Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(1): 713–732.
DOI:10.3934/math.2023034
Received: 15 June 2022
Revised: 19 August 2022
Accepted: 05 September 2022
Published: 11 October 2022

Research article

Weight-2 input sequences of $1/n$ convolutional codes from linear systems point of view

Victoria Herranz[1,*], **Diego Napp**[2] **and Carmen Perea**[1]

[1] Institute Center of Operations Research, Miguel Hernández University, Spain
[2] Departament of Mathematics, University of Alicante, Spain

* **Correspondence:** Email: mavi.herranz@umh.es; Tel: +34-966-658-537; Fax: +34-966-658-715.

Abstract: Convolutional codes form an important class of codes that have memory. One natural way to study these codes is by means of input state output representations. In this paper we study the minimum (Hamming) weight among codewords produced by input sequences of weight two. In this paper, we consider rate $1/n$ and use the linear system setting called (A, B, C, D) input-state-space representations of convolutional codes for our analysis. Previous results on this area were recently derived assuming that the matrix A, in the input-state-output representation, is nonsingular. This work completes this thread of research by treating the nontrivial case in which A is singular. Codewords generated by weight-2 inputs are relevant to determine the effective free distance of Turbo codes.

Keywords: convolutional codes; input-state-output representations; linear time-invariant systems; effective free distance
Mathematics Subject Classification: 94B10, 93C05, 11T71

1. Introduction

In this work we are interested in investigating codewords of $1/n$ convolutional codes that are produced by weight-2 information sequences. These codewords play an important role in the computation of the effective free distance in the context of Turbo codes (see [14]) and therefore a better understanding of this particular set of codewords may lead to improvements in the construction of Turbo codes. In this work we focus on the mathematical analysis of these set rather than on possible direct consequences in the performance of Turbo codes. We perform this mathematical investigation within the so-called input state output representations.

Convolutional codes can be modelled by means of input state output representations in the framework of linear time-invariant systems (see [3, 5, 6, 8, 16, 27, 30] for an introduction of the basic theory of this approach). The main advantage of this approach is that the dynamics of the state (memory) of the system (convolutional code) are explicit in this representation. Moreover this enables the application of the huge and powerful machine of systems theory problems in the context of coding theory.

In [14] Divsalar and McEliece studied codewords of convolutional codes that are produced by weight-2 information sequences, derived some theoretical bounds for the effective free distance and posed a conjecture. In this paper, we also make use of a state-space representations but choose representations as introduced in [30] which are slightly different to the driven variable representations used in [14]. These representations led to several important theoretical and practical results of convolutional codes (see [7,8,10,18,21,25,26]) and we continue the study in [19] using the (A, B, C, D) input state output representation of finite-weight convolutional codes. In [19], an upper bound on the effective free distance distance was provided for the particular case in which the matrix A in the input state output representation is an invertible matrix. In this paper we consider the case in which the matrix A is singular. Thus, this work can be considered as an extension of previous results. When the matrix A, that represents the update of the state of the system, is nonsingular, the last input entering into the system must immediately steer the state vector to the zero vector in order to obtain a finite-weight codeword. However, when A is singular, this is not necessarily true, and the state vector might remain nonzero some time after the last input has been introduced into the system. For this reason the extension of the results in [19] to the general case is not straightforward as we show in this work. Nevertheless, we present new characterizations of this set of codewords and provide an upper-bound on the effective free distance. As we show in the this paper, the analysis of these systems (with A singular) turned out to be highly nontrival and so the optimally of the upper-bound could not be formally proven.

The paper is organized as follows: In Section 2 we briefly introduce finite-weight convolutional codes defined over any Galois field and a particular input-state-output representation of such codes. We also recall the relevance of codewords generated by weight-2 inputs and their relation to turbo codes. Section 3 is devoted to provide the main results of the paper. In particular, for a given convolutional code C of dimension one defined over any finite field with an input-state-output representation given by (A, B, C, D) and A a singular matrix, we analyse the dynamics that can occur between the input and the state of the system in this case. We present a conjecture and a novel upper bound on $\mathrm{z}_{\min}(C)$ based on this conjecture and, in turn, an upper bound on the effective free distance of C. Finally, we present and study a concrete construction of a class of convolutional codes for which we can compute $\mathrm{z}_{\min}(C)$ up to a difference of one value and provide an example to illustrate the results. We conclude the paper by presenting some conclusion and possible future work within this thread of research.

2. Basic definitions and properties of 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 [30] and [28], a rate k/n convolutional code C of complexity δ can be described by the linear system governed by the equations

$$\left.\begin{array}{rcrcr} \vec{x}_{t+1} & = & A\vec{x}_t & + & B\vec{u}_t \\ \vec{y}_t & = & C\vec{x}_t & + & D\vec{u}_t \end{array}\right\}, \quad t = 0, 1, 2, \ldots \tag{2.1}$$

$$\vec{v}_t = \begin{pmatrix} \vec{y}_t \\ \vec{u}_t \end{pmatrix}, \quad x_0 = 0, \tag{2.2}$$

where for each time instant t, $\vec{x}_t \in \mathbb{F}^\delta$ is the *state vector*, $\vec{u}_t \in \mathbb{F}^k$ is the *input* (also call *information vector*) and $\vec{y}_t \in \mathbb{F}^{n-k}$ is the *parity 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 [28]) and it has been widely used in the last years to analyze and construct convolutional codes [8, 9, 29, 30]. In terms of Linear Systems, the complexity δ, is the McMillan degree of the linear system (2.2). In the following, we adopt the notation used by McEliece [24] and we call a convolutional code of rate k/n and complexity δ an (n, k, δ)-code.

Note that the description given by expression (2.2) is in general not unique. But if 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. 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 [29]), the controllability matrix has full rank, $\operatorname{rank} \Phi_\delta(A, B) = \delta$, where

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

The controllablility matrix is a well-known matrix in the area of system theory as it allows to characterized the controlability of the linear system. 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 (see [29]). If the pair (A, B) is controllable, it means that, by an appropriate choice of input vectors, it is possible to drive a given state vector to any other state vector in finite time. Analogously, the observability of the pair (A, C) means that it is possible to determine the state vector at a given time t_0 by observing the output vectors for a finite number of time steps beginning with t_0 (see, for example, [28, 30]).

Following the approach adopted in [29] we only consider $\{\vec{v}_t\}_{t \geq 0}$ in Eq (2.2) to be a finite-weight codeword (see [29] for more details of the algebraic reasons to do so), that is, Equation (2.2) holds for all $t = 0, 1, 2, \ldots$ and there is an integer γ such that $\vec{x}_{\gamma+1} = 0$, $\vec{u}_t = 0$, for $t \geq \gamma + 1$, and therefore, $\vec{y}_t = 0$ for $t \geq \gamma + 1$, so the code sequence has finite weight. In this work we denote such a finite-weight codeword by $\mathcal{V}_\gamma$.

