Noname manuscript No.
(will be inserted by the editor)

$1/n$ Turbo Codes from linear system point of view

Victoria Herranz · Diego Napp · Carmen Perea

Received: date / Accepted: date

Abstract The performance of turbo codes at the error floor region is largely determined by the effective free distance, which corresponds to the minimum Hamming weight among all codewords sequences generated by input sequences of weight two. In this paper, we study turbo codes of dimension one obtained from the concatenation of two equal codes and present an upper bound on the effective free distance of a turbo code with these parameters defined over any finite field. We do that making use of the so-called (A, B, C, D) state-space representations of convolutional codes and restrict to the case where A is invertible. A particular construction, from a linear systems point of view, of a recursive systematic convolutional code of rate $1/n$ so that the effective free distance of the corresponding turbo code attains this upper bound is also presented.

An earlier version of this paper was presented at the Conference Linear Algebra, Matrix Analysis and Applications. ALAMA2018, held in Sant Joan dAlacant on May/June 2018.

Victoria Herranz
The Institute Center of Operations Research, University Miguel Hernández of Elche, Avda. Universidad, s/n., 03202 Spain
Tel.: +34-96-6658537
Fax: +34-96-6658715
E-mail: mavi.herranz@umh.es

Diego Napp
Departamento de Matemticas, Universidad de Alicante. Apartado de correos, 99. 03080, Alicante
Tel.: +34-96-5903531
E-mail: diego.napp@ua.es

Carmen Perea
The Institute Center of Operations Research, University Miguel Hernández of Elche, Avda. Universidad, s/n., 03202 Spain
Tel.: +34-96-6749618
Fax: +34-96-6658715
E-mail: perea@umh.es

1 Introduction

A turbo encoder is formed by parallel concatenation of several recursive systematic convolutional encoders separated by a random interleaver. Turbo codes were first introduced in 1993 by Berrou, Glavieux, and Thitimajshima [5]. Currently, they are one of the most effective methods of generating codes with high error correction capability. For the best performance of turbo codes, it is necessary to choose "good" component codes from the set of all possible recursive convolutional codes with a particular rate and complexity.

Benedetto and Montorsi [3] and later Benedetto, Garello and Montorsi [4] addressed this problem for two identical linear systematic convolutional codes in the binary context. They demonstrate that the component codes must be recursive for the interleaver to provide significant gain, and that the lowest weight of the parity check vector generated by information sequences of weight two, $z_{\min}$, is the dominant parameter determining turbo code performance. Divsalar and McEliece [14] introduce and establish some theoretical bounds for the effective free distance. More recently, Vatta, Graell, Banerjee and Costello [36], as well as, Chatzigeorgiou and Wassell [7] provide new expressions for calculation of the effective free distance of nonsystematic turbo codes and pseudo-radomly punctured turbo codes.

Since the introduction of turbo codes numerous valid applications have been developed, the most important can be found in [35]. Moreover, in recent years, new lines of research have appeared, such as the study of non-binary turbo codes. Here, the encoder structure is the same to the one used for binary turbo codes, except that the operations are performed on the non-binary field (every ring) considered. These new turbo code families aim to improve the performance, especially by lowering the error floor and reducing its latency (as the data block is more compact). See [2,6,20,28] for more details. In many realistic scenarios, codewords of a finite field of q elements, are converted to binary codewords in order to be transmitted in a binary channel (see for instance [17]). If the finite field has q elements, we will need N bits for each element (where N is the minimum value where $2^N > q$)

In this paper we propose to investigate turbo codes from a system-theoretical point of view, an approach that has been extensively used to study convolutional codes [9,23,25,32]. In particular, we focus on the crucial notion of maximum effective free distance which has not been carefully investigated within this approach, see [1,24] for constructions of codes with maximum column distance. This can be considered as an elaboration of the line of work firstly developed in [15,18]. In this work we consider a turbo code obtained by the parallel concatenated convolutional codes whose encoder is formed by two or more constituent systematic recursive encoders joined by an interleaver. We address codes of rate $1/n$. Low rate codes have particularly practical interest due, for instance, to the fact that their decoding complexity is much lower than high rate turbo codes, see [13,27] for details.

In the context of systems theory, in Section 2 we explain some results in convolutional codes defined over any Galois field and we give the basic

concepts about turbo codes. We provide an upper bound on $\mathrm{z}_{\min}(\mathcal{C})$ of a rate $1/n$ recursive systematic convolutional code $\mathcal{C}$ defined over any finite field, and therefore an upper bound on the effective free distance of the turbo code obtained from $\mathcal{C}$ in Section 3. In addition, we develop a particular construction of a convolutional code whose $\mathrm{z}_{\min}(\mathcal{C})$ (see Definition 1) attains this upper bound.

2 Turbo Codes and Linear Systems

In this paper, we denote by $\mathbb{F} = GF(q)$ the Galois field of q elements and $\mathbb{F}[z]$ the polynomial ring on the variable z with coefficients in $\mathbb{F}$.

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 $D \in \mathbb{F}^{(n-k)\times k}$. Following [29] and [32], a rate k/n convolutional code $\mathcal{C}$ of complexity δ can be described by the linear system governed by the equations

$$\left.\begin{array}{rl} \mathbf{x}_{t+1} &= A\mathbf{x}_t + B\mathbf{u}_t \\ \mathbf{y}_t &= C\mathbf{x}_t + D\mathbf{u}_t \end{array}\right\}, \quad t = 0, 1, 2, \ldots \tag{1}$$

$$\mathbf{v}_t = \begin{pmatrix} \mathbf{y}_t \\ \mathbf{u}_t \end{pmatrix}, \quad \mathbf{x}_0 = 0,$$

where for each time instant t, $\mathbf{x}_t \in \mathbb{F}^\delta$ is the *state vector*, $\mathbf{u}_t \in \mathbb{F}^k$ is the *input* (also call *information vector*) and $\mathbf{y}_t \in \mathbb{F}^{n-k}$ is the *parity check vector*. In linear systems theory, this representation is known as the *input-state-output representation*. This representation was introduced by Rosenthal, York and Schumacher (see [29]) and it has been widely used in the last years to analyze and construct convolutional codes [10,11,31,32]. In terms of Linear Systems, the complexity δ, is the McMillan degree of the linear system (1). In the following, we adopt the notation used by McElliece [21] and we call a convolutional code of rate k/n and complexity δ an (n, k, δ)-code.

Convolutional codes, as we defined above, always admit image representations, in the sense that for each convolutional code $\mathcal{C}$, there exists a polynomial matrix $G(z)$ such that

$$\mathcal{C} = \{\mathbf{v}(z) \in \mathbb{F}^n[z] \ : \ \exists \mathbf{u}(z) \in \mathbb{F}^k[z] \text{ such that } \mathbf{v}(z) = G(z)\mathbf{u}(z)\},$$

where the matrix $G(z)$ is called generator matrix or encoder of $\mathcal{C}$ (see, for example [3,21,29,30,32]).

