PHYSCON 2011, León, Spain, September, 5–September, 8 2011

ERROR CORRECTING CODES UNDER LINEAR SYSTEMS POINT OF VIEW

L.E. Um
Faculté des Sciences
Université Mohammed V Agdal
Morocco
laurainlee@yahoo.fr

El M. Souidi
Faculté des Sciences
Université Mohammed V Agdal
Morocco
emsouidi@yahoo.com

M. I. García-Planas
Departament de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Spain
maria.isabel.garcia@upc.edu

Abstract

In this work we make a detailed look at the algebraic structure of convolutional codes using techniques of linear systems theory. In particular we study the input-state-output representation of a convolutional code. We examine the output-controllability property and we give conditions for this property.

Key words

Codes, linear systems, output-controllability.

1 Introduction

The convolutional codes are binary codes that are an alternative to the block codes by their simplicity of generation with a little shift registers. The convolutional codes was introduced by Elias [P. Elias, (1955)] where it was suggested to use a polynomial matrix $G(z)$ in the encoding procedure and they allow to generate the code online without using a previous buffering. Convolutional codes are used extensively in numerous applications as satellite communication, mobile communication, digital video, radio among others.

There is a considerable amount of literature on the theory of convolutional codes over finite fields, (see [P. Elias, (1955), Ch. Fragouli, R.D. Wesel, (1999), M. Kuijper, R. Pinto, J,L Massey, M.K. Sain, (1967), J. Rosenthal, J.M. Schumacher, E.V. York, (1996)] for example).

A description of convolutional codes can be provided by a time-invariant discrete linear system called discrete-time state-space system in control theory.

The aim of this article is to make a survey of the convolutional codes with the help of the tools of systems theory, input-output representation of a convolutional code is examined, and output-controllable systems are characterized.

2 Preliminaries

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

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 be positive integers with $k \leq n$.

We are interested in the case when $\mathcal{A} = \mathbb{F}_q = GF(q)$ the Galois field of q elements $\mathbb{Z}_q$.

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

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 sequences 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 2.1. *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 [J. Rosenthal, E. V. York, (1999)], a convolutional code is defined as a submodule of $\mathbb{F}^n[s]$.

Definition 2.2. *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 2.1. *There exists an injective morphism of modules*

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

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

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

The rate k/n is known as the ratio of 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 2.1. *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 $G_1(s)U(s) = G_2(s)$.*

3 Systems and Codes

A dynamic system is a process which has a magnitude which varies with the time according a deterministic or stochastic law. More specifically:

Definition 3.1. *A dynamic system is a triple $\Sigma = (T, \mathcal{A}, \mathcal{B})$ where $T \subseteq \mathbb{R}$ is the time, $\mathcal{A}$ is the alphabet of signals, and $\mathcal{B} \subseteq \mathcal{A}^T \subset \mathcal{A}^*$ is the behavior. The elments of $\mathcal{B}$ are called trajectories.*

3.1 Realization

From now on $T = \mathbb{Z}^+$ $\mathcal{A} = \mathbb{F}^n$ where $\mathbb{F} = \mathbb{F}_q = GF(q)$ is finite field (the q elements Galois field).

Theorem 3.1. *Let $\mathcal{C} \subseteq \mathbb{F}^n[s]$ be un k/n-convolutional of complexity δ. Then, there exist matrices K, L of size $(\delta + n - k) \times \delta$ an a matrix M of size $(\delta + n - k) \times n$ having their coefficients in $\mathbb{F}$ such that the code $\mathcal{C}$ is defined as:*

$$\begin{aligned}\mathcal{C} = \{v(s) \in \mathbb{F}[s] \mid \exists x(s) \in \mathbb{F}^\delta[s] :\\ sKx(s) + Lx(s) + Mv(s) = 0\}\end{aligned}$$

Moreover, K is a column full rank matrix, $\begin{pmatrix} K & M \end{pmatrix}$ is a row full rank matrix and rang $\begin{pmatrix} s_0K + L & M \end{pmatrix} = \delta + n - k$, $\forall s_0 \in \mathbb{F}$.

The triple (K, L, M) satisfying the above it is called *minimal representation* of $\mathcal{C}$.