Hence, it follows that both the input and the state sequence (and hence the output) must to have finite support in a finite-weight codeword. The set of finite-weight codewords has a module structure over the polynomial ring $\mathbb{F}[z]$ (see [29]). By abuse of notation, we will denote this module by $C(A, B, C, D)$ and we refer to it as the *finite-weight convolutional code* generated by the matrices A, B, C, D. Proposition 2.4 of [29] gives us a characterization of finite-weight codewords. Let us denote by $\mathcal{V}_\gamma$ a finite-weight codeword sequence constituted by $\begin{pmatrix} \vec{y}_0 \\ \vec{u}_0 \end{pmatrix}, \begin{pmatrix} \vec{y}_1 \\ \vec{u}_1 \end{pmatrix}, \ldots, \begin{pmatrix} \vec{y}_\gamma \\ \vec{u}_\gamma \end{pmatrix} \in \mathbb{F}^n$ represents with $\begin{pmatrix} \vec{y}_0 \\ \vec{u}_0 \end{pmatrix}$ and $\begin{pmatrix} \vec{y}_\gamma \\ \vec{u}_\gamma \end{pmatrix} \neq 0$. Hence, the Eqs of (2.2) are satisfied for all $t \geq 0$ and

$$\begin{pmatrix} A^\gamma B & A^{\gamma-1}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} \vec{u}_0 \\ \vec{u}_1 \\ \vdots \\ \vec{u}_{\gamma-1} \\ \vec{u}_\gamma \end{pmatrix} = 0. \tag{2.3}$$

Remark 2.1. Notice that it is easy to check that if S is an invertible matrix, then it holds that

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

The representation considered here, i.e., (2.2), is indeed the description of the dynamics of a rational and systematic encoder, since by Lemma 2.14 of [29], if $C(A, B, C, D)$ is an (n, k, δ)-code, then, the matrices A, B, C and D describe a proper rational transfer function of $C(A, B, C, D)$, given by

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

Furthermore, $G(z) = \begin{pmatrix} T(z) \\ I_k \end{pmatrix}$ is a systematic encoder of $C(A, B, C, D)$.

Remark 2.2. We note that the state-space realizations considered in this work are different from the driving variable realizations often found in the coding literature [15, 23], given by

$$\left.\begin{array}{rcrcr} \vec{x}_{t+1} & = & \mathcal{A}\vec{x}_t & + & \mathcal{B}\vec{u}_t \\ \vec{v}_t & = & \mathcal{C}\vec{x}_t & + & \mathcal{D}\vec{u}_t \end{array}\right\}, \tag{2.4}$$

where $\vec{u}_t \in \mathbb{F}^k$ is the *information vector*, $\vec{v}_t \in \mathbb{F}^n$ the codewords that are, in this case, the outputs of the linear system and $\vec{x}_t \in \mathbb{F}^\delta$ as above. Although driving-variable representations have been considered the standard way in which convolutional codes were presented in terms of linear systems, many authors have considered linear systems as described in (2.1) and (2.2) in the last decades as they have many advantages when analyzing convolutional codes [28, 29, 33]. One of these advantages is that in the driving variable representations, the matrix $\mathcal{A}$ has to be nilpotent whereas in the one described in (2.1) and (2.2) the matrix A does not have such a restriction. This fact facilitates the construction of optimal input state output representations of convolutional codes (see [29, 32, 33]). Another advantage of the setting considered in this paper is that these representations are particularly suitable not only for constructing convolutional codes but also for dealing with finite-weight codewords, see [29,30] for more details. These properties allow us to derive new results regarding lowest weight of the parity vectors of the convolutional code C generated by information sequences of weight two.

Block codes having optimal error correcting capabilities, i.e., with maximum minimum, are quite well-understood, e.g. the class of Reed-Solomon codes [20, 34]. However, in order to derive codes with efficient performance, i.e., codes coming closest to the Shannon limit, having large minimum distance it is same times not enough. To achieve optimal performance parallel concatenation of convolutional codes, known as Turbo Codes, were presented by Glavieux and Thitimajshima, see [2]. In a turbo code $\mathcal{TC}$ two convolutional codes, C_1 and C_2 of rates k/n_1 and k/n_2, respectively, are connected via an inter-leaver in such a way that the first encoder, C_1, operates directly on the input information $\vec{u}_t$ $(t = 0, 1, 2, \ldots)$ and the second one, C_2, encodes the interleaved input information, denoted by $P\vec{u}_t$ $(t = 0, 1, 2, \ldots)$, where P is a permutation matrix of order k. Therefore, a codeword of these code in divided in the parity vectors of both encoders followed by the information vector. In [4] the input-state-output representation for the turbo code $\mathcal{TC}$ was introduced from the state representation of the constituent encoders. For more results on these concatenated (convolutional) codes within a linear systems approach the reader is reffered to [8], [9], [11], [15] and [17].

The most important parameter through which the constituent convolutional codes influence the turbo code performance is $\mathrm{z}_{\min}(C)$ (see [1], [12], [13] and [14]), which it is defined below.

Definition 2.1. Let C be a convolutional code. We define $\mathrm{z}_{\min}(C)$ as the lowest weight of the parity vectors of the convolutional code C generated by information sequences of weight two.

In [1] and [14] it was shown that the performance of turbo codes is primarily driven by the weight-2 input minimum distance, which is directly related to the minimum weight among the set of codeword sequences generated by input sequences of weight two. Hence, if one considers a $\mathcal{TC}$ with $C_1 = C_2 = C$, its weight-2 input minimum distance, which is also referred to as the *effective free distance* of $\mathcal{TC}$ [1], $\mathrm{d}_{\text{free,eff}}(\mathcal{TC})$, is described as

$$\mathrm{d}_{\text{free,eff}}(\mathcal{TC}) = 2 + 2\,\mathrm{z}_{\min}(C). \tag{2.5}$$

3. Upper bounds on the effective free distance of $1/n$ turbo codes

On a AWGN cannel, code performance is determined largely by the effective free distance. In this section, we get bounds on this distance. Moreover, the design objective for the constituent recursive convolutional encoders of a turbo code is to obtain $\mathrm{z}_{\min}$ as large as possible. In [1] it was shown that in the binary case there exists a rate $1/n$ recursive systematic convolutional code C with complexity δ that achieve the maximum value of $\mathrm{z}_{\min}(C)$, described by

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

Consequently, for a turbo code $\mathcal{TC}$ with two equal systematic convolutional codes, they obtain the following upper bound on the effective free distance of $\mathcal{TC}$

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

Recently, in [19] turbo codes were again studied within a linear systems point of view, over finite field. In particular, they consider a turbo code obtained by the concatenation of two identical $1/n$ recursive systematic convolutional codes C given by its input-state-output representation (A, B, C, D) where the matrix A is invertible. They studied how to obtain the value of $\mathrm{z}_{\min}(C)$, and derived an upper bound that we present next. First, we need to introduce the following definition, which refers to the minimum time instant at which the last nonzero input is introduced into the system.

As at each time instant the input belongs to the field, in the case the rate is $1/n$, we use the typography u_t rather than $\vec{u}_t$, to distinguish between scalars and vectors.

Definition 3.1. We define $\hat{s}$ to be the least s for which there exists a finite-weight codeword $\mathcal{V}_\gamma$ of a convolutional code C generated by a vector $(u_0, u_1, \dots, u_s, u_{s+1}, \dots, u_\gamma)$ with weight equal to two and $u_0, u_s \neq 0$. Such an $\hat{s}$ is called the *minimum effective index of* C.

In [19] an upper bound on the value of $\mathrm{z}_{\min}(C)$ among all convolutional codes with equal set of parameters $(n, 1, \delta)$ was introduced, as we show in the following theorem.

Theorem 3.1. *[Corollary 1 of [19]] Let $C(A, B, C, D)$ be an $(n, 1, \delta)$-code, in such a way that the pair (A, B) is controllable and A is an invertible matrix. Let $\hat{s}$ be the minimum effective index of C. Then,*

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

and, in turn, the effective free distance of $\mathcal{TC}$ satisfies

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

The authors of [19] give conditions for an $(n, 1, \delta)$-code to achieve such a bound and they moreover present a concrete construction of an $1/n$ recursive systematic convolutional code C whose $\mathrm{z}_{\min}(C)$ is as maximum as possible for these parameters.