Remark 1 We note that the input-state-output representation (1) considered here is different from the commonly used *driving variable representation* of $\mathcal{C}$, see [16,22], given by

$$\left.\begin{array}{rl} \mathbf{x}_{t+1} &= \mathcal{A}\mathbf{x}_t + \mathcal{B}\mathbf{u}_t \\ \mathbf{v}_t &= \mathcal{C}\mathbf{x}_t + \mathcal{D}\mathbf{u}_t \end{array}\right\}, \tag{2}$$

where $\mathbf{u}_t \in \mathbb{F}^k$ is the *information vector*, $\mathbf{v}_t \in \mathbb{F}^n$ the codewords that are, in this case, the outputs of the linear system and $\mathbf{x}_t \in \mathbb{F}^\delta$ as above.

In this context the image representation $\mathbf{v}(z) = G(z)\mathbf{u}(z)$ is usually described through state-space equations like (2) where the input $\mathbf{u}(z)$ drives the output $\mathbf{v}(z)$. In contrast to this, system (1) is a state-space description where k components $\mathbf{u}(z)$ of the codeword $\mathbf{v}(z)$ drive the remaining $n-k$ components $\mathbf{y}(z)$ of $\mathbf{v}(z)$.

Representation (2) has been considered the standard way in which convolutional codes were presented in terms of linear systems. However, many authors considered that linear system (1) is the better choice to study convolutional codes [29,31,34,38]. One of the reasons for this is that in the driving variable representations, the matrix $\mathcal{A}$ has to be nilpotent (when $G(D)$ is polynomial as it is our case) whereas in the one described in (1) the matrix A does not have such a restriction. This fact facilitates the construction of optimal input state output representations of convolutional codes (see [31,33,34,38] for constructions with A invertible). In particular, in this paper we shall also deal with invertible matrices A for technical reasons (see Remark 3).

Note that the input-state-output description (1) describes the dynamics of a rational and systematic encoder in a natural way, since by Lemma 2.14 of [31], if $\mathcal{C}(A, B, C, D)$ is an (n, k, δ)-code, then, the matrices A, B, C and D describe a proper rational transfer function of $\mathcal{C}(A, B, C, D)$, given by

$$T(z) = C(zI - A)^{-1}B + D.$$

Moreover, $G(z) = \begin{pmatrix} T(z) \\ I_k \end{pmatrix}$ is a systematic encoder of the convolutional code $\mathcal{C}(A, B, C, D)$. In particular, the convolutional code $\mathcal{C}(A, B, C, D)$ is a systematic convolutional code.

For algebraic reasons, we assume that $\{\mathbf{v}_t\}_{t\geq 0}$ in Equation (1) is a finite-weight codeword (see [31]), i.e., equation (1) is satisfied for all $t = 0, 1, 2, \ldots$ and there is an integer γ such that $\mathbf{x}_{\gamma+1} = 0$, $\mathbf{u}_t = 0$, for $t \geq \gamma + 1$, and therefore, $\mathbf{y}_t = 0$ for $t \geq \gamma + 1$, so the code sequence has finite weight. Throughout the paper we will denote such a finite-weight codeword by $\mathcal{V}_\gamma$.

Then, for a finite-weight codeword both the input sequence and the state sequence (and hence the output sequence) need to have finite support. The set of finite-weight codewords has a module structure over the polynomial ring $\mathbb{F}[z]$ (see [31]). By abuse of notation, we will denote this module by $\mathcal{C}(A, B, C, D)$ and we refer to it as the *finite-weight convolutional code* generated by the matrices A, B, C, D. Proposition 2.4 of [31] gives us a characterization of finite-weight codewords. In particular, if $\{\begin{pmatrix} \mathbf{y}_t \\ \mathbf{u}_t \end{pmatrix} \in \mathbb{F}^n \mid t = 0, 1, \ldots, \gamma\}$ represents a finite-weight codeword, then the equations of (1) are satisfied for all $t \geq 0$ and

$$\begin{pmatrix} A^\gamma B & A^{\gamma-1}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\gamma-1} \\ u_\gamma \end{pmatrix} = 0. \tag{3}$$

Note that the description given by expression (1) is in general not unique. But if $\mathcal{C}$ has complexity δ, then it is possible to choose the matrices A, B, C, and D of sizes $\delta \times \delta$, $\delta \times k$, $(n-k) \times \delta$ and $(n-k) \times k$, respectively (see [19]). In convolutional coding theory, an input-state-output representation (A, B, C, D), having the above sizes, is called a *minimal representation* and it is characterized through the condition that the pair (A, B) is *controllable*, that is (see [31]),

$$\operatorname{rank} \Phi_\delta(A, B) = \delta,$$

where

$$\Phi_j(A, B) := \begin{pmatrix} B & AB & \cdots & A^{j-2}B & A^{j-1}B \end{pmatrix}, \quad j \in \mathbb{N}. \tag{4}$$

If (A, B) is a controllable pair, then we call the smallest integer κ having the property that $\operatorname{rank} \Phi_\kappa(A, B) = \delta$ the *controllability index* of (A, B).

On the other hand, we say that (A, C) is an *observable* pair if (A^T, C^T) is a controllable pair, that is (see [31]),

$$\operatorname{rank} \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{\delta-1} \end{pmatrix} = \delta$$

Remark 2 Note that it is straightforward to verify that if S is an invertible matrix, then it holds that

$$\mathcal{C}(SAS^{-1}, SB, CS^{-1}, D) = \mathcal{C}(A, B, C, D).$$

In terms of an input-state-output representation, the free distance of a convolutional code $\mathcal{C}$ can be defined as

$$\mathrm{d}_{\mathrm{free}}(\mathcal{C}) = \min_{\mathbf{u}_0 \neq \mathbf{0}} \left(\sum_{t=0}^{\infty} \mathrm{wt}(\mathbf{u}_t) + \sum_{t=0}^{\infty} \mathrm{wt}(\mathbf{y}_t) \right)$$

where $\mathrm{wt}(\mathbf{v}_t)$ denotes the Hamming weight of a vector $\mathbf{v}_t$.

Moreover, the jth column distance of the convolutional code $\mathcal{C}$ is given by

$$d_j^c(\mathcal{C}) = \min_{\mathbf{u}_0 \neq 0} \left\{ \sum_{t=0}^{j} \mathrm{wt}(\mathbf{u}_t) + \sum_{t=0}^{j} \mathrm{wt}(\mathbf{y}_t) \right\} \quad \text{for } j = 0, 1, 2, \ldots.$$

Finally, the free distance of an (n, k, δ)-code $\mathcal{C}$ is always upper-bounded by the *generalized Singleton bound* (see [30])

$$\mathrm{d}_{\mathrm{free}}(\mathcal{C}) \leq (n-k) \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) + \delta + 1.$$

In addition, the convolutional code $\mathcal{C}$ is called maximum-distance separable (MDS) if its free distance is equal to the generalized Singleton bound.

On the other hand, in order to obtain codes coming closest to the Shannon limit, Berrou, Glavieux and Thitimajshima consider parallel concatenation of convolutional codes, known as turbo codes (see [5]).

