Convolutional codes under control theory point of view. Analysis of output-observability

M. I. GARCÍA-PLANAS
Universitat Politècnica de Catalunya
Departament de Matemàtica Aplicada
Mineria 1, 08038 Barcelona
SPAIN
maria.isabel.garcia@upc.edu

El M. SOUIDI
Université Mohammed V
Département d'Informatique
B. P. 1014, Rabat
MOROCCO
emsouidi@yahoo.com

L.E. UM
Université Mohammed V
Département d'Informatique
B. P. 1014 , Rabat
MOROCCO
laurainlee@yahoo.fr

Abstract: In this work we make a detailed look at the algebraic structure of convolutional codes using techniques of linear systems theory. The connection between these concepts help to better understand the properties of convolutional codes, in particular the concepts of controllability and observability of linear systems can be translated into the context of convolutional codes relating these properties with the noncatastrophicity of the codes. We examine the output-observability property and we give conditions for this property.

Key–Words: Codes, linear systems, output-observability.

1 Introduction

At the origin, coding theory has been devoted mainly to information theory. In coding theory had in fact emerged from the need for better communication and better computer data storage. Concretely, convolutional codes are used on many occasions to transfer data with high demands on speed. To this end, we require potent codes of high rates. These codes are frequently implemented in composite with a hard-decision code, particularly Reed Solomon. Before turbo codes, such constructions were the most efficient, coming closest to the Shannon limit.

The convolutional codes are binary codes that are an alternative to the block codes by their simplicity of generation with a little shift register. Convolutional codes were introduced by Elias [1] which suggests using a polynomial matrix $G(z)$ in the encoding process and allow the generation of the code line without using a previous buffer. G. D Forney in [2] 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.

A key problem in convolutional codes theory was to find a method for constructing codes of a given rate and complexity with good free distance. Several methods have been introduced for this task. There is a considerable amount of literature on the theory of convolutional codes over finite fields, (see [1, 3, 4, 5, 6, 7] for example).

It is well known the connection between convolutional codes and linear system theory over finite fields. So, a description of convolutional codes can be provided by a time-invariant discrete linear system (see [7, 8]). We want to note that linear systems theory is quite general and it permits all kinds of time axes and signal spaces.

The aim of this work is to analyze properties of convolutional codes with the help of the tools of systems theory. Input-output representation of a convolutional code is presented, and output-observable systems are characterized. The output-observability describes the possibility to know the states by the knowledge of the outputs. In this paper a new test for system theory and convolution codes to compute output-observability is presented that is simpler to use than those existing in the literature.

In the case of state space linear systems over real or complex numbers the control problem has been largely studied (see [9, 10, 11] for example). Control problem for systems over commutative rings has also been studied (see [12] for example). For convolutional codes theory, Rosenthal [13], presented a first step toward an algebraic decoding algorithm. It is based on an input/state/output description of the code and relies on the controllability matrix being the parity check matrix of an algebraically decodable block code. More recently other authors also study convolutional codes using the tools of control theory [14, 15, 16].

2 Preliminaries

In this section, we present some basic notions about codes theory.

ISBN: 978-1-61804-164-7

Let $\mathcal{A} = \{a_1, \cdots, a_q\}$ be a finite set of symbols, called alphabet of the message. We denote by $\mathcal{M}$ the set containing all sequences of symbols in $\mathcal{A}$ of length k. Also we denote by $\mathcal{R}$ the set consisting of all sequences of symbols in $\mathcal{A}$ of length n. We consider k and n positive integers with $k \leq n$.

We are interested in the case when $\mathcal{A} = \mathbb{F}_q$ is a commutative finite field of q elements.

Consider $f : \mathcal{A} \longrightarrow \mathcal{A}^*$ where $\mathcal{A}^* = \bigcup_{n \geq 0} \mathcal{A}^n$ and $\mathcal{A}^n = \mathcal{A} \times \ldots \times \mathcal{A}$.

A code is defined as the image $f(\mathcal{A}^n) = \mathcal{C} \subseteq \mathcal{A}^*$.