Remark 3.1. If we consider that case in which the matrix A is nonsingular, we get $\mathrm{z}_{\min}(C)$ over the parity vectors of finite-weight codewords $\mathcal{V}_\gamma$ generated by input vectors $(u_0, u_1, \dots, u_s)$ of weight two with u_0,$u_s \neq 0$, with $\gamma = s$, since at time instant s the state of the system must go to zero. Thus, the last input u_s entering into the system has to yield $x_{s+1} = 0$. More concretely, let $\mathcal{V}_\gamma$ be a finite-weight codeword generated by an information vector $(u_0, u_1, \dots, u_s, u_{s+1}, \dots, u_\gamma)$ of weight two with u_0,$u_s \neq 0$. Then,

$$\begin{pmatrix} A^\gamma B & A^{\gamma-1}B & \cdots & A^{\gamma-s}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_s \\ \vdots \\ u_{\gamma-1} \\ u_\gamma \end{pmatrix} = A^{\gamma-s} \begin{pmatrix} A^sB & A^{s-1}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{s-1} \\ u_s \end{pmatrix} = 0 \qquad (3.1)$$

implies

$$\begin{pmatrix} A^sB & A^{s-1}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{s-1} \\ u_s \end{pmatrix} = 0,$$

since A is nonsingular. In other words, if A is nonsingular, it follows that the minimum effective index $\hat{s}$ of C is obtained by the minimum of the integers s that satisfy the conditions indicated at the beginning of the remark. Moreover, Theorem 1 of [19] indicates that $\mathrm{z}_{\min}(C)$ is derived only by the weight of the parity vectors of any finite-weight codeword $\mathcal{V}_{\hat{s}}$ of the convolutional code produced by sequences with length $\hat{s} + 1 \geq \delta + 1$ where the two nonzero inputs are the first and the last ones.

When the matrix A is singular we may have that

$$\begin{pmatrix} A^sB & A^{s-1}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{s-1} \\ u_s \end{pmatrix} \neq 0$$

but relation (3.1) holds. This intuitively means that the state of the system (A, B, C, D) does not necessarily vanish at instant s and could remains nonzero for some time after the second (that is, the last) input $u_s \neq 0$ enters into the system. Moreover, let $\mathcal{V}_\gamma$ and $\tilde{\mathcal{V}}_{\tilde{\gamma}}$ be two finite-weight codewords with input vectors $(u_0, u_1, \dots, u_s, u_{s+1} \dots, u_\gamma)$ and $(\tilde{u}_0, \tilde{u}_1, \dots, \tilde{u}_{\tilde{s}}, \tilde{u}_{\tilde{s}+1} \dots, \tilde{u}_{\tilde{\gamma}})$ of weight two with u_0,u_s, $\tilde{u}_0$, $\tilde{u}_{\tilde{s}} \neq 0$ and such that $\tilde{s} > s$. As opposed to the case in which A is nonsingular, in this case we cannot ensure that

$$\mathrm{wt}(y_0, \dots, y_s, y_{s+1}, \dots, y_\gamma) \leq \mathrm{wt}(\tilde{y}_0, \dots, \tilde{y}_s, \dots, \tilde{y}_{\tilde{s}}, \tilde{y}_{\tilde{s}+1}, \dots, \tilde{y}_{\tilde{\gamma}}),$$

that is, the minimum effective index $\hat{s}$ given in Definition 3.1 is not directly related to $\mathrm{z}_{\min}(C)$ is in the case where the matrix A is singular. Therefore, the ideas used to show Theorem 3.1 for A nonsingular cannot be straightforward applied in this case and we need to use a different approach.

3.1. $z_{\min}$ *of a rate* $1/n$ *recursive systematic convolutional code* $C(A,B,C,D)$ *with* A *singular.*

Next, we investigate the set of finite-weight codewords generated by input vectors of weight two which give us the value of $z_{\min}$ when an $(n,1,\delta)$-code C is given by an input-state-output representation (A,B,C,D) such that the matrix A that updates the state vector of the system is singular. As noted in Remark 3.1 the length $\gamma+1$ of the finite-weight codeword $\mathcal{V}_\gamma$ can be much larger than the minimum time instant of the last nonzero input, denoted by s. Note that in these $\gamma-s$ instants, the corresponding input is zero but the state is nonzero and continues to generates outputs vectors $y_i = Cx_i$, $i = s+1,\dots,\gamma$. This makes it difficult to obtain an upper bound on $z_{\min}$ in terms of the minimum effective index. Nevertheless, we can delimit the inputs that will generate the finite-weight codewords where $z_{\min}$ will be reached, as we will see at the end of this section.

Now suppose that $C(A,B,C,D)$ is a rate $1/n$ convolutional code with complexity δ. Then, the matrices (A,B) form a controllable pair, so

$$\operatorname{rank}\Phi_\kappa(A,B) = \operatorname{rank}\begin{pmatrix} B & AB & \cdots & A^{\kappa-1}B\end{pmatrix} = \delta, \tag{3.2}$$

where κ is the so-called controllability index of (A,B). Also, in the case that $C(A,B,C,D)$ is an $(n,1,\delta)$-code with (A,B) controllable, it follows that the controllability index κ is equal to the complexity δ, $\kappa=\delta$.

Now, let $\mathcal{V}_\gamma$ be a finite-weight codeword with $u_0 \neq 0$. Then, relations (2.3) and (3.2), imply necessarily $\gamma > \kappa-1$ and therefore, we get the following result.

Lemma 3.1. *Let $C(A,B,C,D)$, with (A,B) controllable, be an $(n,1,\delta)$-code. It holds that the length $\gamma+1$ of a finite-weight codeword with input weight 2 satisfies that $\gamma \geq \delta$.*

Among all the parity vectors of finite-weight codewords generated by input vectors of weight two we can restrict ourselves to a smaller set in order to compute $z_{\min}(C)$, as stated in the following lemma.

Lemma 3.2. *Let $C(A,B,C,D)$ be an $(n,1,\delta)$-code with the pair (A,B) controllable. Let $\mathcal{V}_\gamma$ be a finite-weight codeword generated by the input vector $(u_0,u_1,\dots,u_s,u_{s+1}\dots,u_\gamma)$ of weight two with $u_0,u_s \neq 0$. Then, the codeword $\mathcal{V}_{\gamma+m}$ generated by the input vector $(u_0,u_1,\dots,u_s,u_{s+1}\dots,u_\gamma,u_{\gamma+1},\dots,u_{\gamma+m})$ of weight two with $u_0,u_s \neq 0$ is a finite-weight codeword for all $m \in \mathbb{N}$. Moreover,*

$$\mathrm{wt}(\vec{y}_0,\dots,\vec{y}_s,\vec{y}_{s+1},\dots,\vec{y}_\gamma) \leq \mathrm{wt}(\vec{\tilde{y}}_0,\vec{\tilde{y}}_1,\dots,\vec{\tilde{y}}_s,\vec{\tilde{y}}_{s+1},\dots,\vec{\tilde{y}}_\gamma,\dots,\vec{\tilde{y}}_{\gamma+m}).$$