In a turbo code $\mathcal{TC}$ two convolutional codes, $\mathcal{C}_1$ and $\mathcal{C}_2$ of rates k/n_1 and k/n_2, respectively, are linked through an interleaver so that the first encoder, $\mathcal{C}_1$, operates directly on the input information $\mathbf{u}_t$ $(t = 0, 1, 2, \ldots)$ and the second one, $\mathcal{C}_2$, encodes the interleaved input information, denoted by $P\mathbf{u}_t$ $(t = 0, 1, 2, \ldots)$, where P is a permutation matrix of order k. Thus, a codeword of the turbo code consists of the parity vectors of both encoders followed by the information vector. In particular, Devesa, Herrranz and Perea [8] introduce the input-state-output representation for the turbo code $\mathcal{TC}$ from the input-state-output representation of the constituent encoders. More results on concatenated convolutional codes using a linear systems approach can be found in [10], [11] and [12], [15] and [18].

The most important parameter through which the constituent convolutional codes influence the turbo code performance is $\mathrm{z}_{\min}(\mathcal{C})$, which it is defined below (see [3,14] for more details).

Definition 1 Let $\mathcal{C}$ be a convolutional code. We define $\mathrm{z}_{\min}(\mathcal{C})$ as the lowest weight of the parity check vectors of the convolutional code $\mathcal{C}$ generated by information sequences of weight two.

Several authors ([3,26]) have agreed that the performance of turbo codes is determined by the weight-2 input minimum distance, which corresponds to the minimum Hamming weight among all codeword sequences generated by input sequences of weight two. If we consider a turbo code $\mathcal{TC}$ with $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}$, its weight-2 input minimum distance, which is also referred to as the *effective free distance* of $\mathcal{TC}$ (see [3]), $\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC})$, can be written as

$$\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC}) = 2 + 2\,\mathrm{z}_{\min}(\mathcal{C}) \tag{5}$$

The effective free distance plays a similar role to that of the free distance for convolutional codes. For a turbo code with a uniform interleaver, the free distance dominates the error performance at high SNR's. However, the free distance may be smaller than the effective free distance $\mathrm{d}_{\mathrm{free,eff}}$ (see [37]).

The design objective for the constituent recursive convolutional encoders is to obtain $\mathrm{z}_{\min}$ as large as possible. Benedetto and Montorsi [3] prove that in the binary case there exists a rate $1/n$ recursive systematic convolutional code $\mathcal{C}$ with complexity δ that achieve the maximum value of $\mathrm{z}_{\min}(\mathcal{C})$, given by

$$\mathrm{z}_{\min}(\mathcal{C}) \leq (n-1)(2^{\delta-1}+2).$$

The notion of $\mathrm{z}_{\min}(\mathcal{C})$ and, therefore, of $\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC})$ will be of central interest in this paper.

3 An upper bound for the $\mathrm{z}_{\min}$ of a rate $1/n$ recursive systematic convolutional code

From relation (5), we get that the maximization of $\mathrm{z}_{\min}(\mathcal{C})$ obviously results in a maximization of the effective free distance. It follows then that the component encoders should not only be recursive and systematic, but should also

be selected so as to maximize $\mathrm{z}_{\min}(\mathcal{C})$. In the rest of the paper, we study how to obtain the value of $\mathrm{z}_{\min}(\mathcal{C})$ of recursive systematic convolutional codes $\mathcal{C}(A,B,C,D)$ of rate $1/n$ and A invertible. Moreover, we present an upper bound on the effective free distance of a turbo code composed (as in [3]) by the concatenation of two equal linear systematic convolutional codes. From now on, we restrict our attention to turbo codes obtained in this way and we denote them by $\mathcal{TC}$. Finally, since an input at time t is in fact an element of the field in the particular case where $\mathcal{C}(A,B,C,D)$ has a rate $1/n$, we adopt the typography u_t instead of $\mathbf{u}_t$, corresponding to the general case (where the inputs are vectors), in order to distinguish between scalars (for the particular case of single input convolutional codes) and vectors (for the general case).

Assume that (A,B,C,D) is a minimal representation of a recursive systematic convolutional code of rate $1/n$ and complexity δ. In particular, the matrices (A,B) form a controllable pair, so

$$\operatorname{rank}\Phi_\kappa(A,B) = \operatorname{rank}\left(B\ AB\ \cdots\ A^{\kappa-1}B\right) = \delta, \tag{6}$$

where κ is the controllability index of (A,B). Moreover, if $\mathcal{C}(A,B,C,D)$ is an $(n,1,\delta)$-code with the pair (A,B) controllable, then the controllability index κ matches the complexity δ, $\kappa=\delta$.

Now, let $\mathcal{V}_\gamma$ be a finite-weight codeword with $u_0 \neq 0$. Then, relations (3) and (6), imply necessarily $\gamma > \kappa - 1$ and therefore, we get the following result.

Lemma 1 *Let $\mathcal{C}(A,B,C,D)$ be an $(n,1,\delta)$-code with the pair (A,B) controllable. Then, the length $\gamma+1$ of a finite-weight codeword with input weight 2 verifies $\gamma \geq \delta$.*

Then, in order to get the $\mathrm{z}_{\min}(\mathcal{C})$ of an $(n,1,\delta)$-code $\mathcal{C}$, we evaluate the minimum weight of parity check vectors corresponding to finite-weight codewords $\mathcal{V}_\gamma$ with $\gamma \geq \delta$ generated by information vectors $(u_0,u_1,\ldots,u_\gamma)$ with weight two and such that $u_0 \neq 0$.

Moreover, the following result characterizes finite-weight codewords generated by information sequences of weight two in terms of the minimum distance of a block code whose parity check matrix has the same structure as the matrix $\Phi_j(A,B)$ given by relation (4).

Lemma 2 *Let $\mathcal{C}(A,B,C,D)$ be an $(n,1,\delta)$-code with the pair (A,B) controllable. Let m be an integer such that the matrix*

$$\Phi_m(A,B) = \left(B\ AB\ \cdots\ A^{m-2}B\ A^{m-1}B\right)$$

is the parity check matrix of an $(m, m-\delta)$ block code $\mathcal{B}$ with minimum distance $\mathrm{d}_{\min}(\mathcal{B}) \geq 3$. Then, any finite-weight codeword $\mathcal{V}_\gamma$ with input weight 2 and $u_0 \neq 0$ verifies $\gamma \geq m$.

Proof First, since $\Phi_m(A,B)$ is the parity check matrix of a $(m, m-\delta)$ block code $\mathcal{B}$ with minimum distance $\mathrm{d}_{\min}(\mathcal{B}) \geq 3$, then any two columns of $\Phi_m(A,B)$ are linearly independent. Now, let $\mathcal{V}_\gamma$ be a finite-weight codeword with information vector $(u_0,u_1,\ldots,u_\gamma)$ of weight two and first component u_0 nonzero.

Specifically, an integer r exists with $0 < r \leq \gamma$ such that $u_r \neq 0$ and $u_j = 0$ for all $j \neq 0, r$. Moreover, since $\mathcal{V}_\gamma$ is a finite-weight codeword, the information vector verifies relation (3), so

$$A^\gamma B u_0 + A^{\gamma - r} B u_r = 0.$$

If $\gamma < m$, then $A^\gamma B$ and $A^{\gamma-r}B$ are in fact two columns linearly dependent of the matrix $\Phi_m(A, B)$, which contradicts the fact that the block code $\mathcal{B}$ has minimum distance $\mathrm{d_{min}}(\mathcal{B}) \geq 3$.

In addition to the integer γ, we need to introduce also the time instant at which the last input is introduced into the system.