Proposition 3.1. *If (K_1, L_1, M_1) is another representation of the convolutional code $\mathcal{C}$. Then, there exist invertible matrices T and S of adequate size, such that*

$$(K_1, L_1, M_1) = (TKS^{-1}, TLS^{-1}, TM). \quad (1)$$

It is obvious that the relation (1), is an equivalence relation induced by the Lie group $\mathcal{G} = \{(T, S) \in Gl(\delta + n - k, \mathbb{F}) \times Gl(\delta; \mathbb{F})\}$.

Corollary 3.1. *The triple (K, L, M) can be written as:*

$$K = \begin{pmatrix} -I_\delta \\ 0 \end{pmatrix},\ L = \begin{pmatrix} A \\ C \end{pmatrix},\ M = \begin{pmatrix} 0 & B \\ -I_{n-k} & D \end{pmatrix}. \quad (2)$$

Corollary 3.2.

$$\begin{aligned}\mathcal{C} = \{v(s) \in \mathbb{F}[s] \mid \exists x(s) \in \mathbb{F}^\delta[s] :\\ \begin{pmatrix} sI-A & 0 & -B \\ -C & I & -D \end{pmatrix} \begin{pmatrix} x(s) \\ v(s) \end{pmatrix} = 0\}.\end{aligned}$$

Proof. From theorem 3.1, we have

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

and the result is obtained.

If we divide the vector $v(s)$ into two parts $v(s) = \begin{pmatrix} y(s) \\ u(s) \end{pmatrix}$ depending on the size of the matrix, the equality $\begin{pmatrix} sI-A & 0 & -B \\ -C & I & -D \end{pmatrix} \begin{pmatrix} x(s) \\ v(s) \end{pmatrix} = 0$ can be expressed as $\left.\begin{aligned} sx(s) = Ax(s) + Bu(s) \\ y(s) = Cx(s) + Du(s) \end{aligned}\right\}$. Applying the Z antitransform we obtain the system $\left.\begin{aligned} x_{t+1} = Ax_t + Bu_t \\ y_t = Cx_t + Du_t \end{aligned}\right\}$, $v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix}$, $x_0 = 0$.

3.2 Convolutional code as input-state-output

Let $\mathbb{F} = \mathbb{F}_q$ be the q-elements Galois field and consider the matrices $A \in \mathbb{F}^{\delta \times \delta}$, $B \in \mathbb{F}^{\delta \times k}$, $C \in \mathbb{F}^{(n-k) \times \delta}$ and $D \in \mathbb{F}^{(n-k) \times k}$. A convolutional code $\mathcal{C}$ of rate k/n and complexity δ can be described by the following linear system of equations:

$$\left.\begin{aligned} x_{t+1} = Ax_t + Bu_t \\ y_t = Cx_t + Du_t \end{aligned}\right\}, \quad \begin{aligned} v_t = \begin{pmatrix} y_t \\ u_t \end{pmatrix}, \\ x_0 = 0. \end{aligned} \quad (3)$$

In terms of systems theory the variable x_t is called a state variable of the system at time t, u_t the input vector and y_t the vector output obtained from the combination of input and state variable.

Based on the system (3), one can find a minimal representation of a code, it suffices simply to define the triple (K, L, M) as (2).

In terms of the theory of codes, we have the input of the encoder after time t which is called the information o vector message u_t; the vector y_t created by the encoder is called parity vector, the code vector v_t is transmitted via the communication channel. We will write the code convolution created in this way, for $\mathcal{C}(A, B, C, D)$.

We want to define an equivalence relation over the set of quadruples (A, B, C, D) in such way that the code representations (K, L, M), associated to the equivalent quadruples, are equivalent by the equivalence defined in (1). Then we consider the following equivalence relation:

Definition 3.2. *The quadruple* (A_1, B_1, C_1, D_1) *is equivalent to* (A, B, C, D) *if and only if, there exist an invertible matrix* S *in such a way that:*

$$(A_1, B_1, C_1, D_1) = (SAS^{-1}, SB, CS^{-1}, D). \quad (4)$$

Obviously

$$\left(\begin{pmatrix} -I_\delta \\ 0 \end{pmatrix}, \begin{pmatrix} A_1 \\ C_1 \end{pmatrix}, \begin{pmatrix} 0 & B_1 \\ -I_{n-k} & D_1 \end{pmatrix}\right) = \\ \left(\begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} -I_\delta \\ 0 \end{pmatrix}S^{-1}, \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} A \\ C \end{pmatrix}S^{-1}, \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix}\begin{pmatrix} 0 & B \\ -I_{n-k} & D \end{pmatrix}\right).$$

3.3 Output-Controllability

Now we introduce the following important property in the dynamical study of control systems.