Proof. Since $\mathcal{V}_\gamma$ is a finite-weight codeword, taking into account relation (2.3), we know that $A^\gamma u_0 + A^{\gamma-s}u_s = 0$. In particular, $A^m(A^\gamma u_0 + A^{\gamma-s}u_s) = A^{\gamma+m}u_0 + A^{\gamma+m-s}u_s = 0$, so $\mathcal{V}_{\gamma+m}$ is a finite-weight codeword. Now, observe that the components of the parity vector $(\vec{y}_0,\vec{y}_1,\dots,\vec{y}_s)$ of $\mathcal{V}_\gamma$ are given by the following relations

$$\begin{aligned}
\vec{y}_0 &= Du_0\\
\vec{y}_j &= CA^{j-1}Bu_0 \quad \text{for } j = 1,2,\dots,s-1\\
\vec{y}_s &= CA^{s-1}Bu_0 + Du_s\\
\vec{y}_j &= CA^{j-1}Bu_0 + CA^{j-s}Bu_s \quad \text{for } j = s+1,\dots,\gamma
\end{aligned}$$

and the components of the parity vector $(\vec{\tilde{y}}_0, \vec{\tilde{y}}_1, \dots, \vec{\tilde{y}}_s, \vec{\tilde{y}}_{s+1}, \dots, \vec{\tilde{y}}_\gamma, \dots, \vec{\tilde{y}}_{\gamma+m})$ of $\tilde{\mathcal{V}}_{\gamma+m}$ are in fact

$$\begin{aligned}
\vec{\tilde{y}}_0 &= Du_0 = \vec{y}_0 \\
\vec{\tilde{y}}_j &= CA^{j-1}Bu_0 = \vec{y}_j \quad \text{for } j = 1, 2, \dots, s-1 \\
\vec{\tilde{y}}_s &= CA^{s-1}Bu_0 + Du_s = \vec{y}_s \\
\vec{\tilde{y}}_j &= CA^{j-1}Bu_0 + CA^{j-s}Bu_s \quad \text{for } j = s+1, \dots, \gamma+m
\end{aligned}$$

So,

$$\mathrm{wt}(\vec{y}_0, \dots, \vec{y}_s, \vec{y}_{s+1}, \dots, \vec{y}_\gamma) \leq \mathrm{wt}(\vec{\tilde{y}}_0, \vec{\tilde{y}}_1, \dots, \vec{\tilde{y}}_s, \vec{\tilde{y}}_{s+1}, \dots, \vec{\tilde{y}}_\gamma, \dots, \vec{\tilde{y}}_{\gamma+m}).$$

□

Assume now that $C(A, B, C, D)$ is a rate $1/n$ convolutional code with A singular. It is well-known that if (A, B) is a controllable pair, we can assume without loss of generality (see Remark 2.1) that

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ p_{\delta-1} & p_{\delta-2} & p_{\delta-3} & \cdots & p_0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{3.3}$$

(the so-called controllable canonical realization [22]). If A is a singular matrix, then there exists an integer $\tau \geq 1$ such that $p_{\delta-j} = 0$ for $j = 1, 2, \dots, \tau$ and $p_{\delta-\tau-1} \neq 0$.

In the remain of this section, we work with the controllable canonical form of (A, B) with A singular. Let $\mathcal{V}_\gamma$ be a finite-weight codeword generated by an information vector $(u_0, u_1, \dots, u_s, u_{s+1}, \dots, u_\gamma)$ of weight two, with only $u_0, u_s \neq 0$. From (2.3) we have that

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

that is,

$$A^sBu_0 + Bu_s \in \ker(A^{\gamma-s}). \tag{3.4}$$

So we focus our attention in the kernel of the matrix A^η, for $\eta \geq 1$.

The following result provide us with the structure of the η-th power of the matrix A, that we will need later on. Throughout all the paper, we denote by $O_{\alpha\times\beta}$ the $\alpha \times \beta$ zero matrix and by I_m the identity matrix of size m.

Lemma 3.3. *Let (A, B, C, D) be the controllable canonical realization of an $(n, 1, \delta)$ convolutional code C, that is, A and B are matrices as in (3.3). Assume that A is singular and let τ be the integer such that $p_{\delta-j} = 0$ for $j = 1, 2, \dots, \tau$ and $p_{\delta-\tau-1} \neq 0$. Denote by A^η the η-th power of A for $\eta \geq 1$ and by $a(\eta)_{ij}$ the element of A^η corresponding to the row i and the column j. Then:*

1. *If $\eta \leq \delta - 1$, then*

$$A^{\eta} = \begin{pmatrix} O_{(\delta-\eta)\times\eta} & A(\eta)_{12} \\ A(\eta)_{21} & A(\eta)_{22} \end{pmatrix},$$

where $A(\eta)_{12} = I_{(\delta-\eta)}$ and $A(\eta)_{21}$ and $A(\eta)_{22}$ are matrices of sizes $\eta\times\eta$, and $\eta\times(\delta-\eta)$, respectively. Furthermore, the matrix $A(\eta)_{21}$ is a square matrix such that

- *If $\eta \leq \tau$, then $A(\eta)_{21} = O_{(\delta-\eta)\times(\delta-\eta)}$*

- *If $\eta > \tau$, then the elements $(a(\eta)_{ij})_{\substack{i = \delta - \eta + 1,\dots,\delta \\ j = 1,\dots,\delta}}$ are given by*

$$a(\eta)_{ij} = \begin{cases} 0 & \textit{if} \left\{ \begin{array}{l} i = \delta - \eta + 1,\dots,\delta \\ j = 1,\dots,\tau \end{array} \right. \\ a(\eta-1)_{i+1,j} & \textit{if} \left\{ \begin{array}{l} i = \delta - \eta + 1,\dots,\delta - 1 \\ j = \tau + 1,\dots,\eta \end{array} \right. \\ p_{\eta-2}a(\eta-1)_{\delta-\eta,j} + \cdots + p_1 a(\eta-1)_{\delta-1,j} + p_0 a(\eta-1)_{\delta,j} & \textit{if} \left\{ \begin{array}{l} i = \delta \\ j = \tau + 1,\dots,\eta \end{array} \right. \end{cases}$$

and the elements $(a(\eta)_{ij})_{\substack{i = \delta - \eta + 1,\dots,\delta \\ j = \eta + 1,\dots,\delta}}$ of the matrix $A(\eta)_{22}$ are given by

- *If $\eta \leq \tau$, then*

$$a^{(\eta)}_{ij} = \begin{cases} 0 & \textit{if} \left\{ \begin{array}{l} i = \delta - \eta + 1,\dots,\delta \\ j = \eta + 1,\dots,\tau \end{array} \right. \\ a(\eta-1)_{i+1,j} & \textit{if} \left\{ \begin{array}{l} i = \delta - \eta + 1,\dots,\delta - 1 \\ j = \tau + 1,\dots,\delta \end{array} \right. \\ p_{\eta-2}a(\eta-1)_{\delta-\eta+2,j} + \cdots + p_0 a(\eta-1)_{\delta,j} & \textit{if} \left\{ \begin{array}{l} i = \delta \\ j = \eta + 1,\dots,\tau + \eta \end{array} \right. \\ p_{\delta-j+\eta-1} + p_{\eta-2}a(\eta-1)_{\delta-\eta+2,j} + \cdots + p_0 a(\eta-1)_{\delta,j} & \textit{if} \left\{ \begin{array}{l} i = \delta \\ j = \tau + \eta + 1,\dots,\delta \end{array} \right. \end{cases}$$