We remark the following concepts:

- The left translation operator σ and the right translation operator σ^{-1} over the sequence spaces $\mathcal{A}^*$ are defined as: $\sigma(a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots)$, $\sigma^{-1}(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots)$,
- $\mathcal{C} \subseteq \mathcal{A}^*$ is said to be invariant by right (left) translation when $\sigma^{-1}\mathcal{C} \subseteq \mathcal{C}$ ($\sigma\mathcal{C} \subseteq \mathcal{C}$).
- If for each element of $\mathcal{C}$ there is a finite number of non-zero elements, we say that $\mathcal{C}$ is compact.

Definition 1 *An error correcting code $\mathcal{C} \subseteq \mathcal{A}^*$ is said that is a convolutional code, when $\mathcal{C}$ is linear (considered as a vector space over $\mathbb{F}_q$ with the usual sum of vectors) invariant by right translation operator and has compact support.*

Following Rosenthal and York [8], a convolutional code is defined as a submodule of $\mathbb{F}^n[s]$.

Definition 2 *Let $\mathcal{C} \subseteq \mathcal{A}^*$ be a code. Then $\mathcal{C}$ is a convolutional code if and only if $\mathcal{C}$ is a $\mathbb{F}[s]$-submodule of $\mathbb{F}^n[s]$.*

Corollary 3 ([8]) *There exists an injective morphism of modules*

$$\begin{array}{rl} \psi : \mathbb{F}^k[s] & \longrightarrow \mathbb{F}^n[s] \\ u(s) & \longrightarrow v(s). \end{array} \tag{1}$$

Equivalently, there exists a polynomial matrix $G(s)$ (called encoder) of order $n \times k$ and having maximal rank such that

$$\mathcal{C} = \{v(s) \mid \exists u(s) \in \mathbb{F}^k[s] : v(s) = G(s)u(s)\}. \tag{2}$$

The rate k/n is known as the ratio of a convolutional code. We denote by ν_i the maximum of all degrees of each of the polynomials of each line, we define the complexity of the encoder as $\delta = \sum_{i=1}^{n} \nu_i$, and finally we define the complexity convolution code $\delta(\mathcal{C})$ as the maximum of all degrees of the largest minors of $G(s)$.

The representation of a code by means a polynomial matrix is not unique, but we have the following proposition.

Proposition 4 ([8]) *Two $n \times k$ rational encoders $G_1(s)$, $G_2(s)$ define the same convolutional code, if and only if there is a $k \times k$ unimodular matrix $U(s)$ such that $G_1(s)U(s) = G_2(s)$.*

After a suitable permutation of the rows, we can assume that the generator matrix $G(s)$ is of the form

$$G(s) = \begin{pmatrix} P(s) \\ Q(s) \end{pmatrix} \tag{3}$$

with right coprime polynomial factors $P(s) \in \mathbb{F}^{(n-k)\times k}$ and $Q(s) \in \mathbb{F}^{k\times k}$, respectively.

It is possible to consider the equivalent rational encoder

$$\begin{pmatrix} P(s) \\ Q(s) \end{pmatrix} Q^{-1}(s) = \begin{pmatrix} P(s)Q^{-1}(s) \\ I \end{pmatrix}. \tag{4}$$

2.1 Systems and Codes

A dynamic system is a model of an isolated fragment of the nature with a dynamic behavior that can be observed and studied: This behavior is the response of the system to an external stimulus or response to initial conditions, and this response may not be always the same, but rather depend also on the current circumstances of the dynamical system.

In other words, a dynamic system is a process which has a magnitude which varies with the time according a deterministic or stochastic law. More specifically ([17]):

Definition 5 *A discrete linear time-invariant system is described by the equations*

$$\left.\begin{array}{rl} x(t+1) & = Ax(t) + Bu(t) \\ y(t) & = Cx(t) + Du(t) \end{array}\right\} \tag{5}$$

where $A \in M_\delta(\mathbb{F})$, $B \in M_{\delta\times k}(\mathbb{F})$, $C \in M_{(n-k)\times\delta}(\mathbb{F})$, $D \in M_{(n-k)\times k}(\mathbb{F})$ are constant matrices over the field $\mathbb{F}$, and $u(t) \in \mathbb{F}^k$, $x(t) \in \mathbb{F}^\delta$, $y(t) \in \mathbb{F}^p$ are the input, state and output vectors, respectively.