Definition 2 Let s be the least integer $\hat{s}$ for which there is a finite-weight codeword $\mathcal{V}_\gamma$ of a convolutional code $\mathcal{C}$ generated by an information vector $(u_0, u_1, \ldots, u_{\hat{s}}, u_{\hat{s}+1}, \ldots, u_\gamma)$ of weight two with u_0,$u_{\hat{s}} \neq 0$. We shall call such an s, the *minimum effective index of* $\mathcal{C}$.

Remark 3 Observe that if $\mathcal{C}(A, B, C, D)$ is a rate $1/n$ convolutional code with A invertible, then the integer s can be defined as the minimum integer for which exists a finite-weight codeword $\mathcal{V}_s$ with length $s+1$ generated by an information vector $(u_0, u_1, \ldots, u_s)$ of weight two with u_0,$u_s \neq 0$. Indeed, let $\mathcal{V}_\gamma$ be a finite-weight codeword generated by an information vector $(u_0, u_1, \ldots, u_{\hat{s}}, u_{\hat{s}+1}, \ldots, u_\gamma)$ of weight two with u_0,$u_{\hat{s}} \neq 0$. In particular,

$$\left(A^\gamma B \; A^{\gamma-1} B \cdots A^{\gamma-s} B \cdots AB \; B \right) \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\hat{s}} \\ \vdots \\ u_{\gamma-1} \\ u_\gamma \end{pmatrix} = A^{\gamma-\hat{s}} \left(A^{\hat{s}} B \; A^{\hat{s}-1} B \cdots AB \; B \right) \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\hat{s}-1} \\ u_{\hat{s}} \end{pmatrix} = 0 \tag{7}$$

implies

$$\left(A^{\hat{s}} B \; A^{\hat{s}-1} B \cdots AB \; B \right) \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\hat{s}-1} \\ u_{\hat{s}} \end{pmatrix} = 0,$$

since A is invertible. So necessarily, $\hat{s} = \gamma$. That is, if A is invertible, then the minimum effective index of $\mathcal{C}$ is obtained by the minimum of the integers that satisfy the conditions indicated at the beginning of the Remark.

In the case A singular, this does not necessarily hold, and we may have that

$$\left(A^{\hat{s}} B \; A^{\hat{s}-1} B \cdots AB \; B \right) \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\hat{s}-1} \\ u_{\hat{s}} \end{pmatrix} \neq 0$$

but relation (7) holds. That is, there may be a finite-weight codeword $\mathcal{V}_\gamma$ of $\mathcal{C}$ generated by an information vector $(u_0, u_1, \ldots, u_{\hat{s}}, \ldots, u_\gamma)$ of weight two with u_0,$u_{\hat{s}} \neq 0$ and $\hat{s} < \gamma$. This intuitively means that the state of the system (A, B, C, D) does not necessary vanish at instant $\hat{s}$ and could remain nonzero for some time after the last input $u_{\hat{s}} \neq 0$ enters into the system.

As we show in the following lemma, the minimum effective distance depends on the complexity δ.

Lemma 3 *If $\mathcal{C}(A, B, C, D)$ is a rate $1/n$ convolutional code with (A, B) controllable and A invertible, then $s \geq \delta$.*

Proof Let $\mathcal{C}(A, B, C, D)$ be an $1/n$ convolutional code with (A, B) controllable and A invertible. Assume that there exists a finite-weight codeword $\mathcal{V}_\gamma$ of $\mathcal{C}$ generated by an information vector $(u_0, u_1, \ldots, u_s, \ldots, u_\gamma)$ of weight two with u_0,$u_s \neq 0$ and $s < \delta$. Then,

$$\begin{pmatrix} A^\gamma B & A^{\gamma-1}B & \cdots & A^{\gamma-s}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_s \\ \vdots \\ u_{\gamma-1} \\ u_\gamma \end{pmatrix} = A^\gamma B u_0 + A^{\gamma-s} B u_s = A^{\gamma-s}(A^s B u_0 + B u_s) = 0$$

implies that $A^s B u_0 + B u_s = 0$, since A is invertible. Now, if $s < \delta$, then $\operatorname{rank} \Phi_\delta(A, B) < \delta$, which contradicts the fact that (A, B) is controllable. So $s \geq \delta$.

Next result states that the complexity of a convolutional code is equal to 1 if and only if $s = 1$.

Lemma 4 *Let $\mathcal{C}(A, B, C, D)$ be an $(n, 1, \delta)$-code with (A, B) controllable. Then, $\delta = 1$ if and only if $s = 1$.*

Proof If $s = 1$, the complexity of $\mathcal{C}$ is trivially $\delta = 1$, since $s \geq \delta$. Now, if the complexity of the convolutional code $\mathcal{C}(A, B, C, D)$ is $\delta = 1$ and the pair (A, B) is controllable, then the matrices A and B are nonzero scalars of the field $\mathbb{F}$. So, the least integer s for which there is a finite-weight codeword $\mathcal{V}_s$ generated by an information vector $(u_0, u_1, \ldots, u_s)$ of weight two with u_0,$u_s \neq 0$ is $s = 1$.

3.1 An upper bound for the $\mathrm{z}_{\min}$ of a rate $1/n$ recursive systematic convolutional code $\mathcal{C}(A, B, C, D)$ with A invertible

Next theorem shows that if the matrix A is invertible, we can obtain $\mathrm{z}_{\min}(\mathcal{C})$ from the weight of the parity-check vectors of any finite-weight codeword of length $s + 1$ generated by input vectors of weight two, where s is the integer described in Definition 2.

Throughout this paper, we adopt the following notation. If E is an $m \times 1$ matrix, then $\mathrm{wt}(E)$ denotes the Hamming weight of the vector E, that is, the number of nonzero components of E.

Theorem 1 *Let $\mathcal{C}(A,B,C,D)$ be an $(n,1,\delta)$-code with (A,B) controllable and A invertible and s the minimum effective index of $\mathcal{C}$. Then, it holds that*

1. *s is the first integer γ such that $A^\gamma B, B$ are linearly dependent.*
2. *$\mathrm{z}_{\min}(\mathcal{C})$ is obtained by the weight of the parity-check vectors of any finite-weight codeword $\mathcal{V}_s$ of the convolutional code generated by information sequences with length $s+1 \geq \delta+1$ where the two inputs different from zero are the first and the last ones.*
3. *Moreover, $\mathrm{z}_{\min}(\mathcal{C})$ has the following value*

$$\mathrm{z}_{\min}(\mathcal{C}) = \begin{cases} \mathrm{wt}(D) + \mathrm{wt}(D - CA^{-1}B) & \text{if } \delta = 1 \\ \mathrm{wt}(D) + \sum_{j=0}^{s-2} \mathrm{wt}(CA^jB) + \mathrm{wt}(D - CA^{-1}B) & \text{if } \delta \geq 2 \end{cases}. \quad (8)$$

Proof Statements 1. and 2. Since $\mathrm{z}_{\min}(\mathcal{C})$ is defined as the minimum of the weights of the parity-check vectors obtained from finite-weight codewords with information vectors of weight two, it is obvious from Remark 3 and Lemma 3 that this minimum in the particular case where A is an invertible matrix, is attained among the codewords $\mathcal{V}_s$ generated by information sequences $(u_0, u_1, \ldots, u_s)$ with length $s+1 \geq \delta+1$, where the only nonzero inputs are u_0 and u_s.

