O Representations of families of convolutional codes over R. Let us denote by $\{Br(R)\}$ the set of locally Brunovsky linear systems over R with state space the rank δ. Let $[(A,B)^{\mathfrak{C}}]$ be the classes of feedback equivalence of $\{(A,B)\}^{\mathfrak{C}}$ under feedback equivalence of families of convolutional codes given in Definition 5.2.4 and let $[Br(R)]$ the classes of feedback isomorphisms of $\{Br(R)\}$ under feedback isomorphism of Brunovsky Linear Systems over commutative rings.

By Theorem 5.2.6 and Theorem 4.3.7

$$\#\ \{\ \text{feedback classes of } \mathfrak{C}\} = \#\ \{[(A,B)^{\mathfrak{C}}]\} \subseteq \#\{[Br(R)]\}$$

By Lemma 5.2.5, $\#\ \{\ \text{feedback classes of } \mathfrak{C}\} = p(\delta)^t$ and by Corollary 2.2.6, this number is equal to $\#\{[Br(R)]\}$ and we conclude that

$$[(A,B)^{\mathfrak{C}}] = [Br(R)]$$

□

Remark 5.2.8. *Note that if $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ and let e_j be the structural idempotent of $\mathbb{F}_j$ then*

$$R \xrightarrow{\sim} \mathbb{F}_1 \times \ldots \times \mathbb{F}_j \times \ldots \times \mathbb{F}_t$$

$$e_j \mapsto (0, \ldots, 0, 1, 0, \ldots, 0)$$

Then (by abuse of notation we state in self-explain notation)

$$\Sigma = e_1 \cdot \{ \textit{ Brunovsky Form } (\kappa_1^1 \ldots \kappa_k^1)\} + \ldots + e_t \cdot \{ \textit{ Brunovsky Form } (\kappa_1^t \ldots \kappa_k^t)\}$$

Example 5.2.9. *The structural idempotents of $\mathbb{Z}/2 \cdot 3 \cdot 5 \cdot 7\mathbb{Z}$ are*

$$e_1 \to 3 \cdot 5 \cdot 7 = 105$$

$$e_2 \to 2 \cdot 5 \cdot 7 = 70$$

$$e_3 \to 2 \cdot 3 \cdot 7 = 42$$

$$e_4 \to 2 \cdot 3 \cdot 5 = 30$$

Example 5.2.10. *Let R be $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $\Sigma = (A, B)$ be a dynamical linear system over $\mathbb{Z}/6\mathbb{Z}$. Let $\mathfrak{K}^{\Sigma} = [(1,2),(1,0)]$ be the Kronecker indices of Σ.*

Let Σ be the following system over $\mathbb{Z}/6\mathbb{Z}$

$$\Sigma = \left[\begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix} \right]$$

Then

$$3 \cdot \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right] + 2 \cdot \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]$$

Part IV

Conclusions.

In this work we have successfully completed the study of the number of feedback classes of locally Brunovsky linear systems over different classes of rings. Furthermore, we have characterized von Neumann regular rings by properties of linear systems.

Moreover, we have generalized the connection between convolutional codes and linear systems by first order and I/S/O representations to certain commutative rings with identity which allows us to construct observable families of convolutional codes using reachable and observable linear systems.

Finally, we have shown that the number of locally Brunovsky linear systems over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ with $\mathbb{F}_j$ a finite field for $j = 1, \ldots, t$ is equal to the number of dynamic parts of the representations I/S/O of families of convolutional codes over R under a feedback equivalence defined by the indices of Kronecker of both types of systems.

The main results of the thesis are listed below:

1. We have computed the number of feedback isomorphisms of locally Brunovsky linear systems (and hence reachable systems) over different classes of rings:

   a) Finite product of rings. In particular, finite product of projectively trivial rings.

   b) von Neumann regular noetherian rings and hence over rings of modular integers $\mathbb{Z}/l\mathbb{Z}$ where $l = p_1 \ldots p_t$ is square free.

   c) Dedekind domains. In this result a new combinatorial number $\nu(n, k) = \nu(n, k, p) + \nu(n, k, p')$ appears.

2. Moreover, we have shown that a von Neumann regular ring is a locally Brunovsky ring.

3. We have defined a family of convolutional codes over a commutative ring with identity. We have studied some properties of the code and of its encoder.

4. We have computed a first order representation of a family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ where $\mathbb{F}_j$ is a finite field for each j.

5. From the above point, we have obtained an I/S/O representation of a family of convolutional codes over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ and we have studied properties such as reachability, observability and locally Brunovsky.

6. We have defined a feedback equivalence relation between convolutional codes and its Kronecker Indices over finite fields. Moreover, we have computed the number of classes of this feedback equivalence.

7. Finally, we have generalized the above feedback relation between the set of Kronecker indices of a family of convolutional codes $\mathfrak{C}$ over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ and the Kronecker indices (or Kronecker's conjugate partition indices) of I/S/O representation that we get from $\mathfrak{C}$. This feedback relation allows us to conclude that there exists a bijective correspondence between feedback isomorphisms of locally Brunovksy linear systems over R and feedback classes of dynamical behaviours of I/S/O's representations of families of convolutional codes over R.

Applications to cybernetics, codes and cryptography. Future research.

We give an overview of some areas of research with which this work is related. Some of them are a field of future research in order to conclude a complete theory of feedback classification between convolutional codes and sytems over commutative rings. The other areas can be considered as a field of implementation and applications of this work.

Convolutional codes are used in numerous applications such as satellite communication, mobile communication, digital video or radio among others. Moreover, the use in the NASA of error-correcting codes in the Cassini orbiter in its communication with Earth is only an example of the fact that convolutional codes are a very powerful tool in the transmission system of information such as systems that send and receive data information from deep space. Another application of convolutional codes is given by its applications to hard decision codes, in particular Reed Solomon codes. Recent advances in parallely and serial concatenated convolutional codes focus on their implementation in the construction of turbocodes.

Our results can be useful in coding theory in the following way: to develop the relationship between dynamical systems and convolutional codes over rings can extend the study of new ways to build convolutional codes with certain characteristics and study the decoding process by linear systems. In the encoding and decoding processes we can apply our work if we want to send a message to t receivers but each receiver is able to receive only part of the message. In this case, a finite base of t communication systems is used, so that the message is encoded in the product of the t fields: $R \simeq \mathbb{F}_1 \times \mathbb{F}_2 \times ... \times \mathbb{F}_t$. That

is, we can use the code generated over R to send a message to each $\mathbb{F}_j[z]$ receiver such that each one receives only part of the message. Note that a continuity between receivers is not needed. Moreover, if the messages over $\mathbb{F}_j$ is shared, it would be possible to create the original message that we assume unique.

In the area of cryptography the possible relevance of our results comes from different points of view. In the same way than in [22], we can apply convolutional codes to try to decode cryptosystems. Furthermore the number of feedback isomorphims of locally Brunovsky linear systems over Dedekind domains can be applied in the case of the unit circle and so, in the case of all closed curves that are homeomorphic with the unit circle as topological spaces and then, our results could be interesenting in the study of convolutional codes over elliptic and other curve by systems approach.

Regarding cybersecurity, duality between convolutional codes and trellis representations supposes the main apported chance of use of convolutional codes modelling networks. This work can be implemented to obtain algebraic system of simultaneous signal encodings in *multicast* linear coding networks. In particular, the closed relation between convolutional codes, trellis representations, graphs of networks and linear systems allows us to apply our results, for example, over Boolean rings. Boolean networks are quite useful in modeling and quantitative description of cell regulation. A new technique has been developed for analyzing and synthesizing Boolean (control) networks based on the conversion of the logical dynamics of a Boolean network into a standard discrete-time dynamics (see [20]).

Databases of the services of information security are growing quicker than needed tools to treat the information with a better management of the amount of the data and the classification of the bases. It supposes studying and storing input data. Recent works present the implementation of algebraic and stochastic algorithms in order to optimize the procces of classification. The study is focused on antiterrorism, see [81] for details.

A possible line of future research could be to extend the classsification to systems and convolutional codes to other classes of rings, thus, the relation between them. Another line could be to give a complete characterization of families of convolutional codes over other rings and its representations, and study properties like distances, construction of codes, and enconding and decoding processes.

Finally, the combinatorial number $\nu(n,k)$ has been studied by our current research group in order to find a generatrix formula and to complete the properties of the number.

Part V

Resumen en castellano.

Índice en castellano.

Chapter 6

Resumen.

Gran parte de los fenómenos de la naturaleza se modelan matemáticamente a través de sistemas lineales de ecuaciones diferenciales. En este trabajo estudiamos la clasificación, bajo equivalencia feedback, de sistemas lineales localmente Brunovsky sobre anillos conmutativos con unidad.

La generalización a anillos conmutativos de la clasificación feedback para sistemas lineales existente ([8] y [44]) no es una tarea sencilla, pero sí podemos encontrar una familia completa de invariantes feedback para los sistemas lineales conocidos como localmente Brunovsky, pudiendo construir una forma canónica de Brunovsky, veáse [40].

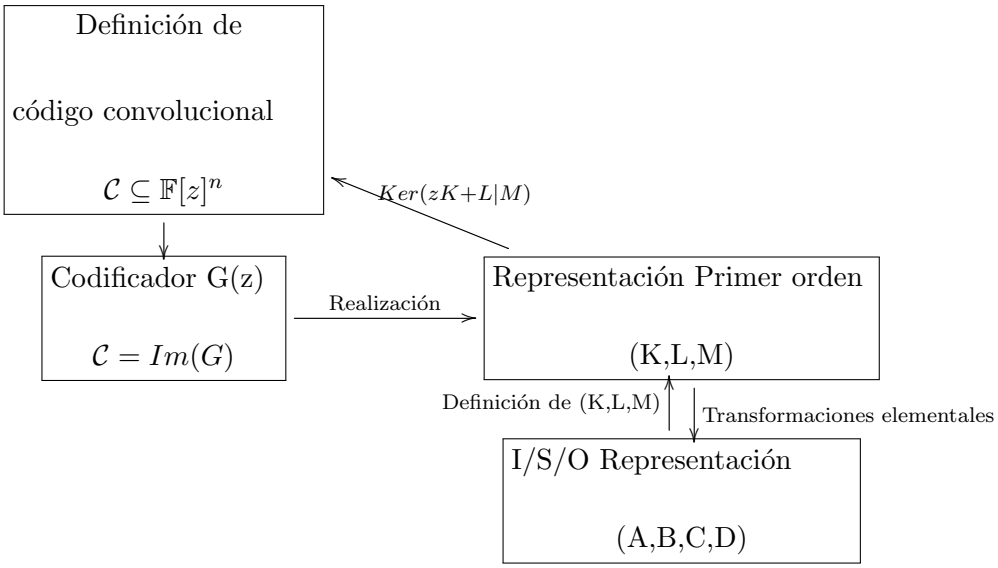
Además, en [8] y [44], se calcula el número de clases de equivalencia feedback de sistemas accesibles sobre un $\mathbb{K}$-espacio vectorial n-dimensional siendo igual al número de particiones del entero n, $p_{\mathbb{N}}(n)$. Este resultado ha sido generalizado en [10] al marco general de sistemas lineales regulares (localmente Brunovsky) sobre anillos conmutativos con unidad.

Nuestro objetivo en este trabajo es, aplicando los resultados de [10], calcular el número de clases de isomorfismos feedback de sistemas lineales localmente Brunovsky con espacio de estados X sobre diferentes anillos conmutativos con unidad.

Por otra parte, los códigos convolucionales pertenecen a la clase de códigos correctores, fundamentales en la transmisión de datos digitales y en los sitemas que transmiten este tipo de datos. El estudio de códigos convolucionales mediante otros campos de conocimiento es muy útil para, por ejemplo, construir códigos convolucionales con determinadas propiedades. En este trabajo estamos interesados en la relación existente entre códigos convolucionales y sistemas lineales. El paso de un campo a otro viene dado, sobre cuerpos

fintos, en términos de ternas de matrices que conforman representaciones de primer orden del código y nos permiten obtener una representación I/S/O en la que las entradas y salidas del sistema son parte de las palabras del código (los resultados principales pueden encontrarse en [47], [70], [71] y [83]). El proceso de decodificación del código se puede llevar a cabo mediante la *output controllability matrix*, es decir, la matriz que resuelve el sistema dinámico asociado al código, veáse [27], [28] y [29].

A continuación se expone un diagrama sobre el proceso donde una flecha significa que existe un procedimiento disponible para pasar de un lado al otro.



La pregunta natural es: ¿podemos generalizar el anterior diagrama al marco de los anillos conmutativos con unidad? En este trabajo estudiamos la generalización (definición, propiedades, representaciones de primer orden y representaciones como sistemas lineales) para familias de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ con $\mathbb{F}_j$ un cuerpo finito para $j = 1, \ldots, t$. Además, trabajamos con familias observables de códigos convolucionales así como con su contrucción mediante sistemas lineales asociados que sean accesibles y observables sobre R.

Finalmente, estudiamos la equivalencia feedback entre códigos convolucionales mediante sus índices de Kronkecker, así como la relación de los sistemas dinámicos lineales asociados y los sistemas localmente Brunovsky. Estos resultados son generalizados también para el caso de $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ con $\mathbb{F}_j$ un cuerpo finito para $j = 1, \ldots, t$ y familias de códigos convolucionales sobre R.

A continuación pasamos a enumerar los resultados originales de este trabajo. Las demostraciones no se incluyen y se remite al lector al documento íntegro en inglés. A lo largo de todo el trabajo R se considera un anillo conmutativo con unidad.

6.1. Avances en la clasificación de sistemas lineales sobre anillos conmutativos.

La equivalencia feedback de sistemas lineales sobre anillos conmutativos ha sido estudiada extensamente usando álgebra conmutativa, veáse por ejemplo [7],[5],[6],[38] y [78].

Para el caso de cuerpos, el Teorema de Brunovsky establece que cada sistema lineal accesible sobre $\mathbb{K}$ es equivalente feedback a una forma canónica de Brunovsky ([8] y [44]). Además, se demuestra en [11] que la clase de anillos donde cada sistema accesible es de tipo Brunovsky es exactamente la clase de los cuerpos.

La generalización al caso de los anillos conmutativos con unidad requiere nuevas maneras de calcular formas canónicas e invariantes. En [40], se demuestra que es posible encontrar una familia completa de invariantes feedback para sistemas lineales conocidos como localmente Brunovsky; es decir, para sistemas lineales que admiten localmente una forma canónica de Brunovsky. Además, en [10] se demuestra que el número de clases de isomorfismos feedback de sistemas lineales localmente Brunovsky con espacio de estados X (proyectivo finitamente generado) es igual al número de soluciones de la siguiente ecuación diofántica

$$X \simeq Z_1 \oplus Z_2^2 \oplus \cdots \oplus Z_s^s \tag{6.1}$$

en el monoide $(\mathbf{P}(R), \oplus)$ de R-módulos proyectivos finitamente generados. Este resultado traslada el problema al campo de la combinatoria y las particiones.

El objetivo de esta sección es responder, de forma explícita ,a la siguiente pregunta: '?Cuántos sistemas lineales de control *multi input* diferentes existen con un espacio de estados fijado X sobre diferentes tipos de anillos conmutativos? Denotaremos a este número por $fe_R(m)$ donde m denota la clase de isomorfismos del espacio de estados en $\mathbf{P}(R)$; es decir, $[X]$.

Primero responderemos a la pregunta cuando el anillo R es un producto finito de anillos $R \simeq R_1 \times \ldots \times R_t$ en términos de cada factor directo R_i. Además, en particular, estudiamos el número de isomorfismos feedback sobre el producto finito de anillos pro-

yectivamente triviales. A continuación, estudiamos los anillos de von Neumann regulares y demostramos que son anillos de Brunovsky, es decir, que sobre un anillo regular von Neumann cada sistema accesible es localmente Brunovsky y esta propiedad caracteriza esta clase de anillos. Además, si R es un anillo von Neumann regular noetheriano podremos calcular el número de sistemas lineales localmente Brunovsky (accesibles) isomorfos feedback sobre R. En particular, se incluyen en este caso los anillos de enteros modulares $R = \mathbb{Z}/l\mathbb{Z}$ donde l es libre de cuadrados. Finalmente, calculamos $fe_R(m)$ en el caso de trabajar sobre R siendo éste un dominio de Dedekind. En estos anillos, una aproximación combinatoria es dada y el número combinatorio $\nu(n,k)$ es introducido.