For simplicity and if confusion is not possible we simply write $p = n - k$. Also we will denote a system as the quadruple of matrices (A, B, C, D).

A solution of the system (5) can be obtained making use the Z-transform. Let $U(s)$, $X(s)$, $Y(s)$ be

ISBN: 978-1-61804-164-7

the Z-transforms of the variables u, x, y of a time invariant linear system. Then by applying the Laplace transform to the equations of the system (5) we have

$$\left.\begin{array}{rl} sX(s) & = AX(s) + BU(s) \\ Y(s) & = CX(s) + DU(s) \end{array}\right\} \qquad (6)$$

and as a result we have

$$Y(s) = (C(sI - A)^{-1}B + D)U(s), \qquad (7)$$

called the transfer function of the system and

$$C(sI - A)^{-1}B + D \qquad (8)$$

the matrix transfer.

The transfer function formulation of the system does not give information about the behavior inside the system, such as unobservable unstable modes. Therefore, the transfer matrix cannot be used to study the control properties of a system. The input-output description permits to study the control properties of a dynamical system.

Definition 6 *A realization of a proper rational matrix $H(s)$ is a linear system (A, B, C, D) such that its transfer matrix $C(sI - A)^{-1}B + D$ is $H(s)$.*

From now on we consider a realization (A, B, C, D) of the rational matrix $P(s)Q^{-1}(s)$ obtained from the matrix code $G(s)$.

Example 1 Let $G(s)$ the following encoder matrix

$$G(s) = \begin{pmatrix} 1 + s + s^2 \\ 1 + s^2 \end{pmatrix} = \begin{pmatrix} P(s) \\ Q(s) \end{pmatrix} \qquad (9)$$

So, $C(sI - A)^{-1}B + D = P(s)Q(s)^{-1} = \frac{1+s+s^2}{1+s^2}$ and we can decompose $P(s)Q(s)^{-1}$ into a polynomial matrix and a strictly proper matrix: $P(s)Q(s)^{-1} = 1 + \frac{s}{1+s^2}$. Then, we take the matrix D as the polynomial, and $C(sI - A)^{-1}B$ the strictly rational part.

So, $D = 1$ and $C(sI - A)^{-1}B = \frac{c_0+c_1 s}{a_0+a_1 s+s^2}$. Then $A = \begin{pmatrix} -a_1 & -a_0 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $C = \begin{pmatrix} c_1 & c_0 \end{pmatrix}$. So, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 0 \end{pmatrix}$.

3 Output-observability

Related to the minimality realization of an encoder is the output observability property.

Definition 7 ([3]) *The system (A, B, C, D) is said be output observable if the state sequence $x(0), \dots, x(\ell)$ is determined by the knowledge of the output sequence $y(0), \dots, y(\ell)$ for a finite number of steps $\ell \in \mathbb{N}$.*

We observe that $x(1), \dots, x(\ell)$ are determined by the knowledge of $x(0)$ and $u(0), \dots, u(\ell-1)$ because of

$$\begin{array}{rl} x(1) & = Ax(0) + Bu(0) \\ x(2) & = Ax(1) + Bu(1) = \\ & = A^2x(0) + ABu(0) + Bu(1) \\ \vdots & \\ x(\ell) & = Ax(\ell-1) + Bu(\ell-1) = \\ & = A^\ell x(0) + A^{\ell-1}Bu(0) + \dots + \\ & \; +ABu(\ell-2) + Bu(\ell-1), \end{array} \qquad (10)$$

and the elements $x(0)$, and $u(0), \dots, u(\ell-1)$ can be obtained solving the following system of matrix equations.

$$\begin{array}{rl} y(0) & = Cx(0) + Du(0) \\ y(1) & = Cx(1) + Du(1) = \\ & = CAx(0) + CBu(0) + Du(1) \\ \vdots & \\ y(\ell) & = Cx(\ell) + Du(\ell) = \\ & = CA^\ell x(0) + CA^{\ell-1}Bu(0) + \dots + \\ & \; +CBu(\ell-1) + Du(\ell) \end{array} \qquad (11)$$