- *If $\eta > \tau$, then*

$$a(\eta)_{ij} = \begin{cases} a(\eta-1)_{i+1,j} & \textit{if} \left\{ \begin{array}{l} i = \delta - \eta + 1,\dots,\delta - 1 \\ j = \eta + 1,\dots,\delta \end{array} \right. \\ p_{\eta-2}a(\eta-1)_{\delta-\eta+2,j} + \cdots + p_0 a(\eta-1)_{\delta,j} & \textit{if} \left\{ \begin{array}{l} i = \delta \\ j = \eta + 1,\dots,\delta \end{array} \right. \end{cases}$$

2. *If $\eta \geq \delta$, then*

$$A(\eta) = \begin{pmatrix} O_{(\delta-1)\times\tau} & A(\eta)_{12} \\ 0 & A(\eta)_{22} \end{pmatrix} \tag{3.5}$$

where $A(\eta)_{12}$ and $A(\eta)_{22}$ are matrices of sizes $(\delta-1)\times(\delta-\tau)$ and $1\times(\delta-\tau)$, whose elements are given by

- *For the matrix $A(\eta)_{12}$, $a(\eta)_{ij} = a(\eta-1)_{i+1,j}$, for $i = 1,\dots,\delta-1$ and $j = \tau+1\dots,\delta$.*

- *For the matrix $A(\eta)_{22}$,*

$$a(\eta)_{\delta,j} = p_{\delta-\tau-1}a(\eta-1)_{\tau+1,j} + \cdots + p_0 a(\eta-1)_{\delta,j} \quad \textit{for } j = \tau+1,\dots,\delta$$

Proof. We can consider that the η-th power of A can be expressed in matrix blocks as follows:

$$A^\eta = \begin{pmatrix} A(\eta)_{11} & A(\eta)_{12} \\ A(\eta)_{21} & A(\eta)_{22} \end{pmatrix},$$

where $A(\eta)_{11}$, $A(\eta)_{12}$, $A(\eta)_{21}$ and $A(\eta)_{22}$ are matrices of sizes $(\delta-\eta)\times\eta$, $(\delta-\eta)\times(\delta-\eta)$, $\eta\times\eta$, and $\eta\times(\delta-\eta)$, respectively. We will make the proof using the induction method on the power η of A.

By computation, we get that

$$A^2 = \begin{pmatrix} O_{(\delta-2)\times 2} & I_{\delta-2} \\ A(2)_{21} & A(2)_{22} \end{pmatrix}$$

where the matrix $A(2)_{21}$ is of size 2×2 such that

- If $\tau = 1$, then
$$A(2)_{21} = \begin{pmatrix} 0 & a(1)_{\delta,2} \\ 0 & p_0 a(1)_{\delta,2} \end{pmatrix}$$

- If $\tau \geq 2$, then $A(2)_{21} = O_{2\times 2}$.

On the other hand, the matrix $A(2)_{22}$ is a matrix of size $2\times(\delta-2)$ given by

- If $\tau = 1$, then

$$A^2 = \begin{pmatrix} a(1)_{\delta,3} & a(1)_{\delta,4} & \cdots & a(1)_{\delta,\delta-1} & a(1)_{\delta,\delta} \\ p_{\delta-\tau-1} + p_0 a(1)_{\delta,3} & p_{\delta-\tau-2} + p_0 a(1)_{\delta,4} & \cdots & p_2 + p_0 a(1)_{\delta,\delta-1} & p_1 + p_0 a(1)_{\delta,\delta} \end{pmatrix}$$

- If $\tau \geq 1$, then

$$A^2 = \begin{pmatrix} 0 & \cdots & 0 & a(1)_{\delta,\tau+1} & a(1)_{\delta,\tau+2} & \cdots & a(1)_{\delta,\delta-1} & a(1)_{\delta,\delta} \\ 0 & \cdots & 0 & p_0 a(1)_{\delta,\tau+1} & p_{\delta-\tau-1} + p_0 a(1)_{\delta,\tau+2} & \cdots & p_2 + p_0 a(1)_{\delta,\delta-1} & p_1 + p_0 a(1)_{\delta,\delta} \end{pmatrix}$$

Now, assume that $A^\eta = (a(\eta)_{ij})_{\substack{i=1,\dots,\delta \\ j=1,\dots,\delta}}$ is given by the statement of the lemma.

If $\eta < \delta$, then,

$$A^{\eta+1} = AA^\eta = A\begin{pmatrix} O_{(\delta-\eta)\times\eta} & I_{\delta-\eta} \\ A(\eta)_{21} & A(\eta)_{22} \end{pmatrix} = \begin{pmatrix} O_{(\delta-\eta-1)\times(\eta+1)} & I_{\delta-\eta-1} \\ A(\eta+1)_{21} & A(\eta+1)_{22} \end{pmatrix}$$

where the matrices $A(\eta+1)_{21}$ and $A(\eta+1)_{22}$ are of sizes $(\eta+1)\times(\eta+1)$ and $(\eta+1)\times(\delta-\eta-1)$, respectively, whose elements are given by

- For the matrix $A(\eta+1)_{21}$:
  - If $\eta+1 \leq \tau$, then $a(\eta+1)_{ij} = 0$ for all $i = \delta-\eta,\dots,\delta$ and $j = 1,\dots,\eta+1$,

- If $\eta + 1 > \tau$, then

$$a(\eta+1)_{ij} = \begin{cases} 0 & \text{if} \begin{cases} i = \delta - \eta, \dots, \delta \\ j = 1, \dots, \tau \end{cases} \\ a(\eta)_{i+1,j} & \text{if} \begin{cases} i = \delta - \eta, \dots, \delta - 1 \\ j = \tau + 1, \dots, \eta + 1 \end{cases} \\ p_{\eta-1} a(\eta)_{\delta-\eta+1,j} + \cdots + p_0 a(\eta)_{\delta,j} & \text{if} \begin{cases} i = \delta \\ j = \tau + 1, \dots, \eta + 1 \end{cases} \end{cases}$$

- For the matrix $A(\eta+1)_{22}$:
  - If $\eta + 1 \leq \tau$, then

$$a(\eta)_{ij} = \begin{cases} 0 & \text{if} \begin{cases} i = \delta - \eta, \dots, \delta \\ j = \eta + 2, \dots, \tau \end{cases} \\ a(\eta)_{i+1,j} & \text{if} \begin{cases} i = \delta - \eta, \dots, \delta - 1 \\ j = \tau + 1, \dots, \delta \end{cases} \\ p_{\eta-1} a(\eta)_{\delta-\eta+1,j} + \cdots + p_0 a(\eta)_{\delta,j} & \text{if} \begin{cases} i = \delta \\ j = \eta + 2, \dots, \tau + \eta + 1 \end{cases} \\ p_{\delta-j+\eta-1} + p_{\eta-1} a(\eta)_{\delta-\eta+1,j} + \cdots + p_0 a(\eta)_{\delta,j} & \text{if} \begin{cases} i = \delta \\ j = \tau + \eta + 1, \dots, \delta \end{cases} \end{cases}$$

  - If $\eta + 1 > \tau$, then

$$a(\eta+1)_{ij} = \begin{cases} a(\eta)_{i+1,j} & \text{if} \begin{cases} i = \delta - \eta, \dots, \delta - 1 \\ j = \eta + 2, \dots, \delta \end{cases} \\ p_{\eta-1} a(\eta)_{\delta-\eta+1,j} + p_{\eta-2} a(\eta)_{\delta-\eta,j} + \cdots + p_0 a(\eta)_{\delta,j} & \text{if} \begin{cases} i = \delta \\ j = \eta + 2, \dots, \delta \end{cases} \end{cases}$$