6.1.1. Anillos proyectivamente triviales.

A continuación mostramos los resultados obtenidos de la clasificación feedback de isomorfismos de sistemas lineales localmente Brunovsky sobre anillos proyectivamente triviales.

Definición 1. *R es un anillo proyectivamente trivial si todos los R-módulos proyectivos finitamente generados son libres. En el caso de que R sea conexo, la definición coincide con la dada en el Teorema IV. 49 de [56].*

Algunos ejemplos de anillos proyectivamente triviales son: cuerpos $\mathbb{K}$; anillos locales como $\mathbb{K}[[x_1,...,x_s]]$ o $\mathbb{Z}/p^r\mathbb{Z}$ donde p es primo; dominios de ideales principales como $\mathbb{Z}$ o $\mathbb{K}[x]$; anillos de polinomios como $\mathbb{K}[x_1,...,x_s]$ o $\mathbb{Z}[x_1,...,x_s]$; y el anillo de funciones reales continuas $\mathcal{C}(K)$ sobre espacios topológicos compactos K si K se retrae a un punto.

Observación 6.1.1. *Sea R un anillo proyectivamente trivial. Por Definición 1, el conjunto $\mathbf{P}(R)$ de clases de isomorfismos de R-módulos proyectivos finitamente generados es isomorfo al conjunto de los números naturales es decir, $\mathbf{P}(R) \simeq \mathbb{N}$.*

Notación. *Utilizamos la siguiente notación:*

1. *m denota la clase de isomorfimos de X en $\mathbf{P}(R)$.*
2. *$fe_R(m)$ es el número de clases de isomorfismos feedback de sistemas lineales localmente Brunovsky Σ con espacio de estados X sobre R.*

Lema 2. *Sea R un anillo proyectivamente trivial. Sea $\Sigma = (X, f, B)$ un sistema lineal localmente Brunovsky sobre R con X el espacio de estados de rango n. Entonces*

$fe_R(m)$ = número de soluciones de la ecuación (6.1) en el monoide abeliano $(\mathbf{P}(R), \oplus)$= particiones del entero $\mathrm{rk}(X)$.

6.1.2. Productos finitos de anillos.

A continuación mostramos los resultados obtenidos de la clasificación feedback de isomorfismos de sistemas lineales localmente Brunovsky sobre productos finitos de anillos.

Teorema 3. *Si $R \simeq R_1 \times \cdots \times R_t$ es un producto finito de anillos entonces tenemos una descomposición en idempotentes $Idem(R) \simeq Idem(R_1) \times \cdots \times Idem(R_t)$ y, por lo tanto, $\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times ... \times \mathbf{P}(R_t)$.*

Corolario 4. *Si R_i es un anillo proyectivamente trivial sobre R para $i = 1, \ldots, t$, entonces*

$$\mathbf{P}(R) \simeq \mathbf{P}(R_1) \times \ldots \times \mathbf{P}(R_t) \simeq \mathbb{N}^t.$$

Teorema 5. *Sea $R \simeq R_1 \times \ldots \times R_t$ un producto finito de anillos. Sea $\Sigma = (X, f, B)$ un sistema lineal localmente Brunovsky sobre R. Entonces*

$$fe_R(m) = fe_{R_1}(m_1) \cdot \ldots \cdot fe_{R_t}(m_t)$$

donde m denota la clase de isomorfismos del espacio de estados X en $\mathbf{P}(R)$ y m_i denota la clase de isomorfismos de $X \otimes_R R_i$ en $\mathbf{P}(R_i)$ para cada i.

Corolario 6. *Sea $R \simeq R_1 \times \ldots \times R_t$ un producto finito de anillos proyectivamente triviales. Sea $\Sigma = (X, f, B)$ un sistema lineal localmente Brunovsky sobre R con espacio de estados $X \simeq R^n$. Entonces $fe_R(m) = fe_R(n) = (p_{\mathbb{N}}(n))^t$ donde $p_{\mathbb{N}}(n)$ son las particiones del número natural n.*

Corolario 7. *Sea $R = \mathbb{Z}/l\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_t\mathbb{Z}$ un anillo con l libre de cuadrados, y p_i ideales primos. Sea Σ un sistema lineal sobre R con espacio de estados de rango n. Entonces $fe_{\mathbb{Z}/l\mathbb{Z}}(m) = fe_{\mathbb{Z}/l\mathbb{Z}}(n) = p_{\mathbb{N}}(n)^t$.*

Corolario 8. *Para el anillo $R = \mathbb{Z}/l\mathbb{Z} \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_t^{rt}\mathbb{Z}$, si consideramos Σ, un sistema lineal sobre R con espacio de estados de rango n, entonces $fe_{\mathbb{Z}/l\mathbb{Z}}(m) = fe_{\mathbb{Z}/l\mathbb{Z}}(n) = p_{\mathbb{N}}(n)^t$.*

Observación 6.1.2. *La clasificación feedback de sistemas regulares sobre $\mathbb{Z}/l\mathbb{Z}$ con l libre de cuadrados es ahora completa. En el caso de que l no sea libre de cuadrados, la clasificación no es completa porque hay sistemas accesibles que no son regulares.*

6.1.3. Anillos von Neumann regulares.

La clase de anillos von Neumann regulares han sido estudiados desde el marco de sistemas lineales de control, veáse [16], [72], [73], [74] y [75]. El primer ejemplo de anillo conmutativo von Neumann regular es $\mathbb{Z}/l\mathbb{Z}$ con $l = p_1 \dots p_t$ libre de cuadrados. Otro ejemplo de anillos von Neumann regulares son los anillos Booleanos, es decir, anillos $(\mathbb{B}, +, \cdot)$ tales que $b^2 = b$ para todo $b \in \mathbb{B}$. Estos anillos son muy útiles por sus aplicaciones.

Definición 9 (Definition I, cf.[36])**.** *Un anillo R es un anillo conmutativo von Neumann regular si verifica que para cada $x \in R$ existe $y \in R$ tal que $xyx = x$.*

Obsérvese que los anillos von Neumann regulares R son llamados anillos absolutamente planos por Bourbaki (§2, Ex. 17, [4]) porque cada R-módulo es plano. Además un anillo von Neumann regular R tiene dimensión de Krull igual a cero y es reducido (Teorema 3.71, [51]).

Teorema 10. *(Un Teorema Local de Brunovsky.) Sea R un anillo conmutativo von Neumann regular con $1 \neq 0$. Sea $\Sigma = (X, f, B)$ un sistema lineal sobre R con X un R-módulo finito generado. Entonces es equivalente:*

1. *Σ es accesible.*

2. *Σ es un sistema localmente Brunovsky.*

Teorema 11. *(Anillos localmente Brunovsky.) Sea R un anillo conmutativo con $1 \neq 0$. Sea Σ un sistema lineal sobre R. Entonces es equivalente:*

i) R es un anillo von Neumann regular.

ii) Σ es accesible si y sólo si es localmente Brunovsky donde X es un R-módulo finitamente generado.

A continuación calculamos el número de clases de isomorfimos feedback de sistemas lineales localmente Brunovksy con espacio de estados el R-módulo de rango n, X, sobre anillos conmutativos noetherianos von Neumann regulares.

Theorem 6.1.3. *Sea R un anillo conmutativo con unidad, entonces las siguientes sentencias son equivalentes:*

i) R es un anillo noetheriano von Neumann regular.

ii) Existe un número finito de cuerpos $\mathbb{K}_i$ tales que $R \simeq \mathbb{K}_1 \times \ldots \times \mathbb{K}_t$.

Teorema 12. *Si R es un anillo conmutativo noetheriano von Neumann regular entonces el número de clases de sistemas lineales localmente Brunovsky sobre R con espacio de estados $X \simeq R^n$ es*

$$fe_R(m) = fe_R(n) = [p_{\mathbb{N}}(n)]^{\#Spec(R)}$$

Lema 13. *Los anillos $R = \mathbb{Z}/l\mathbb{Z}$ con $l = p_1 \cdots p_t$ libre de cuadrados y p_i primos diferentes son anillos von Neumann regulares.*

Observación 6.1.4. *Si $R = \mathbb{Z}/l\mathbb{Z}$ con $l = p_1 \cdots p_t$ libre de cuadrados es un anillo noetheriano von Neumann regular entonces cada sistema accesible es localmente Brunovsky, por tanto, $p_{\mathbb{N}}(n)^t$ es el número de clases de sistemas accesibles y sistemas lineales localmente Brunovsky con espacio de estados $X \simeq R^n$.*

Observación 6.1.5. *Si no imponemos la hipótesis de noetheraniedad entonces pueden existir infinitas clases de isomorfimos de sistemas lineales accesibles (localmente Brunovsky) sobre anillos von Neumann regulares R con espacio de estados fijo.*

6.1.4. Dominios de Dedekind.

Después de los anteriores casos, el siguiente paso es estudiar la clasificación feedback de sistemas lineales localmente Brunovsky sobre dominios de Dedekind. Obsérvese que estos anillos son de interés tanto en álgebra lineal como en teoría de sistemas lineales porque pertencen a la clase de anillos BCS, [80], que son la clase conocida más grande de anillos PA (anillos conmutativos donde la accesibilidad y la controlabilidad asintótica son equivalentes, [7]).

Para poder calcular el número de soluciones de la ecuación (6.1) para sistemas lineales localmente Brunovsky Σ sobre dominios de Dedekind primero enunciaremos algunos resultados elementales sobre este tipo de anillos.

En esta subsección R denota un dominio de Dedekind con cuerpo de fracciones $\mathbb{K}(R)$; es decir, un dominio conmutativo (sin divisores de cero) que es noetheriano, íntegramente cerrado y 1-dimensional.

Proposición 14 (cf. I.3.4,[82])**.** *Sea R un anillo conmutativo noetheriano 1-dimensional. Entonces todo R-módulo proyectivo finitamente generado P queda completamente clasificado por su rango, $rank(P) = \dim(P \otimes \mathbb{K}(R))$, y su determinante (un fibrado de línea*

sobre R), $\wedge^{\mathrm{rank}(P)}P$*. En particular, cada R-módulo proyectivo finitamente generado P de rank* ≥ 1 *es isomorfo a* $R^{\mathrm{rk}(P)-1} \oplus \wedge^{\mathrm{rk}(P)}P$*.*

Proposición 15 (cf. *I*§3 [82])**.** *Sea R un anillo conmutativo. Sea* $\mathrm{Pic}(R)$ *el conjunto de clases de isomorfimos de fibrados de línea sobre R (R-módulos proyectivos finitamente generados de rank* $= 1$*). Entonces* $(\mathrm{Pic}(R), \otimes_R)$ *es un grupo abeliano con* $R = 1_{\mathrm{Pic}(R)}$ *y* $P^{-1} = \mathrm{Hom_R(P, R)}$*.*

Proposición 16 (Capítulo VII, §4.,10, Corolario, [4])**.** *Sea R un dominio de Dedekind. Sea P un R-módulo finitamente generado con* $rank(P) = n$*. Entonces* $P \simeq T(P) \oplus M$ *donde* $T(P)$ *es el submódulo de torsión de P y con* $M \simeq R^n$*.*

Observación 6.1.6. *Sea P un R-módulo finitamente generado. La proposición anterior implica que sobre un dominio de Dedekind si* $rank(P) = 0 \Rightarrow det(P) = R$*.*

Proposición 17. *Sea R un dominio de Dedekind. Entonces,*

$$\mathbf{P}(R) \simeq [\mathbb{N}^+ \times Pic(R)] \cup \{0\}$$

Observación 6.1.7. *Sea X un R-módulo proyectivo finitamente generado. Buscar el número de clases de isomorfismos feedback de sistemas lineales localmente Brunovsky sobre R con espacio de estados X es lo mismo que calcular el número de soluciones de la siguiente ecuación*

$$X = Z_1 \oplus Z_2^2 \oplus \cdots \oplus Z_s^s \tag{6.2}$$

en $\mathbf{P}(R) \cong [\mathbb{N}^+ \times Pic(R)] \cup \{0\}$*. Estas soluciones están determinadas por las soluciones de*

$$rank(X) = rank(Z_1) + 2rank(Z_2) + \ldots + srank(Z_s) \text{ in } (\mathbb{N}, +) \tag{6.3}$$

junto con las de

$$\det(X) = \det(Z_1) \otimes \det(Z_2)^{\otimes 2} \otimes \cdots \otimes \det(Z_s)^{\otimes s} \text{ in } Pic(R). \tag{6.4}$$

Por la Observación 6.1.6 debemos darnos cuenta de que las soluciones de la ecuación (2.8) en $Pic(R)$ *dependen de las soluciones de la ecuación de los rangos en* $\mathbb{N}$*.*

Observación 6.1.8. *Obsérvese que si sólo fijamos el rango del espacio de estados,* $rk(X) = n$*, entonces* $X \cong R^{n-1} \oplus L$ *y*

$$\det(X) = \det(R^{n-1} \oplus L) = \wedge^n(R^{n-1} \oplus L) = \bigoplus_{i=0}^{n}[(\wedge^i R^{n-1}) \otimes (\wedge^{n-i} L)] =$$

$$= \bigoplus_{i=0}^{n-2} [R^{\binom{n-1}{i}} \otimes 0] \oplus [(\wedge^{n-1} R^{n-1}) \otimes (\wedge^1 L)] \oplus [\wedge^n R^{n-1} \otimes \wedge^0 L] = R \otimes L = L$$

y la ecuación (6.4) se convierte en

$$L = \det(Z_1) \otimes \det(Z_2)^{\otimes 2} \otimes \cdots \otimes \det(Z_n)^{\otimes n} \tag{6.5}$$

Recuperamos a continuación al Teorema de estructura de los grupos finitos abelianos que nos facilitará el cálculo de las soluciones de la ecuación (6.4) sobre los determinantes.

Proposición 18 (cf.Teorema 7, [21])**.** *Dado un grupo abeliano G, existe un dominio de Dedekind R tal que $Pic(R) \cong G$.*

Observación 6.1.9. *Sea $\mid Pic(R) \mid = p$ el orden de $Pic(R)$ con p primo. Por la anterior proposición tenemos el isomorfimo*

$$(Pic(R),\ \otimes) \xrightarrow{\overset{\alpha}{\cong}} (\mathbb{Z}/p\mathbb{Z}, +)$$

$$L \quad \mapsto \quad \alpha(L)$$

donde, en particular, $\alpha(R) = \overline{0}$ en $\mathbb{Z}/p\mathbb{Z}$

Para resolver las ecuaciones (6.3) y (6.4) introducimos los siguientes números combinatorios.

Definición 19. *Sea n un entero positivo y $1 \leq k \leq n$. Denotaremos por $\nu(n,k)$ el conjunto de las particiones del entero n en k sumandos diferentes. Además denotamos por $\nu(n,k)$ su cardinal.*

Ejemplo 6.1.10. *Como ejemplo podemos estudiar $\nu(5,1)$; esto es el número de particiones del entero 5 en 1 sumandos diferentes y $\nu(5,2)$; es decir, el número de particiones del entero 5 en 2 sumandos diferentes.*

Caso $n = 5$, $k = 1 \Rightarrow \nu(5,1) = 2$, *veáse Tabla 6.1.*

Partición	Diagrama de Young
5=1+1+1+1+1	
5=5	

Table 6.1: $\nu(5,1)$ *Particiones*

Caso $n = 5,\ k = 2 \Rightarrow \nu(5,2) = 5$. *Veáse Tabla 6.2.*

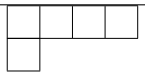
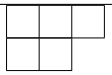
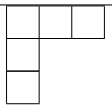
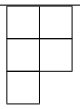
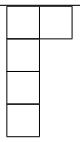
Partición	Diagrama de Young
5=4+1	
5=3+2	
5=3+ 1+1	
5=2+2 +1	
5=2+ 1+1+1	

Table 6.2: $\nu(5,2)$ *Particiones.*

Podemos comprobar que $\nu(5,1) + \nu(5,2) = p_{\mathbb{N}}(5) = 7$.