Calling $T_\ell(A, B, C, D)$ (that we simple write T_ℓ if confusion is not possible) the matrix

$$T_\ell = \begin{pmatrix} C & D & & & & \\ CA & CB & D & & & \\ CA^2 & CAB & CB & D & & \\ \vdots & & \ddots & \ddots & & \\ CA^\ell & CA^{\ell-1}B & CA^{\ell-2}B & \dots & CB & D \end{pmatrix} \qquad (12)$$

We have the following.

Proposition 8 *A system (A, B, C, D) is output observable if and only if the matrix T_ℓ has full row rank for all $\ell \in \mathbb{N}$.*

Proof:

First of all, we observe that for each ℓ, the matrix T_ℓ is the corresponding matrix to de system (11). So, if the number of rows is bigger than the number of columns, there are values of $y(0), \dots, y(\ell)$for which the system has no solution.

Therefore, we assume that the number of rows is less than or equal to the number of columns. It is well known that in this case and for each ℓ, the systems

ISBN: 978-1-61804-164-7

(11) have a solution for all $y(0), \dots, y(\ell)$if and only if the systems have full rank. □

Let (A, B, C, D) be a system and we consider the matrices that we will write $M_\ell(A, B, C, D)$ (that we simply write M_ℓ if confusion is not possible) defined in the following manner:

$$
\begin{array}{l}
M_0 = \begin{pmatrix} C & D \end{pmatrix}\\
M_\ell = \begin{pmatrix}
A & B & -I & 0 & 0 & 0 & \dots & & 0 & 0\\
C & D & 0 & 0 & 0 & 0 & & & & \\
0 & 0 & A & B & -I & 0 & & & & \\
0 & 0 & C & D & 0 & 0 & & & & \\
\vdots & & & & & \ddots & & & & \\
 & & & \dots & & & A & B & -I & 0\\
 & & & \dots & & & C & D & 0 & 0\\
 & & & \dots & & & 0 & 0 & C & D
\end{pmatrix}\\
\in M_{(\ell(\delta+p)+p)\times(\ell+1)(\delta+k)}(\mathbb{F}).
\end{array}
\tag{13}
$$

We have the following result.

Theorem 9 *Let (A, B, C, D) be a system. Then*

$$\operatorname{rank} T_\ell + \ell\delta = \operatorname{rank} M_\ell.$$

Proof: Making block row and column elementary transformations, we have

$$
\operatorname{rank}\begin{pmatrix}
A & B & -I & 0 & 0 & 0 & \dots & & 0 & 0\\
C & D & 0 & 0 & 0 & 0 & & & & \\
0 & 0 & A & B & -I & 0 & & & & \\
0 & 0 & C & D & 0 & 0 & & & & \\
\vdots & & & & & \ddots & & & & \\
 & & & \dots & & & A & B & -I & 0\\
 & & & \dots & & & C & D & 0 & 0\\
 & & & \dots & & & 0 & 0 & C & D
\end{pmatrix} =
\operatorname{rank}\begin{pmatrix}
I & & & & & & \\
 & \ddots & & & & & \\
 & & I & & & & \\
 & & & C & D & & \\
 & & & CA & CB & D & \\
 & & & CA^2 & CAB & CB & D \\
 & & & \vdots & & \ddots & \\
 & & & CA^\ell & CA^{\ell-1}B & & CB & D
\end{pmatrix}
\tag{14}
$$

□

In order to obtain properties, we define the following equivalence relation preserving the required properties.

Definition 10 *The systems (A, B, C, D) and (A_1, B_1, C_1, D_1) are feedback equivalent, that we write*

$$(A, B, C, D) \sim (A_1, B_1, C_1, D_1), \tag{15}$$

if and only if

$$\begin{pmatrix} A_1 & B_1\\ C_1 & D_1\end{pmatrix} = \begin{pmatrix} P^{-1} & W\\ 0 & S\end{pmatrix}\begin{pmatrix} A & B\\ C & D\end{pmatrix}\begin{pmatrix} P & 0\\ V & R\end{pmatrix} \tag{16}$$

for some matrices $P \in M_\delta(\mathbb{F})$, $R \in M_k(\mathbb{F})$, $S \in M_p(\mathbb{F})$, $V \in M_{k\times\delta}(\mathbb{F})$ and $W \in M_{\delta\times p}(\mathbb{F})$.