Assume now that $\eta \geq \delta$ and that matrix A^η is given by relation (3.5). Observe that the matrix A contains the identity matrix of size $(\delta-1) \times (\delta-1)$ (see (3.3)) and the last row of it is

$$\begin{pmatrix} 0 & 0 & \cdots & p_{\delta-\tau-1} & \cdots & p_1 & p_0 \end{pmatrix}.$$

In particular, $A = \begin{pmatrix} O_{(\delta-1)\times 1} & I_{\delta-1} \\ 0 & A(1)_{22} \end{pmatrix}$. For the above reasoning, we can consider that A^η has the following structure

$$A^\eta = \begin{pmatrix} O_{1\times\tau} & A(\eta)_{12} \\ O_{(\delta-1)\times\tau} & A(\eta)_{22} \end{pmatrix}.$$

Consequently,

$$A^{\eta+1} = \begin{pmatrix} O_{(\delta-1)\times 1} & I_{\delta-1} \\ 0 & A(1)_{22} \end{pmatrix} \begin{pmatrix} O_{1\times\tau} & A(\eta)_{12} \\ O_{(\delta-1)\times\tau} & A(\eta)_{22} \end{pmatrix} = \begin{pmatrix} O_{(\delta-1)\times\tau} & A(\eta)_{22} \\ O_{1\times\tau} & A(1)_{22} A(\eta)_{22} \end{pmatrix} = \begin{pmatrix} O_{(\delta-1)\times\tau} & A(\eta+1)_{12} \\ O_{1\times\tau} & A(\eta+1)_{22} \end{pmatrix}.$$

where the matrices $A(\eta+1)_{12}$ and $A(\eta+1)_{22}$ are of sizes $(\delta-1) \times (\delta-\tau)$ and $1 \times (\delta-\tau)$, respectively, satisfying

- $A(\eta+1)_{12} = A(\eta)_{22}$
- $A(\eta+1)_{22} = (a(\eta+1)_{\delta,j})_{j=\tau+1,\dots,\delta}$ with

$$a(\eta+1)_{\delta,j} = p_{\delta-\tau-1}a(\eta)_{\tau+1,j} + p_{\delta-\tau-2}a(\eta)_{\tau+2,j} + \cdots + p_0 a(\eta)_{\delta,j} \qquad \text{for } j = \tau+1,\dots,\delta.$$

So we have proof by the induction method that the η-th power of A is given by the statement of the lemma. □

Now, let $\mathcal{V}_\gamma$ be a finite-weight codeword generated by the input vector $(u_0, u_1, \dots, u_s, u_{s+1} \dots, u_\gamma)$ of weight two with u_0,$u_s \neq 0$. From relation (3.4) we know that $A^s Bu_0 + Bu_s \in \ker(A^{\gamma-s})$. Next result give us the dimension of the kernel of the the η-th power of A. Such a kernel we will need later on.

Lemma 3.4. *Let (A, B, C, D) be the the controllable canonical realization of an $(n, 1, \delta)$ convolutional code C, that is, A and B are matrices as in (3.3). Assume that A is singular and let τ be the integer such that $p_{\delta-j} = 0$ for $j = 1, 2, \dots, \tau$ and $p_{\delta-\tau-1} \neq 0$. Denote by $a_j^{(\eta)}$ the j-th column of the matrix A^η, for each $\eta \geq 1$, that is,*

$$A^\eta = \begin{pmatrix} a_1^{(\eta)} & a_2^{(\eta)} & \cdots & a_{\tau-1}^{(\eta)} & a_\tau^{(\eta)} & \cdots & a_\delta^{(\eta)} \end{pmatrix}.$$

Then, the following holds:

a) If $1 \leq \eta \leq \tau - 1$, then $a_j^{(\eta)} = 0$ for $j = 1, 2, \dots, \eta$ and the column vectors $\{a_{\eta+1}^{(\eta)}, \dots, a_\tau^{(\eta)}, \dots, a_\delta^{(\eta)}\}$ are linearly independent. In particular, dim$(\ker A^\eta) = \eta$.

b) If $\tau \leq \eta \leq \delta - 1$, then $a_j^{(\eta)} = 0$ for $j = 1, 2, \dots, \tau$ and the column vectors $\{a_{\tau+1}^{(\eta)}, \dots, a_\delta^{(\eta)}\}$ are linearly independent. In particular, dim$(\ker A^\eta) = \tau$.

c) If $\eta \geq \delta$, then $a_j^{(\eta)} = 0$ for $j = 1, 2, \dots, \tau$ and dim$(\ker A^\eta) \geq \tau$.

Proof. Taking into account Lemma 3.3, which give us the structure of A^η, we obtain that

a) If $\eta = 1, 2, \dots, \tau - 1$, then the first η columns of A^η are zero and the column vectors $\{a_{\eta+1}^{(\eta)}, \dots, a_\tau^{(\eta)}, \dots, a_\delta^{(\eta)}\}$ are linearly independent, since they contains the identity matrix of size $\delta - \eta$. Consequently, $\dim(\ker A^\eta) = \eta$.

b) If $\tau \leq \eta \leq \delta$, then the first τ columns of A^η are zero and the column vectors $\{a_{\tau+1}^{(\eta)}, \dots, a_\delta^{(\eta)}\}$ are linearly independent, since they contains the identity matrix of size $\delta - \tau$. So $\dim(\ker A^\eta) = \tau$.

c) If $\eta \geq \delta$, then the first τ columns of A^η are zero but we cannot know which columns of the $\delta - \tau$ last columns of A^η are linearly independent. In particular, $\dim(\ker A^\eta) \geq \tau$.

□

Remark 3.2. Observe that if $\eta \geq \tau$, the dimension, and in particular, a basis of the subspace $\ker(A^\eta)$, is independent of η.

Remark 3.3. Lemma 3.3 also shows the relation of recurrence existing between the last column of the different powers of the matrix A. Indeed, if $C(A, B, C, D)$ is an $(n, 1, \delta)$-code with the conditions of Lemma 3.3, and we write $a_\delta^{(\eta)} = \begin{pmatrix} a(\eta)_{1,\delta} \\ a(\eta)_{2,\delta} \\ \vdots \\ a(\eta)_{\delta-1,\delta} \\ a(\eta)_{\delta,\delta} \end{pmatrix}$ for the last column of A^η, $\eta = 2, 3, \dots$.Then:

$$a(\eta)_{i,\delta} = a(\eta-1)_{i+1,\delta} \quad \text{for } i = 1, 2, \dots, \delta - 1$$

and

$$a(\eta)_{\delta,\delta} = p_{\delta-1}a(\eta-1)_{1,\delta} + p_{\delta-2}a(\eta-1)_{2,\delta} + \cdots + p_1a(\eta-1)_{\delta-1,\delta} + p_0a(\eta-1)_{\delta,\delta}$$

Next we investigate how are the codewords that need to be considered to compute $\mathrm{z}_{\min}(C)$. We shall analyse several sets of finite-weight codewords $\mathcal{V}_\gamma$ sorted by their length γ in order to restrict the set of possible codewords that we need to considered to find the minimum of the weight of its parity vectors that yield $\mathrm{z}_{\min}(C)$. This, of course, will optimize the computations required to compute the exact value of $\mathrm{z}_{\min}(C)$.