Definición 20. *Sea* p *un número primo. Denotaremos por* $\nu(n,k,p)$ *el conjunto de particiones en* $\nu(n,k)$ *donde todos los coeficientes de los sumandos son múltiplos de* p. *Además denotamos por* $\nu(n,k,p)$ *su cardinal. Por conveniencia denotaremos por* $\nu'(n,k,p) = \nu(n,k) - \nu(n,k,p)$.

Ejemplo 6.1.11. *Como ejemplo* $\nu(6,2)$ *es el número de particiones del entero* 6 *en* 2 *sumandos diferentes que contiene exactamente las particiones*

$$(51), (42), (411), (3111), (2211), (21111)$$

y entonces $\nu(6,2) = 6$. *Ahora* $\nu(6,2,2) = 1$ *porque la única partición en* $\nu(6,2)$ *con la propiedad de que todos los sumandos son múltiplos de* 2 *es* (42) .

Observación 6.1.12. *Aunque el número combinatorio* $\nu(n,k)$ *necesita de un estudio más profundo podremos utilizar las siguientes propiedades*

(i) $\nu(n,1) = div(n)$*; es decir,* $\nu(n,1)$ *es igual al número de divisores (incluyendo* 1 *y* n*) del entero* n.

(ii) *Si* $n < k(k+1)/2$ *entonces* $\nu(n,k) = 0$ *porque la partición más pequeña que uno puede formar con* k *sumandos diferentes es* $(k, k-1, ..., 2, 1)$ *y entonces es necesario que* $n \geq 1 + 2 + \cdots + k = \frac{k(k+1)}{2}$.

(iii) $\nu(n,1) + \nu(n,2) + \ldots = p_{\mathbb{N}}(n)$

A continuación exponemos nuestro resultado principal sobre dominios de Dedekind:

Teorema 21. *Sea* R *un dominio de Dedekind y sea* $Pic(R)$ *su grupo de Picard. Entonces, el número de clases de isomorfimos feedback de sistemas lineales localmente Brunovsky* $\Sigma = (X, f, B)$ *sobre* R *es calculado como sigue:*

(i) $fe_R(m)$ *es el número de soluciones* $(Z_1, Z_2, \ldots, Z_s)$ *del siguiente sistema de ecuaciones en* $\mathbb{N}$ *y* $Pic(R)$.

$$\begin{cases} rank(X) = rank(Z_1) + 2rank(Z_2) + \cdots + srank(Z_s) \\ \\ \det(X) = \det(Z_1) \otimes \det(Z_2)^{\otimes 2} \otimes \cdots \otimes \det(Z_s)^{\otimes s} \end{cases} \tag{6.6}$$

Para los siguientes items fijaremos el rango del espacio de estados, $rk(X) = n$.

(ii) *Si* $\mid Pic(R) \mid = \infty$ *entonces* $fe_R(m) = \infty$.

(iii) *Si* $\mid Pic(R) \mid = d < \infty$ *entonces* $fe_R(m) = \sum_{k=1}^{n} \nu(n,k) \cdot d^k$ *donde* d *no es primo.*

(iv) *Si* $\mid Pic(R) \mid = p$ *es primo entonces* $fe_R(R^n) = \sum_{k=1}^{n} \left[\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^{k-1}\right]$.

(v) *Si* $\mid Pic(R) \mid = p$ *es primo entonces* $fe_R(R^{n-1} \oplus L) = \sum_{k=1}^{n} \nu'(n,k,p) \cdot p^{k-1}$

Observación 6.1.13. *Si realizamos la suma de todos los cálculos sobre los posibles elementos de* $Pic(R)$*, entonces podemos mostrar la coherencia de nuestra fórmula*

$$\sum_{L \in Pic(R)} fe_R(R^{n-1} \oplus L) = \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^{k-1}\right) + (p-1) \cdot \sum_{k=1}^{n} \nu'(n,k,p) \cdot p^{k-1} =$$

$$= \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + p \cdot \nu'(n,k,p) \cdot p^{k-1}\right) = \sum_{k=1}^{n} \left(\nu(n,k,p) \cdot p^k + \nu'(n,k,p) \cdot p^k\right) =$$

$$= \sum_{k=1}^{n} \left(\nu(n,k,p) + \nu'(n,k,p)\right) \cdot p^k = \sum_{k=1}^{n} \nu(n,k) \cdot p^k.$$

6.2. Familias de códigos convolucionales sobre anillos finitos.

La teoría de la codificación se desarrolla en un contexto donde la mejora de la comunicación es necesaria. Los códigos convolucionales fueron introducidos por Peter Elias in 1955. En [23], él utilizó una matriz polinómica $G(z)$ en el proceso de codificación permitiendo generar un código online sin usar un buffering previo. La primera aproximación teórica algebraica de código convolucional fue dada por Forney en [25] donde desarrolló la relación entre las matrices $n \times k$ sobre el cuerpo de funciones racionales sobre un cuerpo y los códigos convolucionales. Además, él explicó que el término *convolucional* es utilizado porque las secuencias de salida pueden ser consideradas como la convolución de las secuencias de entrada con las secuencias del codificador ([28]).

Muchas propiedades de un código convolucional son estudiadas mediante sus parámetros (tasa, longitud constante y complejidad). En ese sentido, la investigación en teoría de códigos convolucionales está enfocada a la construcción de códigos convolucionales con una determinada tasa, complejidad, y una libre distancia de Hamming adecuada. Además, los códigos convolucionales están estrechamente relacionados con otras áreas de matemáticas que nos permiten estudiarlos desde diferentes puntos de vista como el álgebra, la combinatoria o la geometría algebraica, por ejemplo. En este sentido, en [70], [71] y [83] se desarrolló la relación existente entre códigos convolucionales y teoría de sistemas dinámicos lineales. Rosenthal *et al* propusieron un algoritmo de decodificación basado en la descripción del código como sistema de control I/S/O (input/state/output). Más recientemente, otros autores han estudiado códigos convolucionales utilizando herramientas de teoría de control, poniendo especial énfasis en el problema de controlabilidad y observabilidad (veáse [26], [27], [28],[29], [42], [59], [60] y [61]).

Además, en avances recientes en teoría de la codificación se están estudiando códigos multidimensionales mediante herramientas de controlabilidad, veáse [31], [34], [45] y [84].

Pero, a veces, trabajar con cuerpos finitos es demasiado restrictivo, y éste es el motivo de estudiar códigos convolucionales sobre anillos. La primera aproximación a los códigos convolucionales sobre anillos fue dada por Massey y Mittelholzer en [53] y [54]. Por otra parte, la extensión a códigos convolucionales sobre anillos trae nuevas dificultades pero ofrecen determinadas propiedades en el modelado de determinados comportamientos

dinámicos como los diagramas de fase.

Nuestro objetivo es poder generalizar la relación entre códigos convolucionales y sistemas sobre anillos conmutativos. Basándonos en el estudio realizado en [19] sobre códigos de bloque, en esta sección se resuelven las siguientes cuestiones:

1. ¿Podemos definir una familia de códigos convolucionales sobre R siendo R un anillo conmutativo?

2. Dada una familia de códigos convolucionales $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ con $\mathbb{F}_j$ un cuerpo finito para $j = 1, \ldots, t$, ¿existen ternas de matrices (K, L, M) sobre R que podamos considerar una representación mínima de primer orden de la familia?

3. Además, ¿existen matrices A, B, C y D que nos permiten obtener una representación de espacios de estados controlable de una familia de códigos convolucionales?

4. ¿Cuáles son las propiedades de los ítems anteriores?

6.2.1. Familias de códigos convolucionales sobre anillos conmutativos.

En primer lugar damos una definición consistente de familia de códigos convolucionales sobre un anillo conmutativo con unidad que generalice para el caso de que el anillo sea un cuerpo finto. Esta definición es válida para todo anillo conmutativo con unidad.

Sea R un anillo conmutativo con unidad. Primero damos algunas aclaraciones de notación:

Notación. *1. Denotaremos por $S = Spec(R)$, $\mathbb{A}^1_S = Spec(R[z])$ y $e : R \hookrightarrow R[z]$ la inclusión canónica. Además utilizaremos la notación e para el morfismo inducido entre espectros, $e : \mathbb{A}^1_S \to S$.*

2. Para cualquier ideal primo $\mathfrak{p} \in R$ denotaremos $k(\mathfrak{p}) = R/\mathfrak{p}R$ el cuerpo residual.

3. Sea M un $R[z]$-módulo finitamente generado. Sea $\mathfrak{p}$ un ideal primo de R. Denotaremos $M(\mathfrak{p})$ el $k(\mathfrak{p})[z]$-módulo $M/(\mathfrak{p}M)$.

Definición 22. *Un código convolucional (n, k) sobre R es un submódulo $\mathfrak{C}_R \subset R[z]^n$ tal que $R[z]^n/\mathcal{C}$ es R-plano y $rk(\mathcal{C})(\mathfrak{p}) = k$ para cualquier ideal primo.*

Observación 6.2.1. *Obsérvese que la condición de platitud asegura que para cualquier ideal primo* $\mathfrak{p} \subset R$ *el* $k(\mathfrak{p})[z]$*-módulo* $\mathcal{C}(\mathfrak{p})$ *es aún un submódulo* $\mathcal{C}(\mathfrak{p}) \subset k(\mathfrak{p})[z]^n$ *y, por tanto, un* (n, k) *código convolucional en el sentido clásico.*

La anterior observación nos permite interpretar un código convolucional sobre R como una familia de códigos convolucionales, uno sobre cada punto $\mathfrak{p} \in S$. Antes, veamos las definiciones de codificador y complejidad para un código convolucional sobre R.

Definición 23. *Sea* $\mathcal{C}(\mathfrak{p})$ *un código convolucional sobre* $k(\mathfrak{p})[z]^n$ *donde* $\mathfrak{p}$ *es un ideal primo. Consideraremos el grado del código convolucional* $\delta(\mathcal{C}(\mathfrak{p})) = \delta(\mathfrak{p})$*. Diremos que una familia de códigos convolucionales* $\mathfrak{C}_R$ *tiene grado* δ *si* $\delta(\mathfrak{p}) = \delta$ *para todo* $\mathfrak{p}$*.*

Observación 6.2.2. *A partir de este momento, trabajaremos con familias de códigos convolucionales* $\mathfrak{C}_R$ *con grado* $\delta(\mathfrak{C}_R) = \delta$*.*

Definición 24. *La matriz generadora* $G(z)$ *de una* (n, k) *familia de códigos convolucionales* $\mathfrak{C}_R$ *sobre* R *es una aplicación*

$$G(z) : R[z]^l \longrightarrow R[z]^n$$

$$u(z) \mapsto v(z) = G(z) \cdot u(z)$$

tal que $Im\ G(z) = \mathfrak{C}_R$*.*

Definición 25. *Un codificador* $G(z)$ *de una* (n, k) *familia de códigos convolucionales* $\mathfrak{C}_R$ *sobre* R *es una matriz generadora con* $l = k$ *y* $G(z)$ *inyectiva.*

Desde este punto consideraremos el anillo $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ donde $\mathbb{F}_j$ es un cuerpo finito para cada $j = 1, \ldots, t$. Como fijamos el anillo $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$, denotaremos por $\mathfrak{C} \equiv \mathfrak{C}_R$ para simplificar la notación.

Si consideramos $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ donde $\mathbb{F}_j$ es un cuerpo finito para $j = 1, \ldots t$, entonces un código convolucional sobre R nos da una familia de códigos convolucionales, $\mathfrak{C}$, uno sobre cada cuerpo residual mediante $\{\mathfrak{C} \otimes_R R/\mathfrak{m}\}_{\mathfrak{m} \in max(R)}$. En el anillo R la construcción inversa es posible. Para $\mathcal{C}_\mathfrak{m}$ sobre $R/\mathfrak{m}\ \forall\ \mathfrak{m}$ existe un único código convolucional sobre R tal que $\mathfrak{C} \otimes R/\mathfrak{m} = \mathcal{C}_\mathfrak{m}$.

Sea $\mathfrak{C} \subset R[z]^n$ una familia de códigos convolucionales. Denotaremos por $\mathcal{C}_j$ la restricción de $\mathfrak{C}$ sobre cada $\mathbb{F}_j[z]$, es decir, $\mathcal{C}_j = \mathfrak{C} \otimes_{R[z]} \mathbb{F}_j[z]$. Para cada j, tenemos la aplicación sobreyectiva

$$\varphi_j : R[z]^n \to \mathbb{F}_j[z]^n$$

$$\mathfrak{C} \longmapsto \mathcal{C}_j$$

Por lo tanto, todo $\mathcal{C}_j$ puede ser considerado como $R[z]$-módulo vía φ_j y $\mathfrak{C} = \bigoplus_{j=1}^{t} \mathcal{C}_j$.

6.2.2. Propiedades de una familia de códigos convolucionales.

Sea el anillo $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ con $\mathbb{F}_i$ un cuerpo finito para $i = 1, \ldots, t$.

Definición 26. *Sea $\mathfrak{C} \subset R[z]^n$ una familia de códigos convolucionales sobre R. Diremos que $\mathfrak{C}$ es observable si y sólo si $R[z]^n/\mathfrak{C}$ es plano sobre $R[z]$.*

Sea $\mathfrak{C}$ una familia de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times ... \times \mathbb{F}_t$ con $\mathbb{F}_j$ un cuerpo finito para $j = 1, \ldots, t$.

Proposición 27. *$\mathfrak{C}$ es observable $\Leftrightarrow$ $\mathcal{C}_j$ es observable $\forall$ j.*

Además las familias de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ donde $\mathbb{F}_j$ es un cuerpo finito para cada $j = 1, \ldots, t$ verifican las propiedades de códigos sistemáticos, propios y básicos dadas en [54].

6.2.3. Representaciones de primer orden de familias de códigos convolucionales sobre anillos finitos.

A continuación realizamos un breve resumen sobre los resultados que nos permiten calcular una representación mínima de primer orden para familias de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ con $\mathbb{F}_j$ un cuerpo finito para cada j.

Sea $\mathfrak{C}$ una familia de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Necesitamos dar un resultado algebraico previo para poder construir una representación mínima de primer orden de una familia de códigos convolucionales $\mathfrak{C}$.

Proposición 28. *Sea R un anillo conmutativo con unidad. Sea (K, L, M) una terna de matrices tales que $K, L \in \mathcal{M}_{(\delta+n-k)\times\delta}(R)$ y $M \in \mathcal{M}_{(\delta+n-k)\times n}(R)$. Si consideramos el núcleo del pencil $(zK + L \mid M)$ definido de la siguiente manera*

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

entonces la siguiente sucesión es exacta

$$0 \longrightarrow Ker(zK+L) \longrightarrow Ker(zK+L,M) \longrightarrow Ker(zK+L \mid M) \longrightarrow 0$$

Observación 6.2.3. *Si $R = \mathbb{F}$ entonces $Ker(zK+L \mid M)$ se corresponde con un código convolucional $\mathcal{C}$ como submódulo de $\mathbb{F}[z]^n$ mediante representaciones de primer orden en el sentido de [83].*

Construimos a continuación la representación de primer orden de $\mathfrak{C}$. Consideramos el anillo conmutativo $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ donde $\mathbb{F}_j$ es un cuerpo finito para $j = 1, \ldots, t$. Como $\mathfrak{C} = \bigoplus_{j=1}^{t} \mathcal{C}_j$, cada $\mathcal{C}$ sobre $\mathbb{F}_j$ tiene una representación de primer orden (K_j, L_j, M_j).

Notación. *Sea μ la aplicación $\mu : R \longrightarrow \mathbb{F}_j$. Para aclarar la notación, denotaremos por $\mu_j(R) = R \otimes_R \mathbb{F}_j$ y en términos de matrices denotamos por $\mu_j(A) = A \otimes 1 = A_j$ la restricción de A módulo $\mathbb{F}_j$.*

Las matrices (K, L, M) que son construidas mediante la aplicación μ_j de la forma $\mu_j(K) \simeq K_j$, $\mu_j(L) \simeq L_j$ y $\mu_j(M) \simeq M_j$ donde (K_j, L_j, M_j) son representaciones de primer orden $\mathcal{C}_j \subseteq \mathbb{F}_j[z]^n$ para cada $\mathbb{F}_j$.