Remark 11 *Note that this equivalence generalizes the similarity equivalence:*

$$(A, B, C, D) \simeq (A_1, B_1, C_1, D_1) \tag{17}$$

if and only if

$$(A_1, B_1, C_1, D_1) = (P^{-1}AP, P^{-1}B, CP, D) \tag{18}$$

It suffices to take $V = 0$, $W = 0$, $R = I_m$, $S = I_p$.

Proposition 12 *Let (A, B, C, D) and (A_1, B_1, C_1, D_1) be equivalent systems under equivalence relation considered. Then*

$$\operatorname{rank} M_\ell(A, B, C, D) = \operatorname{rank} M_\ell(A_1, B_1, C_1, D_1),$$

for all $\ell \in \mathbb{N}$.

Proof:

Calling

$$
\mathbf{P} = \begin{pmatrix}
P^{-1} & W & & & & & & \\
0 & S & & & & & & \\
0 & 0 & P^{-1} & W & & & & \\
0 & 0 & 0 & S & & & & \\
 & & & & \ddots & & & \\
 & & & & & P^{-1} & W & \\
 & & & & & 0 & S & \\
 & & & & & & & S
\end{pmatrix}
\tag{19}
$$

and

$$
\mathbf{Q} = \begin{pmatrix}
P & 0 & & & & & & \\
V & R & & & & & & \\
 & & P & 0 & & & & \\
 & & V & R & & & & \\
 & & & & \ddots & & & \\
 & & & & & P & 0 & \\
 & & & & & V & R & \\
 & & & & & & & R \\
 & & & & & & & & R
\end{pmatrix}
\tag{20}
$$

We have:

$$\mathbf{P}\begin{pmatrix} A & B & -I & 0 & 0 & 0 & \dots & & 0 & 0 \\ C & D & 0 & 0 & 0 & 0 \\ 0 & 0 & A & B & -I & 0 \\ 0 & 0 & C & D & 0 & 0 \\ \vdots & & & & & \ddots \\ & & & \dots & & & A & B & -I & 0 \\ & & & \dots & & & C & D & 0 & 0 \\ & & & \dots & & & 0 & 0 & C & D \end{pmatrix}\mathbf{Q} = \begin{pmatrix} A_1 & B_1 & -I & 0 & 0 & 0 & \dots & & 0 & 0 \\ C_1 & D_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & A_1 & B_1 & -I & 0 \\ 0 & 0 & C_1 & D1 & 0 & 0 \\ \vdots & & & & & \ddots \\ & & & \dots & & & A_1 & B_1 & -I & 0 \\ & & & \dots & & & C_1 & D_1 & 0 & 0 \\ & & & \dots & & & 0 & 0 & C_1 & D1 \end{pmatrix}. \quad (21)$$

Then, both matrices have the same rank. □

Corollary 13 *Let* (A, B, C, D), *and* (A_1, B_1, C_1, D_1) *be two equivalent systems under equivalence relation considered. Then*

$$\operatorname{rank} T_\ell(A, B, C, D) = \operatorname{rank} T_\ell(A_1, B_1, C_1, D_1), \quad (22)$$

for all $\ell \in \mathbb{N}$.

4 New test for output-observability

Remark 14 *It is obvious than if the matrix* T_ℓ *(consequently* M_ℓ*) has full row rank for some* $\ell \in \mathbb{N}$*, then all matrices* T_j *(consequently* M_j*) with* $j \leq \ell$ *have full row rank.*

Moreover we have the following.