Definition 3.3. *Dynamical system* (3) *is said to be output controllable if for every* $y(0)$ *and every vector* $y_1 \in \mathbb{R}^p$*, there exist a finite time* t_1 *and control* $u_1(t) \in \mathbb{R}^m$*, that transfers the output from* $y(0)$ *to* $y_1 = y(t_1)$*.*

Therefore, output controllability generally means, that we can steer output of dynamical system independently of its state vector.

For a linear continuous-time system, like (3), described by matrices A, B, C, and D, we define the output controllability matrix

$$oC = \begin{pmatrix} CB \; CAB \; \dots \; CA^{n-1}B \; D \end{pmatrix} \quad (5)$$

and we have the following result.

Theorem 3.2. *Dynamical system* (3) *is output controllable if and only if* rank $oC = p$*.*

Remark 3.1. *Another important property and largely studied is the state controllability characterized by the rank of the controllability matrix*

$$\mathcal{C} = \begin{pmatrix} B \; AB \; \dots \; A^{n-1}B \end{pmatrix}$$

in the sense that the dynamical system (3) *is controllable if and only if It should be pointed out, that the state controllability is defined only the matrix* $\mathcal{C}$ *has full row rank. for the linear differential state equation, whereas the output controllability is defined for the input-output description i.e., it depends also on the linear algebraic output equation. Therefore, these two concepts are not necessarily related.*

Proposition 3.2. *The output controllability character is invariant under feedback.*

Proof.

$$\begin{array}{l} (C + DF)(A + BF)^k B = \\ CA^k B + \sum_{0 \le \ell \le k-1} CA^{k-\ell-1} BF(A + BF)^\ell B + \\ DFA^k B + \sum_{0 \le \ell \le k-1} DFA^{k-\ell-1} BF(A + BF)^\ell B \end{array}$$

In the case where $D = 0$ a proof can be found in [J.L. Dominguez-García, M. I. García-Planas, (2011)]

The above proposition induces to consider the following equivalence relation

Definition 3.4. *The systems* $(A_i, B_i, C_i, D_i), i = 1, 2$ *are equivalents if and only if, there exist matrices* $S \in Gl(\delta; \mathbb{F})$*,* $R \in Gl(m; \mathbb{F})$*,* $T \in Gl(q; \mathbb{F})$*,* $F \in M_{m \times n}(\mathbb{F})$ *such that* $A_2 = SA_1S^{-1} + SB_1F$*,* $B_2 = SB_1R$*,* $C_2 = TC_1S + TD_1F^B$*,* $D_2 = TD_1R$*.*

It is immediate that if we take the subset formed by $R = I, T = I, F = 0$ we obtain the relation (4).

Proposition 3.3. *The output controllability is invariant under new equivalence relation*

Proposition 3.4. *Let* (A_i, B_i, C_i, D_i)*,* $i = 1, 2$ *two equivalent quadruples. Then*

$$\text{rank}\begin{pmatrix} C_1 & D_1 \end{pmatrix} = \text{rank}\begin{pmatrix} C_2 & D_2 \end{pmatrix}.$$

Proof.

$$\begin{array}{l} \text{rank}\begin{pmatrix} C_1 & D_1 \end{pmatrix} = \\ \text{rank}\, T\begin{pmatrix} C_1 & D_1 \end{pmatrix}\begin{pmatrix} S^{-1} & \\ F & R \end{pmatrix} = \text{rank}\begin{pmatrix} C_2 & D_2 \end{pmatrix}. \end{array}$$

In order to obtain conditions for output-controllability we consider an equivalent quadruple (A_c, B_c, C_c, D_c) with $D_c = \begin{pmatrix} 0 & 0 \\ 0 & I_d \end{pmatrix}$, $d = \text{rank}\, D$, $B_c = \begin{pmatrix} B_1 & 0, \end{pmatrix}$, $(A_c, B_1) = \left(\begin{pmatrix} N & \\ & J \end{pmatrix}, \begin{pmatrix} B_{11} \\ 0 \end{pmatrix}\right)$ is a pair of matrices in its Kronecker reduced form and $C_c = \begin{pmatrix} C_{11} & C_{12} \\ 0 & 0 \end{pmatrix}$, (all blocks in matrices are in adequate size).