Las matrices (K, L, M) que obtenemos de la forma anteriormente descrita son una representación de primer orden de la familia de códigos convolucionales $\mathfrak{C}$ sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$.

Teorema 29. *Teorema de Realización: Existencia. Suponemos que $\mathcal{C} \subseteq R^n[z]$ es una (n,k) familia de códigos conolvuionales de complejidad o grado δ. Entonces, las matrices $K, L \in \mathcal{M}_{(\delta+n-k)\times\delta}(R)$ y $M \in \mathcal{M}_{(\delta+n-k)\times n}(R)$ satisfacen que la familia de códigos convolucionales viene descrita por $\mathcal{C} = Ker(zK+L \mid M)$.*

Además, las matrices $(K \mid L \mid M)$ verifican las siguientes condiciones de minimalidad

1. *K tiene rango por columnas máximo .*
2. *$(K \mid M)$ tiene rango por filas máximo.*
3. *La aplicación $(zK+L \mid M)$ definida por*

$$(zK+L \mid M) : R[z]^{\delta+n} \to R[z]^{\delta+n-k}$$

es sobreyectiva.

Observación 6.2.4. *Obsérvese que el Teorema 29 implica que si (K, L, M) es una representación de primer orden de $\mathcal{C}$ entonces (K_j, L_j, M_j) es una representación de primer orden para cada $\mathcal{C}_j$.*

Teorema 30. *Teorema de Realización II: Unicidad.*

Las matrices K, L y M sobre R son únicas en el siguiente sentido: si $(\widehat{K}, \widehat{L}, \widehat{M})$ satisface las condiciones de minimalidad del Teorema 29, entonces existen matrices invertibles únicas T y S sobre R tal que

$$(\widehat{K}, \widehat{L}, \widehat{M}) = (TKS^{-1}, TLS^{-1}, TM)$$

6.2.4. Representaciones I/S/O de una familia de códigos convolucionales sobre anillos finitos.

Sea R el anillo $R \simeq \mathbb{F}_1 \times \ldots \mathbb{F}_t$. Sea $\mathfrak{C}$ una familia de códigos convolucionales sobre R tal que $\mathfrak{C} \simeq \bigoplus_{j=1}^{t} \mathcal{C}_j$. Sean (K_j, L_j, M_j) las t representaciones de primer orden de los códigos convolucionales $\mathcal{C}_j$ sobre cada $\mathbb{F}_j$. Por [83] podemos hacer transformaciones elementales sobre las matrices (K_j, L_j, M_j) y obtener una terna de matrices $(\mathcal{K}_j, \mathcal{L}_j, \mathcal{M}_j)$ tales que

$$\mathcal{K}_j = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, \mathcal{L}_j = \begin{pmatrix} A_j \\ C_j \end{pmatrix} \text{ and } \mathcal{M}_j = \begin{pmatrix} O & B_j \\ -I_{(n-k)} & D_j \end{pmatrix} \tag{6.7}$$

donde las matrices $A_j \in \mathcal{M}_{\delta\times\delta}(\mathbb{F}_j)$, $B_j \in \mathcal{M}_{\delta\times k}(\mathbb{F}_j)$, $C_j \in \mathcal{M}_{(n-k)\times\delta}(\mathbb{F}_j)$ y $D_j \in \mathcal{M}_{(n-k)\times k}(\mathbb{F}_j)$ son representaciones I/S/O (input-state-output) de cada código convolucional $\mathcal{C}_j$.

Observación 6.2.5. *1. Las matrices (K_j, L_j, M_j) y $(\mathcal{K}_j, \mathcal{L}_j, \mathcal{M}_j)$ son representaciones de primer orden del mismo código convolucional $\mathcal{C}_j$ para cada j y entonces $Ker(zK_j + L_j \mid M_j) \simeq Ker(z\mathcal{K}_j + \mathcal{L}_j \mid \mathcal{M}_j)\ \forall\ j$.*

Podemos construir sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ y desde (K_j, L_j, M_j) la terna de matrices (K, L, M) que es una representación de primer orden de $\mathfrak{C}$ y entonces podemos obtener una representación I/S/O de $\mathfrak{C}$.

Teorema 31. *Sea $\mathfrak{C}$ una familia de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \mathbb{F}_t$. Sea (K, L, M) una representación de primer orden de $\mathfrak{C}$. Entonces*

i) Podemos hacer transformaciones elementales sobre (K, L, M) *y obtener una terna de matrices* $(\mathcal{K}, \mathcal{L}, \mathcal{M})$ *tales que*

$$\mathcal{K} = \begin{pmatrix} -I_\delta \\ O \end{pmatrix}, \mathcal{L} = \begin{pmatrix} A \\ C \end{pmatrix} \text{ and } \mathcal{M} = \begin{pmatrix} O & B \\ -I_{(n-k)} & D \end{pmatrix} \tag{6.8}$$

donde $A \in \mathcal{M}_{\delta\times\delta}(R)$, $B \in \mathcal{M}_{\delta\times k}(R)$, $C \in \mathcal{M}_{(n-k)\times\delta}(R)$ *y* $D \in \mathcal{M}_{(n-k)\times k}(R)$.

ii) Además, la terna de matrces obtenida en i) verifica que

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

Las matrices A, B, C y D sobre R obtenidas desde (6.8) son una representación I/S/O de $\mathfrak{C}$, la familia de códigos convolucionales sobre R, esto es, define una representación de sistema lineal de espacio de estados controlable desde

$$\mathfrak{C} = \{v(z) \in R[z]^n \mid \exists x(z) \in R[z]^\delta \text{ tal que } (zK + L)x(z) + Mv(z) = 0\} \tag{6.9}$$

a

$$\begin{cases} x_{t+1} = Ax_t + Bu_t \\ y_t = Cx_t + Du_t \\ v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \ x_0 = 0, \ \exists\gamma : x_{\gamma+1} = 0. \end{cases} \tag{6.10}$$

donde x_t es el n-vector de estados, y_t es el p-vector de salidas y u_t el m-vector de control. Además damos un estado inicial $x_{t_0} = x_0$ a tiempo t_0.

Proposición 32. *Sea* $\mathfrak{C}$ *una familia de códigos convolucionales sobre* $R \simeq \mathbb{F}_1 \times \ldots \mathbb{F}_t$. *Las matrices* (A, B, C, D) *sobre* R *obtenidas desde (6.8) y que conforman una representación I/S/O de* $\mathfrak{C}$ *pueden ser construidas desde el conjunto de matrices* (A_j, B_j, C_j, D_j) *sobre* $\mathbb{F}_j$, *las representaciones I/S/O de los t códigos convolucionales sobre* $\mathbb{F}_j$.

Ejemplo 6.2.6. *En este ejemplo partimos de dos códigos convolucionales y sus codificadores. El primero,* $\mathcal{C}_1$, *sobre* $\mathbb{Z}/2\mathbb{Z}$ *y el segundo,* $\mathcal{C}_2$, *sobre* $\mathbb{Z}/3\mathbb{Z}$. *Calculamos a continuación las representaciones de primer orden de I/S/O de cada uno de ellos.*

Consideramos el codificador de $\mathcal{C}_1$ *sobre* $\mathbb{Z}/2\mathbb{Z}$

$$G_1(z) = \begin{pmatrix} z-1 & 1 \\ z^2+1 & 0 \\ z^2+1 & z+1 \end{pmatrix}$$

Las matrices K_1, L_1 y M_1 son una representación de primer orden de $\mathcal{C}_1$.

$$K_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, L_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \text{ y } M_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

A partir de esta terna de matrices, calculamos las matrices A_1, B_1, C_1 y D_1, mediante las que podemos obtener el sistema dinámico lineal asociado.

$$A_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, B_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, C_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \text{ y } D_1 = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Consideramos ahora el codificador de $\mathcal{C}_2$ sobre $\mathbb{Z}/3\mathbb{Z}$.

$$G_2(z) = \begin{pmatrix} z & -1 \\ 1 & z-1 \\ -z^2+z-1 & 0 \end{pmatrix}$$

La representación de primer orden K_2, L_2 y M_2 es

$$K_2 = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}, L_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ y } M_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Entonces la representación I/S/O es

$$A_2 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}, B_2 = \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 1 & 0 \end{pmatrix}, C_2 = \begin{pmatrix} 0 & 1 & -1 \end{pmatrix}, \text{ y } D_2 = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Obtendremos ahora las correspondientes matrices (A, B, C, D) sobre $\mathbb{Z}/6\mathbb{Z}$ pegando *las matrices (A_1, B_1, C_1, D_1) y (A_2, B_2, C_2, D_2) y que conforman la I/S/O representación de la familia de códigos convolucionales $\mathfrak{C}$ sobre $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$*

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 5 & 4 & 0 \\ 2 & 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 3 & 2 \\ 1 & 3 \end{pmatrix}, C = \begin{pmatrix} 3 & 1 & 5 \end{pmatrix}, \text{ y } D = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Podremos entonces calcular las matrices K, L y M en $\mathbb{Z}/6\mathbb{Z}$ que son una representación de primer orden de la familia de códigos convolucionales $\mathfrak{C}$ sobre $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

$$K = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}, L = \begin{pmatrix} 0 & 1 & 0 \\ 5 & 4 & 0 \\ 2 & 0 & 1 \\ 3 & 1 & 5 \end{pmatrix} \text{ y } M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 1 & 3 \\ -1 & 0 & 0 \end{pmatrix} \tag{6.11}$$

Finalmente, podemos hallar el núcleo de $(zK+L \mid M)$ y obtener el codificador de la familia de códigos convolucionales $\mathfrak{C}$ sobr $\mathbb{Z}/6\mathbb{Z}$

$$G(z) = \begin{pmatrix} z+3 & 5 \\ 3z^2+1 & -2z+2 \\ -z^2+4z-1 & 3z-3 \end{pmatrix} \tag{6.12}$$

Obsérvese que el codificador $G(z)$ restringe a $\mathbb{Z}/2\mathbb{Z}$ obteniendo $G_1(z)$ y a $\mathbb{Z}/3\mathbb{Z}$ obteniendo $G_2(z)$.

Propiedades de las representaciones I/S/O de $\mathfrak{C}$.

Sea $\Sigma = (A, B, C, D)$ un sistema lineal sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$, que es una representación I/S/O obtenida mediante una representación de primer orden de una familia de códigos convolucionales, $\mathfrak{C}$, sobre R. Como el par (A, B) caracteriza la parte dinámica del sistema, denotaremos por $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ el comportamiento dinámico de la I/S/O.

Desde la anterior sección podemos considerar una representación I/S/O para cada código convolucional $\mathcal{C}_j$ sobre cada $\mathbb{F}_j$. Denotaremos sus dinámicas por $\Sigma_j^{\mathcal{C}_j} = (A_j, B_j)^{\mathcal{C}_j}$. Obsérvese que $\Sigma_j^{\mathcal{C}_j}$ es accesible (controlable desde el origen) para todo $j = 1, \ldots, t$.

Proposición 33. *Sea $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ la parte dinámica de una representación I/S/O de una familia de códigos convolucionales, $\mathfrak{C}$, sobre R. Entonces $\Sigma^{\mathfrak{C}}$ es un sistema lineal accesible sobre R.*

Proposición 34. *Sea $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ la parte dinámica de una representación I/S/O de una familia de códigos convolucionales, $\mathfrak{C}$. Entonces $\Sigma^{\mathfrak{C}}$ es un sistema lineal localmente Brunovsky sobre R.*

Construcción de familias observables de códigos convolucionales.

Por [83], si consideramos representaciones I/S/O accesibles y observables de códigos convolucionales sobre cuerpos finitos, entonces podemos construir códigos convolucionales observables mediante representaciones mínimas de primer orden. Generalizamos a continuación este resultado para representaciones I/S/O de familias de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$.

Proposición 35. *Sea $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Sea $(A, B, C, D)^{\mathfrak{C}}$ una representación I/S/O de $\mathfrak{C}$ obtenida mediante representaciones de primer orden. Si $(A, B)^{\mathfrak{C}}$ es observable entonces $\mathfrak{C}$ es una familia observable de códigos convolucionales sobre R.*

6.3. Equivalencia feedback entre códigos convolucionales y sistemas lineales.

Es bien sabido, veáse [83], que la parte dinámica de la representación IS/O de un código convolucional $\mathcal{C}$, denotada por $\Sigma^{\mathcal{C}} = (A, B)^{\mathcal{C}}$, sobre un cuerpo finito $\mathbb{F}$ forma un sistema accesible sobre $\mathbb{F}$. Como un cuerpo es un anillo de Brunovsky (veáse [11]), todo $\Sigma^{\mathcal{C}}$ es un sistema lineal de Brunovsky sobre $\mathbb{F}$. Como hemos dicho anteriormente, el problema de la clasificación feedback de sistemas lineales de Brunovsky sobre espacios vectoriales de dimensión finita es resuelto mediante formas canónicas de Brunovsky. Además, el número de isomorfismos feedback de sistemas lineales de Brunovsky (accesibles) se puede calcular mediante los índices de Kronecker del sistema $\kappa_1 \geq \ldots \geq \kappa_k$ siendo iguales a las particiones de la dimensión de la matriz A (el rango del espacio de estados del sistema). Los resultados anteriores implican que existe una relación clara entre representaciones de espacio de estados controlables de un código convolucional y sistemas lineales de Brunovsky. La clave en esta relación se encuentra en los invariantes de ambos tipos de sistemas bajo equivalencia feedback definidos por sus índices de Kronecker(o de controlabilidad) estudiados en [8], [44], [58] y [79].

Por otra parte y recientemente, la equivalencia feedback en códigos convolucionales ha sido utilizada por sus aplicaciones por la relación entre códigos convolucionales y teoría de sistemas mediante representaciones de primer orden bajo la clase de equivalencia GL_δ (veáse [26], [28],[29], [30], [33] y [70], por ejemplo).

Mediante una relación de equivalencia feedback entre códigos convolucionales y sus índices de Kronecker hemos podido establer una relación entre sistemas lineales de Brunovsky y representaciones de estado controlables de códigos convolucionales y familias de éstos.

Nuestros resultados de esta última parte muestran que no sólo la parte dinámica de una representación I/S/O es un sistema lineal de Brunovsky sobre $\mathbb{F}$, además, el número de clases feedback de códigos convolucionales; es decir, el número de clases feedback de partes dinámicas de una descripción I/S/O es igual al número de sistemas lineales de Brunovsky sobre $\mathbb{F}$.

En el caso de familias de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$, los resultados anteriores se verifican debido a que R es un anillo von Neumann regular noetheriano y, como hemos demostrado, cada sistema accesible es localmente Brunovsky. Además, el número de isomorfismos feedback de sistemas lineales localmente Brunovsky es igual al número de clases feedback de dinámicas de las I/S/O asociadas a familias de códigos convolucionales sobre R.

6.3.1. Invariantes de un código convolucional sobre un cuerpo finito.

Sea $\mathcal{C}$ un (n, k) código convolucional sobre $\mathbb{F}$. Consideramos los índices de Kronecker $\kappa_1 \geq \ldots \geq \kappa_k$ de cualquier codificador mínimo de $\mathcal{C}$. Además, consideramos el grado del código $\mathcal{C}$ definido por sis índices de Kronecker mediante $\delta = \sum_{i=1}^{k} \kappa_i$. El grado del código así como sus índices de Kronecker son invariantes del código.

Observación 6.3.1. *Podemos considerar un codificador mínimo del código convolucional y entonces los índices de Kronecker y los de Forney coinciden y, por lo tanto, el grado del código δ es igual que la complejidad de su encoder, c.*

Notación. *Denotaremos por $\mathfrak{K}^{\mathcal{C}}$ a la k-upla de índices de Kronecker de un (n, k) código convolucional, $\mathcal{C}$, sobre $\mathbb{F}$; es decir, $\mathfrak{K}^{\mathcal{C}} = (\kappa_1, \ldots, \kappa_k)$.*

Definiremos una relación feedback entre los códigos convolucionales en términos de sus índices de Kronecker.