Proposition 15 *Let* (A, B, C, D) *be a system. For all* $\ell \geq n$ *we have that*

$$\operatorname{rank} T_{\ell+1} - \operatorname{rank} T_\ell = \operatorname{rank} T_{\ell+2} - \operatorname{rank} T_{\ell+1} \quad (23)$$

Proof:

Let (A, B, C, D) be a system, taking into account Proposition 12 and Corollary 13, we can consider an equivalent system in the form (A_1, B_1, C_1, D_1) with $A_1 = \begin{pmatrix} 0 & \bar{A}_1 \\ 0 & \bar{A}_2 \end{pmatrix}$, $B_1 = \begin{pmatrix} \bar{B}_1 & 0 \\ \bar{B}_2 & 0 \end{pmatrix}$, $C_1 = \begin{pmatrix} I_c & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$, $D_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & I_d \end{pmatrix}$ with $\bar{A}_2 \in M_{\delta-c}(\mathbb{F})$.

In the case where $d = p$, the matrix $C_1 = 0$ and the result is obvious,

In the case where $d = k$ the matrix $B_1 = 0$. Calling $\bar{C} = \begin{pmatrix} I_c & 0 \\ 0 & 0 \end{pmatrix}$ and taking into account that $A^\delta = \sum_{i=0}^{\delta-1} A^i$, we have

$$\operatorname{rank}\begin{pmatrix} \bar{C} \\ 0 & I_d \\ \bar{C}A & 0 & 0 \\ 0 & 0 & I_d \\ \vdots & & & \ddots \\ CA^{\delta-1} & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & \ddots & I_d \\ 0 & 0 & 0 & 0 & \ddots & & 0 \\ 0 & 0 & 0 & 0 & \ddots & & I_d \\ \vdots \end{pmatrix}. \quad (24)$$

Then,

$$\operatorname{rank} T_{\ell+1} - \operatorname{rank} T_\ell = d, \ \forall \ell \geq \delta. \quad (25)$$

Suppose now, $d \neq p, k$. Firstly, we analyze the particular case where $\bar{A}_1 = 0$. It is easy to observe that

$$\operatorname{rank} T_{\ell+1} - \operatorname{rank} T_\ell = \operatorname{rank} \bar{B}_1 + d.$$

We observe that this case includes one the more particular where $c = \delta$ and then $A_1 = 0$.

Then, we analyze the case $\bar{A}_1 \neq 0$. We have

$$\operatorname{rank} M_\ell = \begin{pmatrix} I_r \\ & I_d \\ & & \ddots \\ & & & I_d \\ & & & & \bar{A}_1 & \bar{B}_1 \\ & & & & \bar{A}_1\bar{A}_2 & \bar{A}_1\bar{B}_2 & \bar{B}_1 \\ & & & & \vdots & & & \ddots \\ & & & & \bar{A}_1\bar{A}_2^\ell & \bar{A}_1\bar{A}_2^{\ell-1} & \dots & \bar{A}_1\bar{B}_2 & \bar{B}_1 \end{pmatrix} \quad (26)$$

Now, we consider the following reduced order system $(\bar{A}_2, \bar{B}_2, \bar{A}_1, \bar{B}_1)$ and we apply the previous steps. □

Corollary 16 *Let* (A, B, C, D) *be a system. For all* $\ell \geq n$ *we have that*

$$\operatorname{rank} M_{\ell+1} - \operatorname{rank} M_\ell = \operatorname{rank} M_{\ell+2} - \operatorname{rank} M_{\ell+1} \quad (27)$$

As a corollary, and taking into account remark 14, we can conclude the following result.

ISBN: 978-1-61804-164-7

Theorem 17 (Main Theorem) *A system (A, B, C, D) is output observable if and only if the matrix M_δ has full row rank.*

This theorem provides an iterative method to compute functional output-observability.

Algorithm

Step 1: Compute rank M_0. If rank $< p$ the system is not output observable,

If rank $= p$, then

Step 2: Compute rank M_ℓ. If rank $< (\ell + 1)p + \ell\delta$ the system is not output observable.

If rank $= (\ell + 1)p + \ell\delta$ and $\ell = \delta$ the system is output observable, and if $\ell < \delta$ go to step 2.

Example 2

Let (A, B, C, D) be a system with $A = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 1 \end{pmatrix}$ and $D = (0)$.