Now, let $\mathcal{V}_\gamma$ be any finite-weight codeword generated by an information vector $(u_0, u_1, \ldots, u_\gamma)$ of weight two with u_0,$u_\gamma \neq 0$ and $u_j = 0$ for all $j = 1, 2, \ldots, \gamma-1$. In particular, it holds that

$$A^\gamma B u_0 + B u_\gamma = 0, \quad (9)$$

so we can compute s as the minimum integer γ such that the above expression is satisfied.

Next we prove statement 3. From relation (9), we obtain that

$$A^{s-1} B u_0 = -A^{-1} B u_s$$

since A is invertible. In this way, the components of the parity check vector $(\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_s)$ are given by the following relations

$$\begin{aligned} \mathbf{y}_0 &= D u_0 \\ \mathbf{y}_1 &= CBu_0 + Du_1 = (D - CA^{-1}B)u_1 \end{aligned} \quad (10)$$

if $s = 1$ and

$$\begin{aligned} \mathbf{y}_0 &= D u_0 \\ \mathbf{y}_j &= CA^{j-1}Bu_0 \quad \text{for } j = 1, 2, \ldots, s-1 \\ \mathbf{y}_s &= CA^{s-1}Bu_0 + Du_s = (D - CA^{-1}B)u_s \end{aligned} \quad (11)$$

if $s \geq 2$.

Since u_0 and u_s are nonzero elements of the field $\mathbb{F}$, relations (10) and (11) actually show that the parity check vectors of finite-weight codewords $\mathcal{V}_s$ of lenght $s+1$ have the same weight, independently of the codeword. Moreover,

observe that using the notation given in the beginning of this subsection for the weights $\mathrm{wt}(D)$, $\mathrm{wt}(D - CA^{-1}B)$ and $\mathrm{wt}(CA^jB)$, for $j = 0, 1, \ldots, \gamma - 2$, then

$$\mathrm{z}_{\min} = \sum_{t=0}^{s} \mathrm{wt}(\mathbf{y}_t) = \begin{cases} \mathrm{wt}(D) + \mathrm{wt}(D - CA^{-1}B) & \text{if } s = 1 \\ \mathrm{wt}(D) + \sum_{j=0}^{s-2} \mathrm{wt}(CA^jB) + \mathrm{wt}(D - CA^{-1}B) & \text{if } s \geq 2 \end{cases}$$

Finally, taking into account Lemma 4, we obtain relation (8).

Theorem above gives us a practical way to compute the values the minimum effective index s and $\mathrm{z}_{\min}(\mathcal{C})$ of a rate $1/n$ convolutional code $\mathcal{C}(A, B, C, D)$ with A being an invertible matrix. It provides also an upper bound on the effective free distance of the turbo code $\mathcal{TC}$.

Corollary 1 *Let $\mathcal{C}(A, B, C, D)$ be an $(n, 1, \delta)$-code, such that the pair (A, B) is controllable and A is an invertible matrix. Let s be the minimum effective index of $\mathcal{C}$. Then,*

$$\mathrm{z}_{\min}(\mathcal{C}) \leq (n - 1)(s + 1), \tag{12}$$

and consequently, the effective free distance of $\mathcal{TC}$ verifies

$$\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC}) \leq 2 + 2(n - 1)(s + 1).$$

Note that, as a consequence of Lemma 4 and Corollary 1, we obtain the following upper bound on the value of $\mathrm{z}_{\min}(\mathcal{C})$ for the particular case where $\mathcal{C}(A, B, C, D)$ is a convolutional code of rate $1/n$ and complexity $\delta = 1$

$$\mathrm{z}_{\min}(\mathcal{C}) \leq 2(n - 1).$$

Moreover, if $\mathcal{TC}$ is of rate $1/n$ and complexity $\delta = 1$ then,

$$\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC}) \leq 2 + 4(n - 1).$$

Next, we present two examples to illustrate the results of Corollary 1.

Example 1 Let α be a primitive element of $\mathbb{F}_8$ with $\alpha^3 + \alpha + 1 = 0$ and let $\mathcal{C}(A, B, C, D)$ be the convolutional code of rate $1/3$ and complexity $\delta = 3$, where

$$A = \begin{pmatrix} \alpha^2 & 0 & \alpha^3 \\ \alpha & \alpha^2 & 1 \\ \alpha & 0 & \alpha^3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 \\ 1 \\ \alpha^2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & \alpha & 1 \\ \alpha^2 & 1 & 1 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} \alpha^6 \\ \alpha^4 \end{pmatrix}$$

Observe that the pair (A, B) is controllable, so the matrices (A, B, C, D) are a minimal representation of the convolutional code $\mathcal{C}$. Also, the pair (A, C) is observable. The minimum effective index of $\mathcal{C}$, s, is $s = 7$ and $\mathrm{z}_{\min}(\mathcal{C}) = 11$. So $\mathrm{z}_{\min}(\mathcal{C})$ does not attain the upper-bound (12) for these parameters, which in this case is 16.

Example 2 Let α be a primitive element of $\mathbb{F}_8$ with $\alpha^3+\alpha+1=0$ and let $\mathcal{C}(A,B,C,D)$ be the convolutional code of rate $1/4$ and complexity $\delta=4$, where

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

Observe that the pair (A,B) is controllable, so the matrices (A,B,C,D) are a minimal representation of the convolutional code $\mathcal{C}$. Also, the pair (A,C) is observable. The minimum effective index of $\mathcal{C}$, s, is 7, but $\mathrm{z}_{\min}(\mathcal{C})$ in this example is equal to 20 and it does not achieve the upper-bound (12), which in this case is 24. Nevertheless, if we consider a new rate $1/4$ convolutional code $\mathcal{C}(A,B,C,D)$ where A is the matrix as above and the matrices B,C and D are given by

$$B=\begin{pmatrix}\alpha\\ 1\\ \alpha^2\\ \alpha^3\end{pmatrix},\quad C=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&\alpha&\alpha^3\end{pmatrix}\quad\text{and}\quad D=\begin{pmatrix}\alpha\\ 1\\ \alpha\end{pmatrix}$$

then, the minimum effective index of $\mathcal{C}$ is $s=7$ and $\mathrm{z}_{\min}(\mathcal{C})=24$ attains the upper-bound (12) of Corollary 1.

Now, we derive the exact value of the integer s for the particular case where the matrix A of the $(n,1,\delta)$-code $\mathcal{C}(A,B,C,D)$ is an invertible diagonalizable matrix.

Lemma 5 *Let α be a primitive element of the Galois field $\mathbb{F}$ of q elements. Let $\mathcal{C}(A,B,C,D)$ be an $(n,1,\delta)$-code with $\delta\geq 2$, such that the pair (A,B) is controllable. Assume that A is an invertible diagonalizable matrix and let $\alpha^{r_1},\alpha^{r_2},\ldots,\alpha^{r_\delta}$ be the eigenvalues of A. Let us define*

$$d=gcd\{r_1,r_2,\ldots,r_\delta\}. \tag{13}$$

Then, the minimum effective index of $\mathcal{C}$ is the integer given by

$$s=\begin{cases}q-1 & \text{if } d \text{ does not divide } q-1\\ \frac{q-1}{d} & \text{if } d \text{ divides } q-1\end{cases} \tag{14}$$

Proof It is obvious, from definition of the minimum effective index (see Definition 2) and conditions of this lemma, that s is exactly the value given by the relation (14).