Definición 36. *Sean $\mathcal{C}$ y $\overline{\mathcal{C}}$ códigos convolucionales sobre $\mathbb{F}$. La relación feedback sobre códigos convolucionales, $\overset{f.c.e}{\sim}$, definida por*

$$\mathcal{C} \overset{f.c.e}{\sim} \overline{\mathcal{C}} \Leftrightarrow \mathfrak{K}^{\mathcal{C}} = \mathfrak{K}^{\overline{\mathcal{C}}}$$

es una relación de equivalencia.

Lema 37. *El número de clases de equivalencia feedback de códigos convolucionales con el mismo grado δ es igual a las particiones del grado del código.*

$$\#\{ \text{ clases feedback equivalencias de } \mathcal{C} \ \} = p(\delta)$$

donde $p(\delta)$ denota las particiones del entero δ.

En el área de sistemas, los índices de Kronecker de un sistema dinámico sobre un espacio vectorial finito, $\mathbb{K}^n$, son conocidos como los índices de controlabilidad (accesibilidad) del par $\Sigma = (A, B)$ y estos índices son invariantes del sistema bajo equivalencia feedback: Si $\Sigma = (A, B)$ es un sistema dinámico lineal sobre un $\mathbb{K}$-espacio vectorial, por la descomposición de Kalman y el Teorema de Brunovsky, la clasificación feedback de sistemas lineales sobre $\mathbb{K}^n$ se reduce a la clasificación de sistemas accesibles. El número de sistemas accesibles equivalentes feedback puede ser calculado utilizando los índices invariantes de Kronecker $\kappa_1 \geq \kappa_2 \geq \cdots \geq \kappa_p$ del pencil$(zI - A, B)$ asociado a $\Sigma = (A, B)$.

Como las representaciones de primer orden de un código convolucional nos permiten calcular descripciones del código $\mathcal{C}$ mediante representaciones I/S/O, la relación entre los índices de controlabilidad del código y los de la I/S/O como sistema lineal dinámico es clara y viene dada por el siguiente teorema :

Teorema 38 (c.f. Theorem 2, [58].)**.** *Si $\Sigma = (A, B)$ forma un par controlable tal que $A \in \mathcal{M}_{\delta\times\delta}(\mathbb{F})$ y $B \in \mathcal{M}_{\delta\times k}(\mathbb{F})$, entonces existen enteros positivos $\kappa_1 \geq \ldots \geq \kappa_k$ (a menudo nos referiremos a estos índices como índices de controlabilidad del par (A, B)) que sólo dependen de las clases de equivalencia GL_δ de (A, B) teniendo las siguientes propiedades:*

1. *$\kappa_1 = \kappa$, índices de controlabilidad o de Kronecker del par (A, B).*
2. *$\sum_{i=1}^{k} \kappa_i = \delta$, la dimensión de la matriz A.*
3. *Existen matrices polinomiales $X(z), Y(z), U(z)$ verificando*

$$Ker \begin{bmatrix} zI - A & 0 & -B \\ -C & I & -D \end{bmatrix} = Im \begin{bmatrix} X(z) \\ Y(z) \\ U(z) \end{bmatrix}$$

y teniendo la propiedad de el grado de la i-ésima columna de $G(z) = \begin{pmatrix} Y(z) \\ U(z) \end{pmatrix}$ *es igual a* κ_i*, y el grado de la i-ésima columna def* $X(z)$ *es igual a* $\kappa_i - 1$ *para* $i = 1, \ldots, k$*.*

Como las representaciones I/S/O sobre cuerptos finitos nos permiten entender un código convolucional como $\mathcal{C} = Ker(zK + L \mid M) = Ker \begin{pmatrix} zI - A & 0 & -B \\ -C & I & -D \end{pmatrix}$, el Teorema 38 puede ser aplicado y los índices de controlabilidad de $\mathcal{C}$ son iguales a los índices de controlabilidad del par $\Sigma^{\mathcal{C}} = (A, B)^{\mathcal{C}}$, la parte dinámica de la representación I/S/O del código como sistema lineal sobre $\mathbb{F}$.

Observación 6.3.2. *En este trabajo nos referiremos a los índices de controlabilidad como los índices de Kronecker.*

Observación 6.3.3 (cf. [10])**.** *Los índices de Kronecker de un sistema lineal dinámico sobre* $\mathbb{F}$ *están en correspondencia biyectiva con los índices de Kronecker conjugados que son dados por* $(\xi_1, \xi_2, \ldots, \xi_p)$ *donde*

$$\xi_1 = rk(B)\ y$$

$$\xi_i = rk(B, AB, ..., A^{i-1}B) - rk(B, AB, ..., A^{i-2}B).$$

Estos índices conjugados ξ *clasifican el sistema.*

Denotaremos por $\xi^{\mathcal{C}}$ *como la k-upla de índices de Kronecker conjugados de la representación I/S/O de un* (n, k) *código convolucional* $\mathcal{C}$*, es decir,* $\xi^{\mathcal{C}} = (\xi_1, \ldots, \xi_k)$*.*

Proposición 39. *Sean* $\mathcal{C}$ *y* $\overline{\mathcal{C}}$ *códigos convolucionales sobre* $\mathbb{F}$*. Denotaremos por f.i la isomorfía feedback entre sistemas lineales accesibles (de Brunovsky). Entonces*

$$\mathfrak{K}^{\mathcal{C}} = \mathfrak{K}^{\overline{\mathcal{C}}} \Leftrightarrow \Sigma^{\mathcal{C}} \overset{f.i}{\simeq} \overline{\Sigma}^{\overline{\mathcal{C}}}$$

Proposición 40. *Sea* $\mathbb{F}$ *un cuerpo finito.*

$$\left\{ \begin{array}{c} \textit{Clases Feedback de} \\ \textit{las partes dinámicas de I/S/O's} \\ \textit{de códigos convolucionales} \\ \textit{over } \mathbb{F} \end{array} \right\} = \left\{ \begin{array}{c} \textit{Clases de isomorfimos Feedback de} \\ \textit{Sistemas Lineales de Brunovsky} \\ \textit{over } \mathbb{F} \end{array} \right\}$$

6.3.2. Invariantes de una familia de códigos convolucionales.

Sea $\mathfrak{C}$ una (n,k) familia de códigos convolucionales sobre $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Sea $\mathcal{C}_j$ el j-ésimo (n,k) código convolucional sobre $\mathbb{F}_j$ tal que $\mathcal{C}_j \simeq \mathfrak{C} \otimes_{R[z]} \mathbb{F}_j$.

Obsérvese que los resultados de la sección sobre cuerpos finitos se mantienen para los códigos convolucionales $\mathcal{C}_j$ para todo $j = 1, \ldots, t$ y, por tanto, $\xi^{\mathcal{C}_j} = \{(\xi_i^j)\}$ y $\mathfrak{K}^{\mathcal{C}_j} = \{(\kappa_i^j)\}$ son índices invariantes de cada código con $i = 1, \ldots, k$.

Definición 41. *Definimos los índices de Kronecker de $\mathfrak{C}$, y los denotamos por $\mathfrak{K}^{\mathfrak{C}}$, como la t-upla de vectores donde cada componente son los índices de Kronecker de cada $\mathcal{C}_j$; es decir,*

$$\mathfrak{K}^{\mathfrak{C}} = [(\kappa_1^1, \ldots, \kappa_1^t), \ldots, (\kappa_k^1, \ldots, \kappa_k^t)]$$

donde (κ_i^j) es el i-ésimo índice de Kronecker del código convolucional $\mathcal{C}_j$.

Definición 42. *Definimos los índices conjugados de Kronecker de $\mathfrak{C}$, y los denotamos por $\xi^{\mathfrak{C}}$, como la t-upla de vectores donde cada componente son los índices de Kronecker conjugados de cada $\mathcal{C}_j$; esto es,*

$$\xi^{\mathfrak{C}} = [(\xi_1^1, \ldots, \xi_1^t), \ldots, (\xi_k^1, \ldots, \xi_k^t)]$$

donde (ξ_i^j) es el i-ésimo índice de Kronecker conjugado del código convolucional $\mathcal{C}_j$.

Observación 6.3.4. *Por la definición de $\mathfrak{C}$ cada código convolucional $\mathcal{C}_j$ tiene el mismo número de índices de Kronecker, k, y el mismo grado del código $\sum_{i=1}^{k} \kappa_i^j = \delta$ para todo $j = 1 \ldots t$.*

Definición 43. *Sean $\mathfrak{C}$ y $\overline{\mathfrak{C}}$ dos familias de códigos convolucionales sobre R. La relación feedback $\overset{f.f.c.e.}{\sim}$ definida como*

$$\mathfrak{C} \overset{f.f.c.e}{\sim} \overline{\mathfrak{C}} \Leftrightarrow \mathfrak{K}^{\mathfrak{C}} = \mathfrak{K}^{\overline{\mathfrak{C}}}$$

es una relación de equivalencia.

Lema 44. *El número de clases de equivalencia feedback de familias de códigos convolucionales con el mismo grado δ es $p_{\mathbb{N}}(\delta)^t$ donde $p_{\mathbb{N}}(\delta)$ es la partición del grado del código.*

A continuación aclaramos alguna notación para evitar errores.

Notación. *Sean $\mathfrak{C}$ y $\overline{\mathfrak{C}}$ familias (n,k) de códigos convolucionales sobre R.*

1. *Sean* $\Sigma = (A, B, C, D)$ *y* $\overline{\Sigma} = (\overline{A}, \overline{B}, \overline{C}, \overline{D})$ *las correspondientes representaciones I/S/O obtenidas mediante el Teorema 29 de* $\mathfrak{C}$ *y* $\overline{\mathfrak{C}}$*. Denotaremos por* $\Sigma^{\mathfrak{C}} = (A, B)^{\mathfrak{C}}$ *y* $\overline{\Sigma}^{\overline{\mathfrak{C}}} = (\overline{A}, \overline{B})^{\overline{\mathfrak{C}}}$ *la parte dinámica de estos sistemas donde* $A, \overline{A} \in \mathcal{M}_{\delta\times\delta}(R)$ *y* $B, \overline{B} \in \mathcal{M}_{\delta\times k}(R)$*.*

2. *Denotaremos por* $\mathfrak{K}^{\mathfrak{C}}$ *y* $\mathfrak{K}^{\overline{\mathfrak{C}}}$ *el conjunto de índices de Kronecker de las familias de códigos convolucionales y por* $\xi^{\mathfrak{C}}$ *y* $\xi^{\overline{\mathfrak{C}}}$ *el conjunto de los índices conjugados de Kronecker de estas familias de códigos.*

3. *Denotaremos por* $\mathfrak{K}^{\Sigma^{\mathfrak{C}}}$ *y* $\mathfrak{K}^{\Sigma^{\overline{\mathfrak{C}}}}$ *el conjunto de los índices de Kronecker de los pares asociados* $(A, B)^{\mathfrak{C}}$ *y* $(\overline{A}, \overline{B})^{\overline{\mathfrak{C}}}$ *a las familias de códigos convolucionales como sistemas lineales sobre* R*. Además, denotaremos por* $\xi^{\Sigma^{\mathfrak{C}}}$ *y* $\xi^{\Sigma^{\overline{\mathfrak{C}}}}$ *el conjunto de los índices de Kronecker conjugados de estos sistemas dinámicos lineales.*

4. *Denotaremos por* $\Sigma^{\mathcal{C}_j} = (A_j, B_j)^{\mathcal{C}_j}$ *y* $\overline{\Sigma}^{\overline{\mathcal{C}_j}} = (\overline{A}_j, \overline{B}_j)^{\overline{\mathcal{C}_j}}$ *las correspondientes dinámicas de las representaciones I/S/O, calculadas mediante representaciones de primer orden, de cada* $\mathcal{C}_j$ *y* $\overline{\mathcal{C}}_j$*, las restricciones a cada cuerpo finito* $\mathbb{F}_j$ *de* $\mathfrak{C}$ *y* $\overline{\mathfrak{C}}$*.*

5. *Denotaremos por* $\mathfrak{K}^{\Sigma^{\mathcal{C}_j}}$ *y* $\mathfrak{K}^{\Sigma^{\overline{\mathcal{C}_j}}}$ *el conjunto de índices de Kronecker del comportamiento dinámico de sus representaciones I/S/O asociadas al código convolucional sobre cuerpos finitos como sistemas lineales. Además, denotaremos por* $\xi^{\Sigma^{\mathcal{C}_j}}$ *y* $\xi^{\Sigma^{\overline{\mathcal{C}_j}}}$ *el conjunto de índices conjugados de Kronecker de estas representaciones I/S/O.*

A continuación nuestros resultados principales:

Teorema 45. *Sean* $\mathfrak{C}$ *y* $\overline{\mathfrak{C}}$ *familias de códigos convolucionales sobre* R*. Sean* $\Sigma^{\mathfrak{C}}$ *y* $\overline{\Sigma}^{\overline{\mathfrak{C}}}$ *las correspondientes partes dinámicas de las representaciones I/S/O. Denotaremos por* $f.i$ *el isomorfismo feedback entre sistemas lineales localmente Brunovsky con espacio de estados de rango* δ*. Entonces*

$$\mathfrak{K}^{\mathfrak{C}} = \mathfrak{K}^{\overline{\mathfrak{C}}} \Leftrightarrow \Sigma^{\mathfrak{C}} \overset{f.i}{\simeq} \overline{\Sigma}^{\overline{\mathfrak{C}}}$$

Teorema 46. *Sea* $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ *donde* $\mathbb{F}_j$ *son cuerpos finitos para todo* j*. Then*

$$\left\{ \begin{array}{c} \textit{Clases Feedback de} \\ \textit{las partes dinámicas de I/S/O's} \\ \textit{de familias de códigos} \\ \textit{convolucionales over } R \end{array} \right\} = \left\{ \begin{array}{c} \textit{Clases de isomorfimos Feedback de} \\ \textit{Sistemas Lineales Localmente Brunovsky} \\ \textit{over } R \end{array} \right\}$$

Conclusiones y futuras investigaciones.

En este trabajo hemos completado con éxito el estudio sobre la enumeración de las clases de isomorfismos feedback de sistemas lineales localmente Brunovsky sobre diferentes anillos base. Es más, en el caso particular de anillos regulares de von Neumann hemos podido caracterizar dichos anillos en términos de ciertas propiedades de sistemas lineales.

Además, hemos podido generalizar la conexión clásica existente entre códigos convolucionales y sistemas lineales a través de representaciones de primer orden y representaciones I/S/O al caso relativo de ciertos anillos conmutativos lo cual nos permite construir familias de códigos convolucionales observables utilizando sistemas lineales observables y accesibles.

Finalmente, hemos probado que la clase de isomorfismos feedback de sistemas localmente Brunovsky sobre un anillo de la forma $R = \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ (siendo $\mathbb{F}_j$ un cuerpo finito para cada $j = 1, \ldots, t$) es igual a la clase de las dinámicas de las representaciones I/S/O de familias de códigos convolucionales sobre R respecto de la relación feedback definida por los índices de Kronecker de ambos tipos de sistemas.

Los resultados principales de esta tesis son

1. Hemos calculado el número de isomorfismos feedback de sistemas localmente Brunovsky (y por tanto accesibles) con coeficientes en diferentes tipos de anillos:

   a) Anillos que descomponen en producto finito de anillos. En particular, productos finitos de anillos proyectivamente triviales..

   b) Anillos regulares noetherianos de von Neumann. En particular, anillos de enteros modulares $\mathbb{Z}/l\mathbb{Z}$ donde $l = p_1 \ldots p_t$ es libre de cuadrados.

   c) Dominios de Dedekind. Para este resultado es necesaria la introducción de cierto número combinatorio $\nu(n, k) = \nu(n, k, p) + \nu(n, k, p')$.

2. Hemos probado que todo anillo regular de von Neumann es localmente Brunovsky.

3. Hemos definido el concepto de familia de códigos convolucionales sobre un anillo conmutativo y hemos estudiado algunas propiedades de dichas familias y de sus codificadores.

4. Hemos determinado la existencia de representaciones de primer orden para familias de códigos convolucionales sobre $R = \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ (siendo $\mathbb{F}_j$ un cuerpo finito).