Theorem 3.2. *Let $C(A, B, C, D)$ be an $(n, 1, \delta)$-code with (A, B) in canonical controllable form and A singular. Let τ be the integer as in Lemma 3.3. Let $\mathcal{V}_\gamma$ be the set of finite-weight codewords of C generated by an information vector $(u_0, u_1, \ldots, u_s, u_{s+1}, \ldots, u_\gamma)$ with $u_0, u_s \neq 0$ and $u_i = 0$ for $i \notin \{0, s\}$. Then, the lowest weight of the parity vectors of $\mathcal{V}_\gamma$ with $s + \tau \leq \gamma \leq s + \delta - 1$ is achieved for $s \leq q^\delta - (q^\tau(q-1))$.*

Proof. Let $\mathcal{V}_\gamma$ be a finite-weight codeword of C generated by an information vector $(u_0, u_1, \ldots, u_s, \ldots, u_\gamma)$ of weight two with u_0,$u_s \neq 0$. Then,

$$\begin{pmatrix} A^\gamma B & A^{\gamma-1}B & \cdots & A^{\gamma-s}B & \cdots & AB & B \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_s \\ \vdots \\ u_{\gamma-1} \\ u_\gamma \end{pmatrix} = A^{\gamma-s}\left(A^sBu_0 + Bu_s\right) = 0,$$

so $\left(A^sBu_0 + Bu_s\right) \in \ker A^{\gamma-s}$. It follows from Remark 3.2 that $\ker A^{\gamma-s}$ is the same subspace for any γ and s, provided $\tau \leq \gamma - s \leq \delta - 1$. As we consider the case in which $s + \tau \leq \gamma \leq s + \delta - 1$ it follows from statement b) of Lemma 3.4 that $\dim(\ker A^{\gamma-s}) = \tau$ and a basis for $\ker A^{\gamma-s} \subseteq \mathbb{F}^{\delta\times 1}$ is given by the column vectors:

$$\mathcal{B}_{\ker A^{\gamma-s}} = \{e_1, e_2, \ldots, e_\tau\}$$

where e_i denotes the i-th vector of the canonical basis of $\mathbb{F}^{\delta\times 1}$, for $i = 1, 2, \ldots, \tau$. Therefore, one has that $A^sBu_0 + Bu_{\hat{s}}$ must be of the form $(d_1, d_2, \ldots, d_\tau, 0, \ldots, 0)^T$ or, equivalently (observe the structure of matrix B given by (3.3)),

$$A^sB = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_\tau \\ 0 \\ \vdots \\ 0 \\ d_\delta \end{pmatrix} \quad \text{where } d_\delta \neq 0 \text{ as we require } u_s \neq 0. \tag{3.6}$$

Hence, s is in fact the smallest integer such that the last column of A^s is a vector like

$$(\overbrace{*,*,\ldots,*}^{\text{any } \tau \text{ elements}},0,\ldots,0,\overbrace{\quad * \quad}^{\text{a nonzero element}})^T.$$

Remark 3.3 provides the structure of the elements of the last column of A^s, that it can be seen as a feedback polynomial of a Linear Feedback Shift Register (LFSR). The maximum cycle of a LFSR of length δ is q^δ if the associated polynomial is primitive.

The number of states of the form (3.6) is $q^{\dim(\ker A^{\gamma-s})} = q^\tau$ times the $(q-1)$ possible nonzero elements for the last row of A^sB. This leads to the following upper-bound on s:

$$s \leq q^\delta - (q^\tau(q-1)),$$

which concludes the proof. □

In the following result we study the set of codewords with length $\gamma + 1$ such that $\gamma < s + \tau$.

Theorem 3.3. *Let $C(A, B, C, D)$ be an $(n, 1, \delta)$-code with (A, B) in canonical controllable form and A singular. Let τ be the integer as in Lemma 3.3. Let $\mathcal{V}_\gamma$ be the set of finite-weight codewords of C generated by an information vector $(u_0, u_1, \ldots, u_s, u_{s+1}, \ldots, u_\gamma)$ with $u_0, u_s \neq 0$ and $u_i = 0$ for $i \notin \{0, s\}$. Then, the lowest weight of the parity vectors of $\mathcal{V}_\gamma$ with $\gamma < s+\tau$, is achieved for $s \leq q^\delta - (q^{(\gamma-s)}(q-1))$.*

Proof. The proof follows the same idea used in the proof of Theorem 3.2. Note that by Lemma 3.1 we have that $\gamma \geq \delta$. Also it holds from Lemma 3.4 that $\dim(\ker A^{\gamma-s}) = \gamma - s < \tau$. Hence, for each value of γ and s such that $\gamma - s < \tau$ we have that s is the smallest integer such that the last column of A^s is a vector of the form

$$(\overbrace{*,*,\ldots,*}^{\text{any } \gamma - s \text{ elements}},0,\ldots,0,\overbrace{\quad * \quad}^{\text{a nonzero element}})^T. \tag{3.7}$$

As there are q^δ possible states and $q^{(\gamma-s)}(q-1)$ different states are of the form (3.7), the maximum value of s such that $A^sBu_0 - Bu_s$ is not in the kernel of $A^{\gamma-s}$ is $q^\delta - (q^{(\gamma-s)}(q-1))$ which yields the result. □

4. Optimal upper-bound on $\mathrm{z}_{\min}$ for a class of $(n, 1, \delta)$ recursive systematic convolutional codes

In this section we present a concrete construction of a class of convolutional codes with $\delta \geq 2$ for which we can compute the minimum effective index and the exact value of $\mathrm{z}_{\min}$ up to a difference of one value. Furthermore, we can show that such upper-bound is optimal and we do that by presenting a particular example that reaches the provided upper-bound. To this end we need a class of matrices that have been very useful for the construction of convolutional codes with large Hamming distance, namely, the so-called superregular matrices.

Definition 4.1 (Page 1314 of [31])**.** *Let A be an $n \times \ell$ matrix over a finite field $\mathbb{F}$. We say that A is a* superregular *matrix if every square submatrix of A is nonsingular.*

The following Lemma is an immediate consequence of Definition 4.1 and it gives a lower bound on the weight of a linear combination of columns of a superregular matrix.

Lemma 4.1 (Lemma 3 of [10])**.** *Let A be a superregular matrix over a finite field $\mathbb{F}$ of size $n \times \ell$, with $n \geq \ell$. It follows that any nontrivial linear combination of m different columns of A cannot have more than $m - 1$ entries equal to zero.*

In the following result we present a particular construction based on a input-state-output representation where the pair (A, B) is in canonical controllable form with A singular, C a superregular matrix and D a column of C. We establish that the lowest weight of the parity vectors of $\mathcal{V}_\gamma$ is achieved in fact by the ones generated by weight-2 input sequences $(u_0, u_1, \ldots, u_\gamma)$ with $u_0 \neq 0$ and $u_1 \neq 0$. Furthermore, we establish a lower and an upper bound of $\mathrm{z}_{\min}(\mathcal{C})$ for these case.