The following lemma gives us the concrete value of $\mathrm{z}_{\min}(\mathcal{C})$ where $\mathcal{C}(A,B,C,D)$ is a $1/n$ convolutional code with A an invertible and diagonalizable matrix.

Lemma 6 *Let $\mathcal{C}(A,B,C,D)$ be an $(n,1,\delta)$-code with the conditions given in Lemma 5, and let $\mathcal{V}_\gamma$ be any finite-weight codeword whose information sequence $(u_0 \neq 0, \ldots, u_\gamma)$ has weight 2. Then, γ is necessarily a multiple of the minimum effective index s of $\mathcal{C}$, $u_0 = -u_\gamma \neq 0$ and the weight of the sequence of the parity-check vectors $(\mathbf{y}_0, \ldots, \mathbf{y}_\gamma)$ of $\mathcal{V}_\gamma$ are given by*

$$\sum_{t=0}^{\gamma} \mathrm{wt}(\mathbf{y}_t) = \mathrm{wt}(D) + \sum_{j=1}^{\gamma-1} \mathrm{wt}(CA^{j-1}B) + \mathrm{wt}(CA^{\gamma-1}B - D)$$

Furthermore,

$$\mathrm{z}_{\min}(\mathcal{C}) = \mathrm{wt}(D) + \sum_{j=1}^{s-1} \mathrm{wt}(CA^{j-1}B) + \mathrm{wt}(CA^{-1}B - D).$$

Proof Let $\mathcal{V}_\gamma$ be any finite-weight codeword whose information sequence $(u_0 \neq 0, \ldots, u_\gamma)$ has weight two. Since A is invertible, necessarily $u_\gamma \neq 0$ (see Remark 3). Also, as it is a finite-weight codeword, it verifies relation (3), so

$$A^\gamma B u_0 + B u_\gamma = 0 \tag{15}$$

Now, taking into account statement 1 of Theorem 1 and the fact that $A^{s-1} = I$ (see Lemma 5), we conclude that relation (15) holds if and only if

$$A^\gamma = I \quad \text{and} \quad u_\gamma = -u_0 \neq 0, \tag{16}$$

where I is the identity matrix of size $\delta \times \delta$. So γ must be necessarily a multiple of s in order to verify relation (16).

Furthermore, the corresponding parity check vector $(\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_\gamma)$ of this codeword is given by the relations

$$\begin{aligned} \mathbf{y}_0 &= Du_0 \\ \mathbf{y}_j &= CA^{j-1}Bu_0 \quad \text{for } j = 1, 2, \ldots, \gamma - 1 \\ \mathbf{y}_\gamma &= CA^{\gamma-1}Bu_0 + Du_\gamma = (CA^{\gamma-1}B - D)u_0 \end{aligned}$$

But u_0 is a nonzero scalar of the field $\mathbb{F}$, since $\mathcal{C}(A,B,C,D)$ is an $(n,1,\delta)$-code, so

$$\sum_{t=0}^{\gamma} \mathrm{wt}(\mathbf{y}_t) = \mathrm{wt}(D) + \sum_{j=1}^{\gamma-1} \mathrm{wt}(CA^{j-1}B) + \mathrm{wt}(CA^{\gamma-1}B - D) \tag{17}$$

Now, from Theorem 1 we know that we can compute $\mathrm{z}_{\min}(\mathcal{C})$ as

$$\mathrm{z}_{\min}(\mathcal{C}) = \sum_{t=0}^{s} \mathrm{wt}(\mathbf{y}_t),$$

where $(\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_s)$ is the sequence of the parity check vectors of a certain finite-weight codeword $\mathcal{V}_s$ whose inputs verify $u_0 = -u_s \neq 0$ and $u_t = 0$ for

$t = 1, 2, \ldots, s-1$. Finally, by applying relation (17) with $\gamma = r = s$ and taking into account that $A^{s-1} = I$, we obtain that

$$\mathrm{z}_{\min}(\mathcal{C}) = \sum_{t=0}^{s} \mathrm{wt}(\mathbf{y}_t) = \mathrm{wt}(D) + \sum_{j=1}^{s-1} \mathrm{wt}(CA^{j-1}B) + \mathrm{wt}(CA^{-1}B - D).$$

Remark 4 Note that it follows from Remark 2 that the integers d and s given by relations (13) and (14) are invariants of the convolutional code $\mathcal{C}$.

As an immediate consequence of the above theorem, we obtain conditions for an $(n, 1, \delta)$-code to have the maximum possible value of $\mathrm{z}_{\min}(\mathcal{C})$ among all the convolutional codes with the same parameters $(n, 1, \delta)$.

Theorem 2 *Let $\mathcal{C}(A, B, C, D)$ be an $(n, 1, \delta)$-code with $\delta \geq 2$, so that pair (A, B) is controllable and the matrix A is invertible and diagonalizable. Assume the minimum effective index s has the value given by (14) Then,*

$$\mathrm{z}_{\min}(\mathcal{C}) \leq (n-1)(s+1).$$

Moreover, if all the elements of matrices D, $CA^{s-1}B - D$ and CA^jB, for $j = 1, 2, \ldots, s-2$, are nonzero, then

$$\mathrm{z}_{\min}(\mathcal{C}) = (n-1)(s+1), \tag{18}$$

and consequently,

$$\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC}) = 2 + 2(n-1)(s+1). \tag{19}$$

In what follows, we present an example of a convolutional code that reach the maximum possible value of $\mathrm{z}_{\min}$, according to the upper-bound given by relation (12).

Example 3 Let α be a primitive element of the field $\mathbb{F} = GF(8)$ with $\alpha^3 + \alpha + 1 = 0$. Let $\mathcal{C}(A, B, C, D)$ be the $(3, 1, 3)$-code, where

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

$$C = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} \alpha^2 \\ 1 \end{pmatrix}.$$

Since (A, B) is controllable, the above matrices give rise to a minimal input state output representation of $\mathcal{C}$. Also, (A, C) is an observable pair. Moreover, the integer d defined by relation (13) of Lemma 5 and the minimum effective index s have the values $d = 1$ and $s = q - 1 = 7$. Furthermore, all the elements of matrices D, $CA^6B - D$ and CA^jB, for $j = 1, 2, \ldots, 5$, are nonzero so from Theorem 2, we obtain that $\mathrm{z}_{\min}(\mathcal{C})$ attains the upper bound given by (18), that is, $\mathrm{z}_{\min}(\mathcal{C}) = 16$.

3.2 Construction of an $(n, 1, \delta)$ recursive systematic convolutional code such that $\mathrm{z_{min}}(\mathcal{C})$ attains the maximum possible value

Next we provide a simple example to illustrate the idea of the general construction presented below.