5. Hemos determinado también la existencia de representaciones I/S/O para familias de códigos convolucionales sobre $R = \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ y hemos estudiado propiedades como la accesibilidad, la observabilidad y la propiedad de ser localmente Brunovsky.

6. Hemos definido una relación (de equivalencia) feedback para códigos convolucionales meidante sus índices de Kronecker. Es más, hemos calculado el número de clases respecto de dicha equivalencia.

7. Finalmente, hemos generalizado la relación feedback anterior definida entre los índices de Kronecker de familias de códigos convolucionales sobre $R = \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ y lso índices de Kronecker (los índices de la partici'on conjugada) de la representación I/S/O que obtenemos de los códigos. Esta relación feedback nos permite concluir que existe una correspondencia biyectiva entre isomorfismos feedback de sistemas lineales localmente Brunovsky y clases feedback de las partes dinámicas de las representaciones I/S/O de las familias de códigos convolucionales sobre R.

6.4. Aplicaciones a la cibernética, teoría de códigos y criptografía. Investigación futura.

Damos ahora un breve repaso a las áreas de investigación relacionadas con el trabajo aquí presentado. Algunas de ellas serán abordadas en el futuro con el objetivo de concluir con un estudio completo de la relación entre la clasificación feedback de códigos convolucionales y la clasificación feedback de sistemas lineales sobre anillos. El resto de áreas pueden ser consideradas como campos de implementación y aplicación de el presente trabajo.

Los códigos convolucionales son utilizados en numerosas aplicaciones como la comunicación por satélite, comunicación a través de terminales móviles, video digital, radio, etc.

El uso por la NASA de códigos correctores de errores en las comunicaciones con la Tierra del orbitador Cassini es solo un ejemplo del hecho de que los códigos convolucionales son una herrmaienta muy potente en los sistemas de transmisión de información. Otra aplicación de los códigos convolucionales la podemos encontrar en su implementación en las teorías de *hard-decision*, en particular los códigos Reed Solomon. Además, las investigaciones recientes en concatenación en serie y en paralelo de códigos convolucionales nos aportan avances significativos en la construcción de Turbocódigos.

Los resultados aquí presentados pueden ser útiles en teoría de códigos de la siguiente manera: desarrollar la relación entre sistemas dinámicos y códigos convolucionales sobre anillos pueden extender el estudio de nuevas métodos de construcción de códigos con ciertas características y el estudio del proceso de decodificación mediante el sistema dinámico asociado.

En el proceso de codificación y decodificación podemos aplicar nuestros resultados si queremos enviar un mensaje a t receptores pero de tal manera que cada receptor recibe únicamente una parte del mensaje. En este caso, se usa una base de t sistemas de comunicación , de tal manera que el mensaje es codificado con un alfabeto producto de t cuerpos finitos $R = \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$. Es decir, podemos usar el código convolucional sobre R para enviar al receptor j-ésimo la parte $\otimes_R \mathbb{F}_j$ del mensaje. Además debemos observar que la continuidad entre receptores no sería necesaria. Es más, si cada parte del mensaje $\otimes_R \mathbb{F}_j$ es compartido por cada receptor es posible reconstruir el mensaje original.

En el área de la criptografía la relevancia de los resultados de esta tesis se puede desarrollar desde diferentes puntos de vista. De la misma forma que en [22], podemos aplicar los códigos convolucionales para decodificar criptosistemas. Además el número isomorfismos feedback de sistemas lineales localmente Brunovsky sobre dominios de Dedekind pueden ser aplicados en el caso del círculo unidad y, por lo tanto, sobre todas las curvas cerradas que son homeomorfas con el círculo unidad. Por lo tanto, nuestros resultados puden ser interesantes en el estudio de códigos convolucionales sobre curvas elípticas (o cualquier otra curva lisa e irreducible) a través de la teoría de sistemas.

Respecto a la ciberseguridad, la dualidad entre códigos convolucionales y representaciones *trellis* supone poder utilizar códigos convolucionales en el modelado de redes. Este trabajo se puede implementar para obtener sistemas algebraicos de codificaciones de señales simultáneas en las redes de codificación lineales de multidifusión. En particular, la

relación existente entre códigos convolucionales, representaciones *trellis*, gráficos de redes y sistemas lineales nos permite aplicar nuestros resultados, por ejemplo, sobre los anillos booleanos (las redes booleanas, por ejemplo, son muy útiles en el modelado y la descripción cuantitativa de la regulación celular). Una nueva técnica, desarrollada en [20], analiza y sintetiza redes booleanas (de control) basándose en la conversión de las dinámicas lógicas de la red en dinámicas de tiempo discreto estándards.

Por último, podemos encontrar otra aplicación de este trabajo en el tratamiento de bases de datos. Las bases de datos de los servicios de seguridad de la información están creciendo más rápido que las herramientas para su tratamiento siendo necesaria una mejor gestión de la cantidad de los datos y la clasificación de estas bases. Estudios recientes, centrados en antiterrorismo, presentan la implementación de algoritmos algebraicos basados en códigos convolucionales con el fin de optimizar los procesos de clasificación (ver [81] para más detalles).

Con respecto a las líneas de investigación futuras una posible vía podría ser extender la clasificación de los sistemas y códigos convolucionales a otras clases de anillos y, por lo tanto, la relación entre ellos.

Otra línea de actuación se centraría en dar una caracterización completa de las familias de códigos convolucionales sobre otros anillos (sus representaciones, propiedades como la distancias de Hamming, la construcción de códigos observables y los procesos de codificación y decodificación).

Finalmente, el número combinatorio $\nu(n, k)$ ha sido estudiado por nuestro actual grupo de investigación con el fin de encontrar una función generatriz y completar las propiedades de dichos números.

References.

[1] P.J. Antsaklis and A.N. Michel, *Linear Systems*, Birkhäuser, Boston, MA, (2006).

[2] M. A. Arbib, H. P. Zeiger, On the relevance of abstract algebra to control theory, *Journal Automatica* (Journal of IFAC), Vol. 5, Issue 5, (1969), pp. 589-606, DOI:10.1016/0005-1098(69)90026-0

[3] M. S. Atiyah, I. G. MCDonald, *Introduction to Algebra Conmutative*, Addison-Wesley Publishing Company, University of Oxford,(1969).

[4] N. Bourbaki, *Elements de Mathematique Algebre commutative*, Chapitres 5-7, Springer-Verlag Berlin, (2006).

[5] J. W. Brewer, L. Klingler, Dynamic feedback over commutative rings, *Linear Algebra and Its Applications*, Vol. 98, (1988), pp. 137-168.

[6] J. W. Brewer, L. Klingler, On feedback invariants for linear dynamical systems, *Linear Algebra and its Applications*, Vol.325, Issues 1-3, (2001), pp. 209-220, DOI: 10.1016/S0024-3795(00)00263-9.

[7] J. W. Brewer, J. W. Bunce, and F. S. Van Vleck, *Linear Systems over Conmutative Rings*, Marcel Dekker, New York, (1986).

[8] P. A. Brunovsky, A classification of linear controllable systems, *Kibernetika*, Vol. 6, No. 3, (1970), pp. 173-187.

[9] M.V. Carriegos, On the local-global decomposition of linear control systems, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 9, Issue 2, (2003), pp. 149-156, DOI: 10.1016/S1007-5704(03)00106-0.

[10] M. V. Carriegos, Enumeration of classes of linear systems via equations and via partitions in a ordered abelian monoid, *Linear Algebra and Its Applications*, Vol. 438, Issue 3, (2013), pp. 1132-1148, DOI: 10.1016/j.laa.2012.08.040

[11] M. Carriegos, T. Sánchez-Giralda, Canonical forms for linear dynamical systems over commutative rings, the local case., *Proceedings of the fifth international conference (SAGA V)* in León, Spain, ISBN 0-8247-0559-9, pp. 113-131, (2001).

[12] M. V. Carriegos, M. López-Cabeceira, There are more locally Brunovsky systems than constant ones , *Conference Proceedings of the 13th WSEAS international conference on Automatic control, Modelling & Simulation*, pp. 249-251, (2011).

[13] M. V. Carriegos, , Noemí DeCastro-García, Partitions of elements in a monoid and its applications to systems theory . *Linear Algebra and Its Applications.In press.* doi:10.1016/j.laa.2015.05.034

[14] M. Carriegos, J.A. Hermida-Alonso, T. Sánchez-Giralda, The pointwise feedback relation for linear dynamical systems, *Linear Algebra and Its Applications*, Vol. 279, Issues 1-3, (1998), pp. 119-134. DOI: 10.1016/S0024-3795(98)00020-2

[15] M.V. Carriegos, N. DeCastro-García, M.M.Cb. López, Enumeration of locally Brunovsky linear systems over $\mathcal{C}(\mathbb{S}^1)$-modules. A procedure. *Cybernetics and Physics*,Vol. 2, (2013), pp. 72-76.

[16] M. Carriegos, J.A. Hermida-Alonso, A. Sáez-Schwedt, T. Sánchez-Giralda , Rosenbrock's theorem for systems over von Neumann regular rings, *Linear Algebra and its Applications*. Vol. 482, (2015), pp. 122-130, DOI: 10.1016/j.laa.2015.05.017

[17] M.V Carriegos, N. deCastro-García A.L. Muñoz Castañeda, *A characterization of von Neumann regular rings in terms of linear systems*, *Submitted to Linear Algebra and Its applications*, September (2015).

[18] J.L.Casti, *Linear Dynamical Systems*, Vol. 135 of Mathematics in science and engineering, Academic Press, (1987), ISSN 0076-5392.

[19] Chang-jia Chen, Construction of linear ring codes for 6 PSK, *IEEE Transactions of Information Theory*, Vol. 40, Issue: 2, (2002), pp.563 - 566, DOI: 10.1109/18.312187.

[20] D. Cheng, Disturbance Decoupling of Boolean Control Networks, *IEEE Transactions Automatic Control*, Vol. 56, Issue: 1, (2011), pp. 2-10. DOI:10.1109/TAC.2010.2050161

[21] L. Claborn, Every abelian group is a class group, *Pacific Journal of Mathematics*, Vol. 18, No 2, (1996), pp. 219-222, DOI: 10.2140/pjm.1966.18.219

[22] J.J. Climent, V. Herranz, C. Perea, V. Tomás, Un criptosistema de clave pública basado en códigos convolucionales, *Proccedings of XXI Congreso de Ecuaciones*

Diferenciales y Aplicaciones & XI Congreso de Matemática aplicada, Ciudad Real, Septiembre 2009, pp.1-8.

[23] P. Elias. Coding for two noisy channels. *IRE Conv. Rec.*, Vol. 4, (1955), pp. 37-46.

[24] Fagnani, F. and S. Zampieri, System-theoretic properties of convolutional codes over rings, *IEEE Transactions Information Theory*, Vol. 47, Issue 6, (2001), pp. 2256-2274, DOI: 10.1109/18.945247.

[25] G.D. Forney. Convolutional codes I: Algebraic structure. *IEEE Transactions Information Theory*, Vol.16, Issue 6, (1970), pp. 720-738, DOI: 10.1109/TIT.1970.1054541

[26] C. Fragouli, R.D. Wesel, Convolutional Codes and Matrix Control Theory, $CiteSeer^x$, DOI: 10.1.1.26.7877.

[27] M.I. García-Planas, J.L. Domínguez- García, Alternative tests for functional and pointwise output-controllability of linear time-invariant systems, *Systems & Control Letters*, Vol. 62, Issue 5, (2013), pp.382-387. DOI: 10.1016/j.sysconle.2013.02.003

[28] M.I. García-Planas, El M. Souidi, L.E. Um, Convolutional codes under linear systems point of view. Analysis of output-controllability. *WSEAS Transactions on Mathematics*. Vol.11, Issue 4, (2010), pp. 324-333.

[29] M.I. García-Planas, El.M. Souidi, L.E. Um, Convolutional codes under control theory point of view. Analysis of output-observability, *Recent Advances in Circuits, Communications and Signal Processing*, (2013), ISBN: 978-1-61804-164-7 .

[30] M.I. García-Planas, El.M. Souidi, L.E. Um, Analysis of control properties of concatenated convolutional codes, *Cybernetics and Physics*, Vol. 1, Issue 4, (2012), pp.252-257.

[31] D.Gesbert, M. Shafi, D.S. Shiu, P. Smith, A. Naguib, From Theory to Practices: An overview of MIMO space-time coded wireless systems, *IEEE: Selected Areas in Communications,*, Vol.: 21, Issue: 3, (2003), pp. 281-302, DOI: 10.1109/JSAC.2003.809458.

[32] H. Gluesing-Luerssen, On the weight distribution of convolutional codes, *Linear Algebra and its Applications*, Vol. 408, (2005), pp. 298-326. DOI: 10.1016/j.laa.2005.06.023

[33] H. Gluesing-Luerssen, G. Schneider, State space realizations and monomial equivalence for convolutional codes, *Linear Algebra and its Applications*, vol. 425, Issues 2-3, (2007), pp. 518-533. DOI: 10.1016/j.laa.2007.03.004

[34] Gluesing-Luerssen, H., J. Rosenthal, and P. A. Weiner, Duality between multidimensional convolutional codes and systems, *Advances in Mathematical Systems Theory*, Birkhäuser, Boston (2000).

[35] H. Gluesing-Luerssen., U. Helmke, J.I. Iglesias Curto, Algebraic Decoding for Doubly Cyclic Convolutional Codes, *Advances in Mathematics of Communications*, Vol.4,(2010), pp.83-99. DOI: 10.3934/amc.2010.4.83

[36] K. R. Goodearl, *von Neumann regular rings* (2 ed.), Malabar, FL: Robert E. Krieger Publishing Co. Inc., (1991).

[37] M.L.J. Hautus, Controllability and observability condition for linear autonomous system. *Ned. Akad. Wetenschappen*, *Proc. Ser. A*, Vol. 72, (1969), pp. 443-448.

[38] M.L.J. Hautus, E.D. Sontag, New results on pole-shifting for parametrized families of systems, *Journal of Pure and Applied Algebra* ,Vol. 40, (1986), pp: 229-244. DOI: 10.1016/0022-4049(86)90043-5

[39] J.A. Hermida-Alonso, On linear algebra over commutative rings, Chapter in: *Handbook of Algebra*, vol. 3, Elsevier Science, (2003), pp. 3-61.

[40] J.A. Hermida-Alonso, M.P. Perez, T. Sanchez-Giralda, Feedback invariants for linear dynamical Systems over a principal ideal domain, *Linear Algebra and its Applications*, Vol. 218, (1995), pp.29-45. DOI: 10.1016/0024-3795(93)00153-Q

[41] J.A. Hermida-Alonso, M.P. Perez, T. Sanchez-Giralda, Brunovsky's canonical form for linear dynamical Systems over commutative rings, *Linear Algebra and its Applications*, Vol. 233, (1996), pp. 131-147. DOI: 10.1016/0024-3795(94)00062-X

[42] R. Hutchinson, J. Rosenthal, R. Smarandache, Convolutional codes with maximum distance profile, *Systems & Control Letters.*, Vol. 54, Issue 1, (2005), pp- 53-63. DOI: 10.1016/j.sysconle.2004.06.005

[43] R. Johannesson, Z.Wan, and E. Wittenmark. Some structural properties of convolutional codes over rings. *IEEE Transactions Information Theory*, Vol. 44, Issue 2, (1998), pp. 839-845. DOI: 10.1109/18.661532

[44] R. E. Kalman, Kronecker invariants and Feedback, in Ordinary Differential Equations, *Academic*, pp. 459-471 (1972).

[45] Kitchens, B., Multidimensional convolutional codes, *SIAM Journal of Discret Mathematics*, Vol. 15, Issue 3, (2002)., pp. 367-381 DOI:10.1137/S0895480100378495

[46] K. Krohn. John L. Rhodes, M.A. Arbib,*Algebraic Theory of Machines, Languages, and Semigroups*, Academic Press (1968), Krohn-Rhodes Research Inst. Inc. Washington DC.