Applying the test we obtain:

1) rank $\begin{pmatrix} C & D \end{pmatrix} = 1 = p$,

2) rank $\begin{pmatrix} A & B & -I & 0 \\ C & D & 0 & 0 \\ 0 & 0 & C & 0 \end{pmatrix} = 1 < 3 = \ell(p+1)+p.$

Then, the system is not output observable.

Notice that using standard test ([3]) we need to compute CA^i and $CA^{i-1}B$ for $1 \leq i \leq \ell$ before to compute the ranks of matrices T_i. Clearly, the new test reduces tasks.

5 Conclusions

In this paper a detailed look at the algebraic structure of convolutional codes using techniques of linear systems theory has been made. The output-observability property has been analyzed and conditions for this property have been given. Finally, an algorithm to evaluate the output-observability is presented. Output observability represents the possibility of an internal state, to be only defined by a finite set of outputs, for a finite number of steps. The output observability character is related to the minimality realization of an encoder in the following sense, among all encoders that produce the same set of output sequences, the one using the smallest number of memory elements is output observable and vice versa. Therefore it is useful to have a simple and computable method to determine whether or not a system is output observable.

References:

[1] P. Elias, *Coding for Noisy Channels*, IRE Conv.Rec. **4**, pp. 37-46, (1955) .

[2] G. D. Forney, *Convolutional codes: Algebraic structure*. IEEE trans. Information Theory, (1970).

[3] Ch. Fragouli, R. D. Wesel, *Convolutional Codes and Matrix Control Theory*, Proceedings of the 7th International Conference on Advances in Communications and Control, Athens, Greece, (1999).

[4] 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. **11** (4), (2010), pp. 324-333.

[5] H. Gluesing-Luerssen., U. Helmke, J.I. Iglesias Curto Algebraic Decoding for Doubly Cyclic Convolutional Codes, Advances in Mathematics of Communications **4**, pp. 83-99, (2010).

[6] M. Kuijper, R. Pinto, *On minimality of convolutional ring encoders*. IEEE Trans. on Information Theory, **55**, (11), pp. 4890-4897, (2009).

[7] 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).

[8] J. Rosenthal, E. V. York, *BCH Convolutional Codes*, IEEE Trans. Information Theory vol. 45 (6), 1833-1844, (1999).

[9] A. Díaz, Mª I. García-Planas, *An alternative collection of structural invariants for matrix pencils under strict equivalence*, Wseas Transactions on Systems and Control, **4**, (10), pp 487-496, (2009).

[10] Mª I. García-Planas, *Bifurcation diagrams of generic families of singular systems under proportional and derivative feedback*. Wseas Transactions on Mathematics, **7** (2), 1-11, (2008).

[11] J.L. Domínguez, M.I. Garcia-Planas, B. Mediano, *Input Observability Analysis of Fixed Speed Wind Turbine*. Mathematical Modelling and Simulation in Applied Sciences. Wseas Press, pp. 13-19, (2012).

[12] H. Loeliger, G. D. Forney, T. Mittelholzer, M.D. Trot, *Minimality and observability of group systems*, Linear Algebra and its Applications, **205-206**, pp. 937-963, (1994).

[13] J. Rosenthal, *An algebraic decoding algorithm for convolutional codes*. In G. Picci and D. S. Gilliam, editors, Dynamical Systems, Control, Coding, Computer Vision; New Trends, Interfaces, and Interplay, pp. 343-360. Birkhäuser, Basel, (1999).

[14] J-J. Climent, V. Herranz, C. Perea, *Linear system modelization of concatenated block and convolutional codes*, Linear Algebra and its Applications, **429**, pp. 1191-1212, (2008).

[15] R. Hutchinson, J. Rosenthal, R. Smarandache, *Convolutional codes with maximum distance profile*, Systems Control Lett. 54 (1), pp- 53-63, (2005).

[16] E. Zerz, *On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings* Asian Journal of Control, **12**, (2), pp. 119 126, (2010).

[17] J. W. Brewer, J. W. Bunce and F. S. VanVleck, *Linear systems over commutative rings*, Marcel Dekker, New York (1986).

ISBN: 978-1-61804-164-7