Example 4 Let α be a primitive element of $\mathbb{F}_{16}$, with $\alpha^4+\alpha+1$. Let $\mathcal{C}(A, B, C, D)$ be the $(4, 1, 3)$-convolutional code described by the matrices

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

Since (A, B) is controllable, the above matrices describe $\mathcal{C}$ in a minimal way. Also, the pair (A, C) is observable. Furthermore, this convolutional code verifies the conditions of Lemma 5, with $s = q - 1 = 15$. Also, we can see that all the elements of the matrices D, $CA^{14}B - D$ and CA^jB, for $j = 1, 2, \ldots, 13$, are nonzero, so, in particular, $\mathcal{C}$ also verifies the conditions of Theorem 2, and therefore $\mathrm{z_{min}}(\mathcal{C})$ attains its maximum value. In fact, $\mathrm{z_{min}}(\mathcal{C}) = 48$.

It is possible to generalize Example 4 in order to get a concrete construction of an $(n, 1, \delta)$ recursive systematic convolutional code $\mathcal{C}(A, B, C, D)$ such that $\mathrm{z_{min}}(\mathcal{C})$ attains the maximum possible value, as the following theorem shows.

Theorem 3 *Let $\mathbb{F}$ be the Galois field of q elements and let α be a primitive element of $\mathbb{F}$. Let n, δ be any positive integers with $n > \delta$ and $2 \leq \delta \leq q$. Let $\mathcal{C}(A, B, C, D)$ be an $(n, 1, \delta)$-code described by the matrices*

$$A = \begin{pmatrix} \alpha^{r_1} & 0 & \cdots & 0 \\ 0 & \alpha^{r_2} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \alpha^{r_\delta} \end{pmatrix}, \qquad B = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \qquad C = \left(c_{ij}\right), \qquad D = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

where $\alpha^{r_i} \neq \alpha^{r_j}$ for all $i, j \in \{1, 2 \ldots, \delta\}$ with $i \neq j$. Let s be the minimum effective index of $\mathcal{C}$. Then, s is given by (14). Furthermore,

- *If $n - 1 = \delta$, let $C = (c_{ij})$ be the $\delta \times \delta$ matrix whose elements are given by*

$$c_{ij} = \begin{cases} \alpha^{p_i} & \text{if } i = j \\ 0 & \text{in the rest of the cases} \end{cases}$$

  assuming in this case that $p_i \neq -(s-1)r_i \bmod (q-1)$, for all $i = 1, 2, \ldots, n-1$.
- *If $n - 1 > \delta$, let $C = (c_{ij})$ be the $(n-1) \times \delta$ matrix whose elements are given by*

$$c_{ij} = \begin{cases} \alpha^{p_i} & \text{if } j = i - \lfloor \frac{i-1}{\delta} \rfloor \delta, \text{ for } i = 1, 2 \ldots, \lfloor \frac{n-1}{\delta} \rfloor \delta + h \\ 0 & \text{in the rest of the cases} \end{cases}$$

  where $0 \leq h < \delta$ is such that $n - 1 = \left\lfloor \frac{n-1}{\delta} \right\rfloor \delta + h$, and assuming that $p_i \neq -(s-1)r_{i \bmod \delta} \bmod (q-1)$.

Then, $\mathcal{C}(A,B,C,D)$ is a minimal representation of $\mathcal{C}$ with (A,C) observable. Moreover, $\mathrm{z}_{\min}(\mathcal{C}) = (n-1)(s+1)$, and

$$\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC}) = 2 + 2(n-1)(s+1).$$

Proof It is straightforward to verify that the pair (A,B) is controllable, the pair (A,C) is observable and the minimum effective index s is given by relation (14). We show that the convolutional code $\mathcal{C}(A,B,C,D)$ generated by the matrices given in the theorem, verifies the conditions of Theorem 2. Indeed, all the elements of D and CA^jB, for $j = 1,2,\ldots,s-2$ are nonzero. Now, observe that $CA^{-1}B - D = CA^{s-1}B - D = (e_{i,1})_{i=1,2\ldots,n-1}$ is the column vector with $n-1$ rows whose elements are given depending on the relationship between $n-1$ and δ. Specifically,

- If $n-1 = \delta$, then $e_{i,1} = \alpha^{p_i+(s-1)r_i} - 1$ for $i = 1,2,\ldots,n-1$.
- If $n-1 > \delta$, then $e_{i,1} = \begin{cases} \alpha^{p_i+(s-1)r_{i \bmod \delta}} - 1 & \text{if } i \bmod \delta \neq 0 \\ \alpha^{p_i+(s-1)r_\delta} - 1 & \text{if } i \bmod \delta = 0 \end{cases}$

By assumption, all the elements of this matrix are nonzero, so the convolutional code $\mathcal{C}(A,B,C,D)$ verifies all the hypothesis of Theorem 2, and we can conclude that its $\mathrm{z}_{\min}(\mathcal{C})$ attains the upper bound (18),

$$\mathrm{z}_{\min}(\mathcal{C}) = (n-1)(s+1),$$

and consequently, the effective free distance of $\mathcal{TC}$ also attains the upper bound (19),

$$\mathrm{d}_{\mathrm{free,eff}}(\mathcal{TC}) = 2 + 2(n-1)(s+1).$$

We conclude the paper with two concrete examples that ilustrate the construction given by Theorem 3.

Example 5 Let α be a primitive element of $\mathbb{F}_8$, with $\alpha^3+\alpha+1$. Let $\mathcal{C}(A,B,C,D)$ be the $(4,1,3)$-convolutional code described by the matrices

$$A = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^4 & 0 \\ 0 & 0 & \alpha^6 \end{pmatrix}, \quad B = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad C = \begin{pmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha^3 & 0 \\ 0 & 0 & \alpha^5 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Observe that $\mathcal{C}(A,B,C,D)$ satisfies the conditions of Theorem 3 and the minimum effective index of $\mathcal{C}$ is $s = q - 1 = 7$. Therefore $\mathrm{z}_{\min}(\mathcal{C})$ attains its maximum value. In fact, $\mathrm{z}_{\min}(\mathcal{C}) = 21$.

Example 6 Let α be a primitive element of $\mathbb{F}_8$, with $\alpha^3+\alpha+1$. Let $\mathcal{C}(A,B,C,D)$ be the $(6,1,3)$-convolutional code described by the matrices A and B of the Example 5 and matrices C and D given by

$$C = \begin{pmatrix} \alpha^2 & 0 & 0 \\ 0 & \alpha^3 & 0 \\ 0 & 0 & \alpha^5 \\ 1 & 0 & 0 \\ 0 & \alpha & 0 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Again $\mathcal{C}(A, B, C, D)$ verifies the conditions of Theorem 3. The minimum effective index of $\mathcal{C}$ is $s = q - 1 = 7$. Hence, $\mathrm{z}_{\min}(\mathcal{C})$ attains its maximum value, that in this case is $\mathrm{z}_{\min}(\mathcal{C}) = 35$.

4 Conclusions and Future Work

In this paper, we provided a first approach to study turbo codes using state-space representations. We showed that these representations can be useful to study turbo codes and presented some results in terms of linear systems. However, we have assumed some restrictions in the parameters of the codes considered in this work. It is a topic for future research to generalize our results to wider classes of turbo codes. For instance, it would be interesting to consider general rates k/n for $k > 1$, the concatenation of two convolutional codes that are not necessarily equal and realizations (A, B, C, D), with A not invertible.