[47] M. Kuijper, *First Order Representations of Linear Systems*, Ph.D. Thesis. Boston, MA: Birkhäuser, 1994

[48] M. Kuijper, R. Pinto, On minimality of convolutional ring encoders, *IEEE Transactions on Information Theory*, Vol.55, Issue 11, (2009), pp. 4890-4897. DOI: 10.1109/TIT.2009.2030486

[49] Kuijper, M., R. Pinto, J. W. Polderman, and P. Rocha, Autonomicity and the absence of free variables for behaviors over finite rings, *Proc. 7th Portuguese Conf. Autom. Control*, Lisbon, Portugal (2006).

[50] P. Kunkel, V. Mehrmann, A new look at pencils of matrix valued functions. *Linear Algebra and its Applications*, Vol.10, (1994); pp. 212-213:215-248. DOI:10.1016/0024-3795(94)90403-0.

[51] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Math. **189**, Springer-Verlag, Berlin, New York, Heidelberg, (1999).

[52] S. Lang, *Algebra*, Graduate Texts in Mathematics, Vol. 211, Springer (2002).

[53] J.L. Massey and T. Mittelholzer. Convolutional codes over rings. *In Proc. Joint Swedish-Soviet Int. Workshop on Inform. Theory*, pp. 14-18, Gotland, Sweeden, (1989).

[54] J.L. Massey and T. Mittelholzer. Systematicity and rotational invariance of con- volutional codes over rings. *In Proc. Int. Workshop on Alg. and Combinatorial Coding Theory*,pp. 154-158, Leningrad, (1990).

[55] H. Matsumura, *Commutative algebra.* Second edition. Mathematics Lecture Note Series, 56. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., (1980). ISBN 0-8053-7026-9

[56] B.R. McDonald, *Linear Algebra over commutative rings*, Marcel Dekker, (1984).

[57] R. J. McEliece. *The algebraic theory of convolutional codes.* In V. Pless and W.C. Huffman, editors, Handbook of Coding Theory, Vol. 1, pp. 1065-1138, (1998).

[58] V. M. Popov, Invariant description of linear time-invariant controllable systems, *SIAM Journal of Control*, Vol. 10, Issue 2, (1972), pp. 252-264 . DOI :10.1137/0310020

[59] M. S. Ravi and J. Rosenthal. A smooth compactification of the space of transfer functions with fixed McMillan degree. *Acta Appl. Math*, Vol. 34, (1994), pp. 329-352.

[60] M. S. Ravi and J. Rosenthal. A general realization theory for higher order linear differential equations. *Systems & Control Letters*, Vol. 25, Issue 5, (1995), pp. 351-360, DOI: 10.1016/0167-6911(94)00085-A.

[61] M. S. Ravi, J. Rosenthal, and J. M. Shumacher, A realization theory for homogeneous AR systems, and algorithmic approach, in *Proc. IFAC Conf. on System Structure and Control*(Nantes, France, (1995), pp. 183-188.

[62] J. Rhodes, Applications of Auotmata Theory and Algebra, *World Scientific*, (2010).

[63] J. Rhodes, P.V. Silva, *Turing machines and bimachines*, Vol. 400, (2008), pp.182-224.

[64] J. Rosenberg, *Algebraic K- Theory and Its Applications*, Graduate Texts in Mathematics, Springer, (1994).

[65] J. Rosenthal, Some interesting problems in systems theory wich are of fundamental importance in coding theory, *Proceedings of the 36th IEEE Conference on Decision and Control*, (1997).

[66] J. Rosenthal, An algebraic decoding algorithm for convolutional codes, In *Dynamical Systems, Control, Coding, Computer Vision; New Trends, Interfaces, and Interplay*, pp. 343-360. Birkhäuser, Basel, (1999).

[67] J. Rosenthal, *Codes, systems and graphical models*, IMA, vol. 123, ch. Connections between linear systems and convolutional codes, pp. 39 - 66, Springer - Verlag, (2001)

[68] J. Rosenthal and J.M.Shumacher, Realization by inspection, *IEEE Transactions on Automatic and Control*, Vol. 42, Issue 9, (1997), pp.1257-1263, DOI: 10.1109/9.623088

[69] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes, *Applicable Algebra in Engineering, Communication and Computing*, Vol. 10, Issue 1, (1999), pp. 15-32. DOI: 10.1007/s002000050120

[70] J. Rosenthal, E. V. York, BCH Convolutional Codes, *IEEE Transactions on Information Theory*, Vol. 45, Issue 6, (1999), pp. 1833-1844, DOI: 10.1109/18.782104

[71] Joachim Rosenthal, J. M. Schumacher, and E. V. York, On behaviors and convolutional codes, *IEEE Transactions on Informations Theory*, Vol. 42, Issue. 6, (1996), pp. 1881-1891, DOI: 10.1109/18.556682.

[72] A. Sáez-Schwedt , Cyclic accessibility of reachable states characterizes von Neumann regular rings. *Linear Algebra and its Applications*, Vol: 433, Issue 6, (2010), pp. 1187 - 1193 , DOI:10.1016/j.laa.2010.04.047

[73] A. Sáez-Schwedt, Assignable polynomials to linear systems over a von Neumann regular rIngs. *Linear Algebra and its Applications*, Vol. 470, Issue 1, (2014), pp. 104-119. DOI: 10.1016/j.laa.2014.04.029

[74] A. Sáez-Schwedt; T. Sánchez-Giralda Strong feedback cyclization for systems over rings, *Systems and Control Letters*, Vol. 57, Issue 1, pp. 71-77, (2008). DOI: 10.1016/j.sysconle.2007.06.017

[75] A. Sáez-Schwedt; W. Schmale, Feedback classification of linear systems over von Neumann regular rings, *Linear Algebra and its Applications*, Vol. 438 , Issue 4, (2013), pp. 1852 - 1862, DOI: 10.1016/j.laa.2011.05.038

[76] L. Skyttner, General systems Theory, *World Scientific*, (2005).

[77] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Transactions on Informations Theory*, Vo.47, Issue 5, (2002), pp. 2045-2049, DOI: 10.1109/18.930938

[78] E.D. Sontag, *Mathematical Control Theory: Deterministic Finite Dimensional Systems*, Springer, New York, (1990).

[79] P. Van Dooren, The computation of Kronecker's canonical form of a singular pencil. *Linear Algebra and Its Applications*, Vol. 27, (1979), pp. 103-141, DOI::10.1016/0024-3795(79)90035-1

[80] W.V.Vasconcelos, C.A. Weibel, Bcs rings, *Journal of Pure and Applied Algebra*, Vol. 52, Issues 1-2, (1988), pp. 173-185, DOI: 10.1016/0022-4049(88)90145-4

[81] M. P. Velasco *et al*, *La lucha antiterrorista a través de algoritmos algebraicos y estocásticos aplicados a los Servicios de Información*, Congreso Jóvenes Investigadores, RSME, September 2015, Murcia (Spain).

[82] C.A. Weibel, *The K-book: an introduction to algebraic K-theory*, Graduate Studies in Mathematics, Vol. 145, AMS, (2013).

[83] E. V. York, *Algebraic description and construction of error correcting codes, a systems theory point of view.*, Ph.D. dissertation, Univ. Notre Dame, 1997. [Online].

[84] E. Zerz, On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings, *Asian Journal of Control*, vol.12,Issue 2, (2010), pp. 119-126, DOI: 10.1002/asjc.169

Appendices

Appendix A

Euler's partitions of an integer number

Euler's Theory of integers partitions goes back to $XVIII$ century and it has been intensely researched. Thus, a research problem of century XXI has in fact been studied from classic math. In the Chapter 16 of Euler's *Introductio in Analysin Infinitorum*, (1748), entitled *De Partitio Numerorum*, the partition of an integer number is computed by Euler's generator function. In the case of partition function of $p_{\mathbb{N}}(n)$, the generator function associated to $S = \{p_{\mathbb{N}}(0), p_{\mathbb{N}}(1), p_{\mathbb{N}}(2), ..., p_{\mathbb{N}}(n), ...\}$ is given by

$$\sum_{n=0}^{\infty} p_{\mathbb{N}}(n) z^n = \prod_{n=1}^{\infty} \frac{1}{1-z^n} = 1 + z + 2z^2 + 3z^3 + 5z^4 + 7z^5 + 11z^6 + ... \qquad \text{(A.1)}$$

where $p_{\mathbb{N}}(n)$ is equal to the coefficient of the power z^n of the formula A.1.

Partitions can be graphically represented with Young diagrams or Ferrers diagrams. The Ferrers diagram of an integer partition is constructed by rows of points, where the number of points in each row corresponds to the number of each summand of the partition. The first row corresponds to the largest part, the second row corresponds to the second largest part, and so on. A Ferrers diagram becomes into a Young diagram changing the points for cells.

The reader can see the partitions of number 5 with their associated diagram of Young in Table A.1.

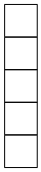
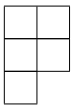
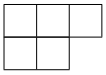
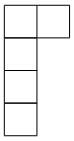
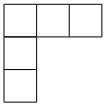
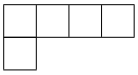
Number	Partition	Young's Diagram
5	1+1+1+1+1	
5	2+2+1	
5	3+2	
5	2+1+1+1	
5	3+1+1	
5	4+1	
5	5	

Table A.1: *Partitions of number* 5.

Appendix B

Basic algebraic results.

In this appendix we give an overview of basic algebraic results that have been very usfeul in some proofs of this work. Throughout this appendix R is a commutative ring with $1 \neq 0$.

B.1. Coprime ideals in a ring and Chinese Remainder Theorem

Theorem B.1.1. *Chinese Reminder Theorem (CRT). Let R be a ring and let J and I ideals such that $R = I + J$. Then $R/I + J \simeq R/I \times R/J$.*

Corollary B.1.2. *Let m, n be coprime integers. Then $\mathbb{Z}/ln\mathbb{Z} \simeq \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Corollary B.1.3. *If $n_1, ..., n_k$ are coprime integers then $\mathbb{Z}/n_1...n_k\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$.*

B.2. Modules over a commutative ring.

Let us review some basic properties of R-modules.

Definition B.2.1. *A R-module M is free if has a basis. If R is a commutative ring, then all basis of M has the same cardinal (rank of module M) and then $M \simeq R^{rank(M)}$.*

Definition B.2.2. *A R-module P is proyective if for all exact sequence of R-modules*

$$M' \to M \to M'' \to 0$$

then the following sequence is exact.

$$Hom_R(P, M') \to Hom_R(P, M) \to Hom_R(P, M'') \to 0$$

Definition B.2.3. *Alternatively, P is proyective if given a surjective morphism $p : M \to M'' \to 0$, then all morphism $f : P \to M''$ lifts to a morphism $g : P \to M$ such that $f = p \circ g$.*

We give some basic results about projective modules over R.

Proposition B.2.4. *Let P be a R-module.*

1. *If P is projective then all exact sequence of R-modules*

$$0 \to N \to M \to P \to 0$$

   splits, namely, there exists an isomorphisms $M \simeq N \oplus P$.

2. *The direct sum of family of projective R-modules is projective if and only if all summands are projective.*

3. *Every finitely generated free R- module is projective.*

4. *A R-module P is projective, if and only if, is direct summand of a free R-module. If P is finitely generated, then the free can be choosen finitely generated.*

5. *All finitely generated projective R-module is finite presented.*

6. *Projectivity preserves by basis change.*

7. *If S is a multiplicative system and M is a projective R-module, then $S^{-1}M$ is a projective $S^{-1}R$-module.*

8. *If R is noetherian then all R-module M is flat if and only if is projective.*

Modules over $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$.

We deal with rings of the form $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ where $\mathbb{F}_i$ are fields for all $j = 1, \ldots, t$, then the following results do apply:

Notation. *For the convenience of the reader we denote by $\mu_j(R) = R \otimes_R \mathbb{F}_j$ and in terms of matrices we denote by $\mu_j(A) = A \otimes 1 \simeq A_j =$ the restriction of A module $\mathbb{F}_j$.*

Theorem B.2.5. *Let $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$ be a ring where $\mathbb{F}_j$ is a finite field for each $j = 1, \ldots, t$. Let A be a matrix over R such that $\mu_j(A) = A_j$ where A_j are matrices over each $\mathbb{F}_j$ for $j = 1, \ldots, t$. Then, the following holds:*

i) If A_j are matrices whose rows are free over $\mathbb{F}_j$ for each j, then A is a matrix whose rows are free over R.

ii) If A_j are matrices whose columns are free over $\mathbb{F}_j$ for each j, then A is a matrix whose columns are free over R.

iii) If A_j are invertible matrices over $\mathbb{F}_j$ for each j, then A is a inertible matrix over R.

Proof. *i)* Let f_i^j be the i-th row of the j-th matrix A_j. And let f_i be the i-th row of A. If there exist rows in A that are not linearly independent over R, then there exists, at least, one row such that

$$f_i = \sum \lambda_k f_k \text{ for some } i \text{ and } \lambda_k \in R \tag{B.1}$$

By μ_j, the equation (B.1) becomes in $\overline{f_i} = \sum \overline{\lambda_k} \cdot \overline{f_k} \Longrightarrow f_i^j = \sum \lambda_k^j \cdot f_k^j$. Since if $\lambda_k^j = \overline{0}$ for some j implies that $\lambda_k = 0$, then we conclude that there does not exist linearly independent rows in A.

ii) Idem.

iii) Let B_j be the inverse of A_j for each j such that $A_j \cdot B_j = B_j \cdot A_j = I$. Let B be a matrix such that $\mu_j(B) = B_j$ for $j = 1, \ldots, t$. We consider C and C' defined as follows: $C = AB$ and $C' = BA$.

Then $\mu_j(AB) = A_j B_j = I$ and $\mu_j(BA) = B_j A_j = I$. Note that if $\mu_j(1_R) = 1_{\mathbb{F}_j}$ then $1_R = 1$ and idem for the zero. We conclude the proof with $B = A^{-1}$ because

a) If $\mu_j(c_{il}) = 1$ for $i = l$ and $\mu_j(c_{il}) = 0$ for $i \neq l$ then $a_{ii} = b_{ii} = 1$ and $a_{il} = b_{il} = 0$.

b) If $\mu_j(c'_{il}) = 1$ for $i = l$ and $\mu_j(c'_{il}) = 0$ for $i \neq l$ then $a_{ii} = b_{ii} = 1$ and $a_{il} = b_{il} = 0$

□

Theorem B.2.6 (c.f.[43])**.** *Elementary transformations on matrices over R can be performed componentwise because $GL_\cdot(R) \cong GL_\cdot(\mathbb{F}_1) \times \ldots \times GL_\cdot(\mathbb{F}_t)$.*

Modules over $R[z] \simeq \mathbb{F}_1[z] \times \ldots \times \mathbb{F}_t[z]$.

First we give a result over $\mathbb{F}[z]$:

Theorem B.2.7. *Let $\mathbb{F}$ be a finite field. Let $\overline{\mathbb{F}}$ be the algebraic clausure of $\mathbb{F}$ and $A(z) : \mathbb{F}[z]^n \to \mathbb{F}[z]^m$ a $n \times m$ matrix with $n \geq m$. Then $A(z)$ is surjective if and only if $rk(A(z_0)) = m \ \forall \ z_0 \in \overline{\mathbb{F}}$.*

Proof. Let us denote $Q(z)$ the cokernel of $A(z)$. Then we have the right exact sequence

$$A(z) : \mathbb{F}[z]^n \to \mathbb{F}[z]^m \twoheadrightarrow Q(z) \to 0 \tag{B.2}$$

Suppose $A(z)$ is surjective. Since surjections are still surjections after any base change we find that

$$A(z) : \overline{\mathbb{F}}[z]^n \to \overline{\mathbb{F}}[z]^m$$

is also surjective. In particular it has maximum rank. Let us assume now that $rk(A(z_0)) = m$ for all $z_0 \in \overline{\mathbb{F}}$. In particular this is also true for all $z_0 \in \mathbb{F}$ so $A(z)$ is surjective. □

Let $R[z]$ be the ring such that $R[z] \simeq \mathbb{F}_1[z] \times \ldots \times \mathbb{F}_t[z]$. We will point out in this section some properties for modules over $R[z]$ and their homomorphism.