Taking into account proposition 3.4 and the reduced form we can consider triples of matrices (A, B, C).

Theorem 3.3. *Let* (A, B, C) *be a triple of matrices in its reduced form. Then*

If $p > n$ the system is not output-controllable,
If $p \leq n$ the system is output-controllable if and only if $\operatorname{rank} C_{11} = p$*. In the particular case where* (A, B) *is completely controllable the condition is* $\operatorname{rank} C = p$*.*

Proof. Let $k_1 \leq \ldots \leq k_r$ the Kronecker indices of (A, B).

Observe that $C_{11} \in M_{p \times k_1 + \ldots + k_r}(\mathbb{F})$.

$$\begin{array}{l} \operatorname{rank} \left(CB\ CAB \ldots CA^{n-1}B\right) = \\ C_{11} \left(B_{11}\ NB_{11} \ldots N^{k_r}B_{11}\right). \end{array}$$

Matrix $\left(B_{11}\ NB_{11} \ldots N^{k_r}B_{11}\right)$ has full rank equal to $\sum_{i=1}^{k_r} k_i$.

Example 3.1. *Let* (A, B, C) *a triple with*

$$A = \begin{pmatrix} 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1 \\ 0\,0\,0\,0\,0 \end{pmatrix},$$

$$B = \begin{pmatrix} 0\,0\,0 \ldots 0 \\ 0\,0\,0 \ldots 0 \\ 1\,0\,0 \ldots 0 \\ 0\,0\,0 \ldots 0 \\ 0\,1\,0 \ldots 0 \end{pmatrix}$$

and

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{p1} & c_{p2} & c_{p3} & c_{p4} & c_{p5} \end{pmatrix}.$$

Following theorem the system is output controllable if and only if $\operatorname{rank} C = p$ *and it is not possible if* $p > 5$.

In this case is easy to compute the output controllability matrix and obtain the rank:

$$\begin{array}{l} \operatorname{rank} \begin{pmatrix} c_{13} & c_{15} & 0 \ldots 0 & c_{12} & c_{14} & 0 \ldots 0 & c_{11} & 0\,0 \ldots 0 \\ \vdots & \vdots & \vdots \ldots \vdots & \vdots & \vdots & \vdots \ldots \vdots & \vdots & \vdots\,\vdots \ldots \vdots \\ c_{p3} & c_{p5} & 0 \ldots 0 & c_{p2} & c_{p4} & 0 \ldots 0 & c_{p1} & 0\,0 \ldots 0 \end{pmatrix} = \\ \operatorname{rank} \begin{pmatrix} c_{13} & c_{15} & c_{12} & c_{14} & c_{11} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{p3} & c_{p5} & c_{p2} & c_{p4} & c_{p1} \end{pmatrix} = \\ \operatorname{rank} C. \end{array}$$

References

J.L. Dominguez-García, M. I. García-Planas, (2011) *Output controllability analysis of fixed speed wind*. To appear to IPACS electronic library.

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

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

Mª I. García-Planas, M.D. Magret, (1999) *An alternative System of Structural Invariants for Quadruples of Matrices*, Linear Algebra and its Applications **291**, (1-3), pp. 83-102.

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

J,L Massey, M.K. Sain, (1967) *Codes, Automata and continuous systems: explicit interconnections.* IEEE Trans. on Automatic Control, Vol AC-12 (6), pp.644-650.

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

J. Rosenthal, J.M. Schumacher, E.V. York, (1996) *On Behaviors and Convolutional Codes*, IEEE Trans. on Information Theory, **42**, (6), pp. 1881-1891.