5 Acknowledgement

The authors would like to thank the anonymous reviewers for the their constructive comments and efforts towards improving our manuscript. D. Napp was partially supported by the the Universitat d'Alacant (Grant No. VIGROB-287) and Generalitat Valenciana (Grant No. AICO/2017/128). V. Herranz and C. Perea were supported by the Ministerio de Economa, Industria y Competitividad within project TIN2016-80565-R.

References

1. Almeida, P., Napp, D., Pinto, R.:Superregular matrices and applications to convolutional codes. Linear Algebra App. **499**, 1–25 (2016).
2. Balta, H., Douillard, C., Lucaciu, R.: Multi-non-binary turbo codes. EURASIP J. Wirel. Comm. **2013**, 279 (2013).
3. Benedetto, S., Montorsi, G.: Design of parallel concatenated convolutional codes. IEEE Trans. Commun. **44**(5), 591–600 (1996).
4. Benedetto, S., Garello, R., Montorsi, G.: A search for good convolutional codes to be used in the construction of Turbo Codes. IEEE Trans. Commun. **46**(9), 1101–1105 (1998).
5. Berrou, C., Glavieux, A., Thitimajshima, P.: Near Shannon limit error-correcting coding and decoding: Turbo Codes (1). Proc. of IEEE ICC 93, 1064–1070 (1993).
6. Briffa, J. A., Schaathun, H. G.: Non-binary turbo codes and applications. Proc. IEEE Int. Symp. Turbo Codes and Related Topics, 294–298 (2008).
7. Chatzigeorgiou, I., Wassell, I. J.: Revisiting the calculation of the effective free distance of turbo codes. Electron. Lett. **44**(1), 43–44 (2008).
8. Campillo, P., Devesa, A., Herranz, V., Perea, C.: Modelization of turbo encoder from linear system point of view. Proc. CMMSE 2010, J. Vigo Aguiar, Ed., 314–317 (2010).
9. Carriegos, M. V., DeCastro-Garca, N.: Partitions of elements in a monoid and its applications to systems theory. Linear Algebra App. **491**, 161–170 (2016).
10. Climent, J.-J., Herranz, V., Perea, C.: A first approximation of concatenated convolutional codes from linear systems theory viewpoint. Linear Algebra Appl. **425**, 673–699 (2007).

11. ——, Linear system modelization of concatenated block and convolutional codes. Linear Algebra App. **429**, 1191–1212 (2008).
12. ——, Parallel concatenated convolutional codes from linear systems theory viewpoint. Syst. Control Lett. **96**, 15–22 (2016).
13. Divsalar, D., Pollara, F.: Low Rate Turbo Codes for Deep Space Communications. Proceedings of 1995 IEEE Int. Symp. Info. Theory (1995).
14. Divsalar, D., McEliece, R. J.: The effective free distance of turbo codes. *Electronics Letters*, **32** (5), 445–446 (1996).
15. Divsalar, D., McEliece, R. J.: On the design of generalized concatenated coding systems with interleavers. TMO Progress Report 42–134, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA. (1998).
16. Fornassini, E., Pinto, R.: Matrix fraction descriptions in convolutional coding. Linear Algebra Appl. **392**, 119–158 (2004).
17. Galiano, V., Gandía, R., Herranz, V.: Increasing forward error correcting codes capabilities with convolutional codes over any finite field. Proc. of the 21st MTNS., Groningen, The Netherlands. (2014).
18. García-Planas, M. I., Soudit, E. M., Um, L. E.: Analysis of control properties of concatenated convolutional codes. Cybern. Phys. **1** (4), 252–257 (2012).
19. Kalman, R. E., Falb, P. L. Arbib, M. A.: Topics in Mathematical System Theory. McGraw-Hill, New York (1969).
20. Liva, G., Paolini, E., Scalise, S., Chiani, M.: Turbo codes based on time-variant memory-1 convolutional codes over $\mathbb{F}_q$. Proc. of Int. Conf. Comm (ICC), 1–6 (2011).
21. McEliece, R. J.: The algebraic theory of convolutional codes. Handbook of Coding Theory. V. S. Pless and W. C. Huffman, Eds. Elsevier, 1065–1138, (1998).
22. Massey, J. L., Sain, M. K.: Codes, automata, and continuous systems: explicit interconnections. IEE Trans. Automat. Contr. **AC-12** (6), 644-650 (1967).
23. Napp, D., Perea, C., Pinto, R.: Input-state-output representations and constructions of finite support 2D convolutional codes. Adv. Math. Commun. **4** (4(), 533–545 (2010).
24. Napp, D., Smarandache, R.: Constructing Strongly MDS convolutional codes with maximum distance profile. Adv. Math. Commun. **10** (5), 275–290 (2016).
25. Napp, D., Pereira, R., Pinto, R., Rocha, P.: Periodic state-space representations of periodic convolutional codes. Cryptogr. Commun. **11** (4), 585–595 (2019).
26. Perez, L. C., Seghers, J., Costello, Jr, D. J.: A distance spectrum interpretation of turbo codes. IEEE Trans. Inform. Theory **42** (6), 1698–1709, (2002).
27. Ping, L. , Leung, W. K., Wu, K. Y.: Low-rate turbo-Hadamard codes. IEEE Trans. Inform. Theory. **49** (12), 3213-3224 (2003).
28. Reid, A. C., Gulliver, T. A., Taylor, D. P.: Rate-1/2 component codes for nonbinary turbo codes. IEEE Trans. Commun. **53** (9), 1417–1422 (2005).
29. Rosenthal, J., Schumacher, J. M., York, E. V.: On behaviors and convolutional codes. IEEE Trans. Inf. Theory **42** (6), 1881–1891 (1996).
30. Rosenthal, J., Smarandache, R.: Maximum distance separable convolutional codes. Appl. Algebr. Eng. Comm. **10** (1), 15–32, (1999).
31. Rosenthal, J., York, E. V.: BCH convolutional codes. Trans. Inform. Theory **45** (6), 1833–1844, (1999).
32. Rosenthal, J.: Connections between linear systems and convolutional codes. Codes, Systems and Graphical Models, ser. The IMA Volumes in Mathematics and its Applications, B. Marcus and J. Rosenthal, Eds. Springer-Verlag, **123**, 39–66 (2001).
33. Smarandache, R., Joachim, R.: Construction of Convolutional Codes using Methods from Linear Systems Theory. Proc.of the 35-th Annual Allerton Conf. on Commun., Control, and Computing 953-960, (1997).
34. Smarandache, R., Joachim, R.: A state space approach for constructing MDS rate $1/n$ convolutional codes. Proc. of the 1998 IEEE Inform. Theory Workshop (ITW 1998), 116-117 (1998).
35. Sripimanwat, K.: Turbo Code Applications. A Journey from a Paper to Realization. Springer. The Netherlands (2005).
36. Vatta, F., Graell i Amat A., Banerjee, A., Costello, D. J.: Nonsystematic turbo codes: Design and bounds on effective free distance. ISITA 2008 (2008).
37. Vucetic, B., Yuan, J.: Turbo Codes. Principles and Applications. Boston, MA: Kluwer Academic Publishers (2000).

38. York, E. V.: Algebraic Description and Construction of Error Correcting Codes: A Linear Systems Point of View. PhD thesis, University of Notre Dame (1997).