Theorem B.2.8. *A minimal set of generators of a finitely generated submodule of $R[z]$ can be obtained. Just proceed componentwise*

$$R[z] \simeq \mathbb{F}_1[z] \times ... \times \mathbb{F}_t[z] \text{ with } \mathbb{F}_j \text{ finite fields for } j = 1...t.$$

Proof. Since $R \simeq \mathbb{F}_1 \times \ldots \times \mathbb{F}_t$, if we tensor by $\otimes_R R[z]$ we get another isomorphism $R \otimes_R R[z] \simeq (\mathbb{F}_1 \times ... \times \mathbb{F}_t) \otimes_R R[z]$. Since $R \otimes_R R[z] \simeq R[z]$ and

$$\left.\begin{array}{c} (\mathbb{F}_1 \times ... \times \mathbb{F}_t) \otimes_R R[z] \simeq (\mathbb{F}_1 \otimes_R R[z]) \times \ldots \times (\mathbb{F}_t \otimes_R R[z]) \\ \mathbb{F}_j \otimes_R R[z] \simeq \mathbb{F}_j[z] \forall j = 1...t \end{array}\right\}$$

we conclude the proof. □

Lemma B.2.9. *$\mathbb{F}_j[z]$ is a flat $R[z]$-module.*

Proof. We start from the fact that $R[z]$ is a free $R[z]$-module and since $R[z] \simeq \oplus_{j=1}^{r} \mathbb{F}_j[z]$, $\mathbb{F}_j[z]$ is a direct summand of a free module and then $\mathbb{F}_j[z]$ is a projective $R[z]$-module. By [4], if $\mathbb{F}_j[z]$ is a projective $R[z]$-module, then it is a flat $R[z]$-module. □

Lemma B.2.10. *Let $R[z] \simeq \mathbb{F}_1[z] \times \ldots \times \mathbb{F}_t[z]$ be a ring where $\mathbb{F}_j$ is a field for each $j = 1, \ldots, t$. Let $A(z)$ be a matrix over $R[z]$ such that $\mu_j[A(z)] = A_j(z)$ where $A_j(z)$ are matrices over each $\mathbb{F}_j[z]$ for $j = 1, \ldots, t$. Then, if $A_j[z]$ are matrices whose rows are free over $\mathbb{F}_j[z]$ for each j, then $A[z]$ is a matrix whose rows are free over $R[z]$.*

Proof. Since $R[z] \simeq \mathbb{F}_1[z] \times \ldots \times \mathbb{F}_t[z]$ and $R[z] \otimes_R \mathbb{F}_j[z] \simeq \mathbb{F}_j[z]$ for all $\mathbb{F}_j$ for $j = 1, \ldots, t$, by [i)] of Theorem B.2.5 we conclude the proof. □

Note that if $R[z] \simeq \mathbb{F}_1[z] \times ... \times \mathbb{F}_t[z]$ so its spectrum is equal to the disjoint union of finitely many lines

$$Spec(R[z]) = \coprod Spec(\mathbb{F}_j[z]) = \coprod \mathbb{A}^1_{\mathbb{F}_j}$$

Therefore each $\mathbb{F}_j[z]$ is a flat $R[z]$-module and a $R[z]$-module is flat if and only if it is over each line.

Lemma B.2.11. *Let $R[z] \simeq \mathbb{F}_1[z] \times \ldots \times \mathbb{F}_t[z]$ be a commutative ring with identity. Let M, N be $R[z]-$modules, and let be $M_j \simeq M \otimes_{R[z]} \mathbb{F}_j[z]$ and $N_j \simeq N \otimes_{R[z]} \mathbb{F}_j[z]$.*

$$\textit{If } M_j \simeq N_j \ \forall j = 1, \ldots, t, \textit{ then } M \simeq N.$$

Proof. Consider the $R[z]$-module $M' = M_1 \times \ldots \times M_t$. Then the canonical surjections

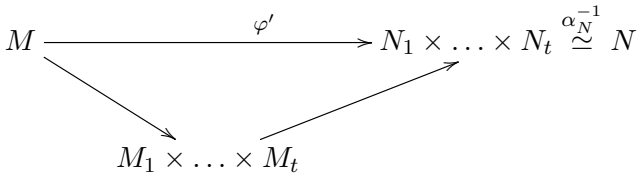
$$\alpha_j : M \longrightarrow M_j = M \otimes_{R[z]} \mathbb{F}_j[z]$$
$$m \mapsto m \otimes 1$$

induce a homomorphism

$$\alpha : M \longrightarrow M'$$
$$m \mapsto \alpha(m) = (\alpha_1(m), \ldots, \alpha_t(m))$$

For any prime ideal $\mathfrak{p} \subset R[z]$, the morphism α localized at $\mathfrak{p}$ and denoted by $\alpha_\mathfrak{p}$ is defined by $M_\mathfrak{p} \xrightarrow{\alpha_\mathfrak{p}} M'_\mathfrak{p} = (M_j)_\mathfrak{p}$ and it is an isomorphism, therefore so is α.

Consider now $M \overset{\pi_j}{\twoheadrightarrow} M \otimes_{R[z]} \mathbb{F}_j[z] = M_j \overset{\varphi_j}{\xrightarrow{\sim}} N_j$. Then we have a morphism φ' such that



Then $\varphi^{'}$ is an isomorphism and the Lemma holds.

□

Appendix C

Line Bundles: Basic Concepts.

C.1. Line Bundle. Definition

Definition C.1.1 (c.f.[82]). *An algebraic line bundle L over a commutative ring R is just a finitely generated projective R-module of constant rank 1.*

We review some properties about line bundles:

1. The tensor product $L \otimes_R M \simeq M \otimes_R L$ of line bundles is again a line bundle.
2. $L \otimes_R R \simeq L$ for all L.
3. Thus up to isomorphism the tensor product is a commutative associative operation on line bundles, with identity element R.

Lemma C.1.2 (c.f. Lemma 3.1[82]). *If L is a line bundle, then the dual module $\widehat{L} = Hom_R(L, R)$ is also a line bundle and $\widehat{L} \otimes_R L \simeq R$.*

Definition C.1.3 (c.f. [82]). *The Picard group $Pic(R)$ of a commutative ring R is the set of isomorphism classes of line bundles over R. As we have seen, the tensor product $\otimes_R$ endows $Pic(R)$ with the structure of an abelian group, the identity element being $[R]$ and the inverse being $L^{-1} = \widehat{L}$.*

Proposition C.1.4 (c.f. Proposition 3.2. [82]). *Pic is a functor from commutative rings to abelian groups. That is, if $R \to S$ is a ring homomorphism then $Pic(R) \to Pic(S)$ is a homomorphism sending L to $L \otimes_R S$.*

Lemma C.1.5 (c.f. Lemma 3.3 [82]). *If L is a line bundle, then $End_R(L) \simeq R$.*

C.2. Determinant line bundle of a projective module.

If M is any module over a commutative ring R and $k \geq 0$, the k-th exterior power $\wedge^k M$ is the quotient of the k-fold tensor product $M \otimes \ldots \otimes M$ by the submodule generated by terms $m_1 \otimes \ldots \otimes m_k$ with $m_i = m_j$ for some $i \neq j$. By convention, $\wedge^0 M = R$ and $\wedge^1 M = M$. Here are some classical facts (see [82]) :

i) $\wedge^k(R^n)$ is the free module of $rank\binom{n}{k}$ generated by terms $e_{i_1} \wedge \ldots \wedge e_{i_k}$ with $1 \leq i_1 < \ldots < i_k \leq n$. In particular, $\wedge^n(R^n) \simeq R$ on $e_1 \wedge \ldots \wedge e_n$

ii) If $R \to S$ is a ring map, there is a natural isomorphism $(\wedge^k M) \otimes_R S \simeq \wedge^k(M \otimes_R S)$ the first $\wedge_k$ being taken over R and the second being taken over S. In particular, $rank(\wedge_k M) = \binom{rank\ M}{k}$ as functions from $Spec(R)$ to $\mathbb{N}$

iii) (Sum Formula) There is a natural isomorphism

$$\wedge^k(P \oplus Q) \cong \bigoplus_{i=0}^{k} (\wedge^i P) \otimes (\wedge_{k-i} Q).$$

If P is a projective module of constant rank n, then $\wedge^k P$ is a finitely generated projective module of constant rank $\binom{n}{k}$, because $\wedge^k P$ is locally free. We write $det(P)$ for $\wedge^n P$, and call it the determinant line bundle of P.

1. If the rank of a projective module P is not constant, we define the determinant line bundle det(P) componentwise.

As the name suggests, the determinant line bundle is related to the usual determinant of a matrix. An $n \times n$ matrix g is just an endomorphism of R^n, so it induces an endomorphism $\wedge^n g$ of $\wedge^n R^n \simeq R$. By inspection, $\wedge^n g$ is multiplication by $det(g)$.

Proposition C.2.1 (c.f. Proposition 3.4 [82])**.** *Let R be a commutative noetherian 1-dimensional ring. Then all finitely generated projective R-modules are completely classified by their rank and determinant. In particular, every finitely generated projective R-module P of rank ≥ 1 is isomorphic to $L \oplus R^f$, where $L = det(P)$ and $f = rank(P) - 1$.*

Appendix D

Approach to convolutional codes from its generator matrix.

Generator matrix G aproximates to $\mathcal{C} \subset \mathbb{F}[z]^n$ in some ways: Polynomial approach, Scalar approach and The state diagram approach.

D.1. Polinomial approach.

If we use polynomial matrix $G(z)$ to encode scalar information then the information in bits is identified with coefficients of a k-uple of polynomials $I = (I_0(z), ..., I_{k-1}(z))$. Then the codeword $C = (C_0(z), ..., C_{n-1}(z))$ would be a n-uple of polynomials defined by $C = I \cdot G$ where $\cdot$ is the product of matrices.

Example D.1.1. *We consider a convolutional code over with an alphabet $\mathbb{Z}/2\mathbb{Z}$ that is characterized by the matrix $G = (z^2+1, z^2+z+1)$. Let $I = (z^3+z+1)$ be the information. Then the codeword C generated is*

$$C = I \cdot G = (z^3 + z + 1)(z^2 + 1, z^2 + z + 1) = (z^5 + z^2 + z + 1, z^5 + z^4 + 1).$$

D.2. Scalar approach.

The most natural way to represent a codeword $C = ((C_0(z), ..., C_{n-1}(z))$ is to get associated polynomical coefficients. From generator matrix $G(z)$ it is easy to construct a scalar version of G with the property $\mathbf{G} = \sum_{\nu=0}^{M} G_\nu z^\nu$ where $\mathbf{G}$ is the expansion of a polynomial of degree M with coefficients G_ν that are matrices of scalars $k \times n$.

This scalar matrix has an infinity number of rows and columns because the information and the polynomical codewords could be arbitrarily so big as we want.

Example D.2.1. *Let $G = (z^2 + 1, z^2 + z + 1)$ be over $\mathbb{Z}/2\mathbb{Z}$. We can see this matrix in the folllowing way*

$$\mathbf{G} = [1, 1] + [0, 1]z + [1, 1]z^2$$

Then scalar matrix generated by the associated convolutional code to G is

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 0 & 1 & 1 & 1 & & \\ & & & & 1 & 1 & 0 & 1 & 1 & 1 \\ & & & & & & & & & \dots \end{pmatrix}$$

Example D.2.2. *Scalar information that corresponds to polynomial $I = (z^3 + z + 1)$ is* 1101 *and the codeword in the scalar way that is associated with the word $C = (z^5 + z^2 + z + 1, z^5 + z^4 + 1)$ is* (111001100011).

The degree of information and the codeword could be as large as we want, but in the practical applications there exists a maximum degree allowed. The degree is called the L-th truncation of a convolutional code.

Definition D.2.3. *It is required that $gr[I_i(z)] \leq L - 1$ for $I = 0, 1, , , K - 1$ so that in the polynomical codeword $C = (C_0(z), ..., C_{n-1}(z))$ we have an associated scalar vector whose components have degree minor or equal to $M + L - 1$. The information $I = (I_0(z), ..., I_{k-1}(z))$ could be represented by kL bits and the codeword C by $n(M + L)$ bits.*

Map of encoding that lets us get C from I could be represented, in scalar notation, as $C = I \cdot G_L$, where scalar matrix G_L is lthe truncated matrix G. The L-th truncation of a convolutional code (n, k) could be studied as a linear block code $(n(M + L), KL)$ and so, a convolutional code is a special block code. The ratio of truncation is given by

$$R_L = \frac{kL}{n(M+L)} = R(1 - \frac{M}{M+L})$$

where $R = \frac{k}{n}$ is the ratio of the convolutional code without truncation.

Example D.2.4. *In the code $\mathcal{C}$ of the example (D.1.1) with $L = 6$ we get a linear block code with encoder*

$$\mathbf{G_6} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & & & & & & & & \\ & & & 1 & 1 & 0 & 1 & 1 & 1 & & & & & \\ & & & & & 1 & 1 & 0 & 1 & 1 & 1 & & & \\ & & & & & & & 1 & 1 & 0 & 1 & 1 & 1 & \\ & & & & & & & & & 1 & 1 & 0 & 1 & 1 & 1 \\ & & & & & & & & & & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

D.3. The shift-register approach.

From the shift-register viewpoint a $\mathcal{C}$ is the collection of all possible output streams from a particular encoder. The shift-register approach gives us directly the most powerful known approach **the state-diagram approach** that allows us to understand an encoder like a process modeled by the linear dinamic system. We can see in the Figure D.1

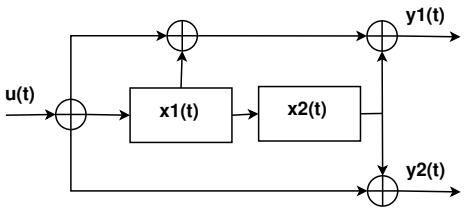
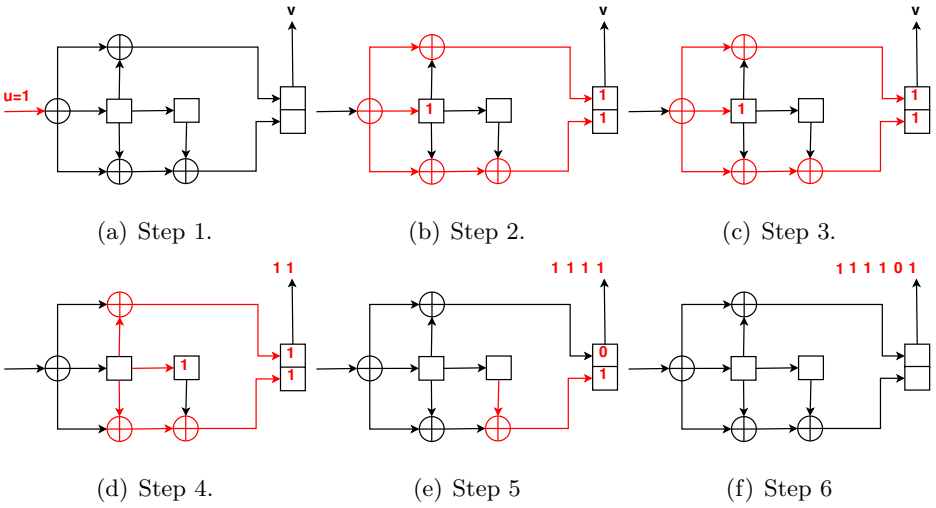


Figure D.1: Encoder like a linear dynamical system

Example D.3.1. *We suppose that we consider a convolutional code over* $\mathbb{F} = \mathbb{Z}_2$ *that consists of two shift registers, three binary adders, and a two-bit output buffer which emits two bits in every shift. The input-output function of this shift-register sequence is linear (because only linear elements are involved) and time- invariant: a delay of 1 shift at the input causes a delay of 2 shifts at the output. Thus, we get a convolutional code* $(2, 1)$*. We can see the example of an input of* $u = 1$ *in the Figure D.2.*



(a) Step 1. (b) Step 2. (c) Step 3.

(d) Step 4. (e) Step 5 (f) Step 6

Figure D.2: A convolutional code over $\mathbb{Z}/2\mathbb{Z}$.

Then the generator polynomial is $G(x) = C[1] = 1 + x + x^2 + x^3 + 0x^4 + x^5$