Theorem 4.1. *Let δ and n be any positive integers with $\delta \geq 2$, $n \geq \delta + 1$ and $q \geq n + \delta$. Let $\mathcal{C}(A, B, C, D)$ be an $(n, 1, \delta)$-code described by the matrices*

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \qquad C = \begin{pmatrix} c_{11} & \cdots & c_{1,\delta} \\ c_{21} & \cdots & c_{2,\delta} \\ \vdots & & \\ c_{(n-1),1} & \cdots & c_{(n-1),\delta} \end{pmatrix} \qquad D = \begin{pmatrix} c_{1,\delta-1} \\ c_{2,\delta-1} \\ \vdots \\ c_{(n-1),\delta-1} \end{pmatrix} \tag{4.1}$$

of sizes $\delta \times \delta$, $\delta \times 1$, $(n-1) \times \delta$ and $(n-1) \times 1$ respectively and where C is a superregular matrix. Then we have that

$$(n-1)(\delta+1) - 1 \leq \mathrm{z}_{\min}(\mathcal{C}) \leq (n-1)(\delta+1). \tag{4.2}$$

Moreover, the minimum effective index $\hat{s}$ achieves its minimum possible value, i.e., $\hat{s} = 1$ and so the value of $\mathrm{z}_{\min}(\mathcal{C})$ is reached in finite-weight codewords of minimum length $\gamma = \delta$ and it is calculate as

$$\mathrm{z}_{\min}(\mathcal{C}) = \mathrm{wt}(D) + \mathrm{wt}(CB - D) + \sum_{j=1}^{\delta-1} \mathrm{wt}(CA^{j}B - CA^{j-1}B). \tag{4.3}$$

Proof. Taking into account the structure of the matrices A and B of (4.1) and Lemma 3.3, the finite-weight codeword of minimal length generated by input of weight two is $\mathcal{V}_\delta$. Furthermore, in this case we have that $u_1 = -u_0$ and $u_2 = u_3 = \cdots = u_\delta = 0$. Then, the parity check vectors of $\mathcal{V}_\delta$ are of the form:

$$\begin{array}{rcl} \vec{y}_0 & = & Du_0 \\ \vec{y}_1 & = & (CB - D)u_0 \\ \vec{y}_2 & = & (CAB - CB)u_0 \\ \vec{y}_3 & = & (CA^2B - CAB)u_0 \\ \vdots & = & \vdots \\ \vec{y}_\delta & = & (CA^{\delta-1}B - CA^{\delta-2}B)u_0 \end{array} \tag{4.4}$$

where

$$\vec{y}_1 = (CB - D)u_0 = \begin{pmatrix} c_{1,\delta} - c_{1,\delta-1} \\ c_{2,\delta} - c_{2,\delta-1} \\ \vdots \\ c_{(n-1),\delta} - c_{(n-1),\delta-1} \end{pmatrix} \qquad \text{and} \qquad \vec{y}_j = (CA^{j-1}B - CA^{j-2}B)u_0 = \begin{pmatrix} c_{1,\delta-j+1} \\ c_{2,\delta-j+1} \\ \vdots \\ c_{n-1,\delta-j+1} \end{pmatrix},$$

for $j = 2, 3, \ldots, \delta$. Furthermore, $n - 2 \leq \mathrm{wt}(\vec{y}_1) \leq n - 1$ since C is a superregular matrix and by Lemma 4.1 any nontrivial linear combination of two different columns of C cannot have more than 1 entry equal to zero. Similarly, we can ensure that $\mathrm{wt}(\vec{y}_j) = n - 1$, since C is superregular. So we obtain the following bounds on the weigth of the parity vectors $\vec{y}_j$ of $\mathcal{V}_\delta$.

$$(n-1)(\delta+1)-1 \leq \sum_{j=0}^{\delta} \mathrm{wt}(\vec{y}_j) = \mathrm{wt}(D) + \mathrm{wt}(CB-D) + \sum_{j=1}^{\delta-1} \mathrm{wt}(CA^jB - CA^{j-1}B) \leq (n-1)(\delta+1) \tag{4.5}$$

Our aim now is to proof that in fact, $z_{\min}(C)$ is obtained from the minimum of the parity vectors of all finite-weight codewords of lenght $\delta+1$. In order to do this, consider now a finite-weight codeword $\mathcal{V}_\gamma$ generated by a input vector $(\bar{u}_0, \bar{u}_1, \dots, \bar{u}_\gamma)$ of weight two with $\gamma > \delta$. Then, there exists a time instant $r \geq 1$ such that $\bar{u}_0 \neq 0$, $\bar{u}_r \neq 0$ and $\bar{u}_j = 0$ for $j \neq 0, r$. From Lemma 3.2, we know that if $r = 1$, then we can ensure that the parity vector $(\vec{\bar{y}}_0, \vec{\bar{y}}_1, \dots, \vec{\bar{y}}_\gamma)$ of $\mathcal{V}_\gamma$ have weight greater or equal to the parity vector $(\vec{y}_0, \vec{y}_1, \dots, \vec{y}_\delta)$ of any finite-weight codeword $\mathcal{V}_\delta$ of lenght $\delta+1$. Furthermore, if $r > 1$, then from the structure of matrices A, B, C, D, Lemma 3.3 and taking into account that C is superregular, then we obtain the following bounds on the weight of the parity vector $(\vec{\bar{y}}_0, \vec{\bar{y}}_1, \dots, \vec{\bar{y}}_\gamma)$

$$(\delta+r)n - \delta r \leq \sum_{j=0}^{\gamma} \mathrm{wt}(\vec{\bar{y}}_j) \leq (n-1)(\delta+r). \tag{4.6}$$

Taking into account relations (4.5) and (4.6) and the fact that $\delta < n$, we obtain

$$\sum_{j=0}^{\delta} \mathrm{wt}(\vec{y}_j) \leq (n-1)(\delta+1) \leq (\delta+r)n - \delta r \leq \sum_{j=0}^{\gamma} \mathrm{wt}(\vec{\bar{y}}_j)$$

where $(\vec{y}_0, \vec{y}_1, \dots, \vec{y}_\delta)$ and $(\vec{\bar{y}}_0, \vec{\bar{y}}_1, \dots, \vec{\bar{y}}_\gamma)$ are the parity vectors of any codewords $\mathcal{V}_\delta$ and $\mathcal{V}\gamma$ with $\gamma > \delta$, respectively. So we can conclude that $z_{\min}(C)$ is obtained by the minimum of the weight of the parity vectors of all the finite-weight codewords $\mathcal{V}_\delta$ generated by input vectors with length $\delta+1$. Furthermore, from relation (4.4), we deduce that in fact

$$z_{\min}(C) = \mathrm{wt}(D) + \mathrm{wt}(CB-D) + \sum_{j=1}^{\delta-1} \mathrm{wt}(CA^jB - CA^{j-1}B).$$

□

In the following example, we show a convolutional code whose $z_{\min}(C)$ reaches the upper bound of the relation (4.2).

Example 4.1. Let $\mathbb{F}$ be the Galois field of 7 elements and let $C(A, B, C, D)$ be an $(4,1,2)$-code described by the matrices

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

It is easy to see that the the $(4,1,2)$-code described by the above matrices A, B, C and D satisfy the hypothesis of Theorem 4.2. Then we know that the

$$\begin{aligned} z_{\min}(C) = {} & \mathrm{wt}(D) + \mathrm{wt}(CB-D) + \mathrm{wt}(CAB-CB) \\ = {} & \mathrm{wt}(\begin{pmatrix} 4 \\ 5 \\ 3 \end{pmatrix}) + \mathrm{wt}(\begin{pmatrix} 1 \\ 4 \\ 1 \end{pmatrix}) + \mathrm{wt}(\begin{pmatrix} 4 \\ 5 \\ 2 \end{pmatrix}) = 9 \end{aligned}$$

That is in this case the code attains the maximal value.

In the example before the superregular matrix C is a Cauchy matrix and it is a small example. If we need to construct a turbo code with a determinate $\mathrm{z}_{\min}(C)$ we must to consider a bigger parameters and consequently a bigger field. Work with a big finite field increases computational costs. In order to minimize the size of the field we introduce a similar construction for a singular A similar to Theorem 4.1 in which we make use of the so-called extended Cauchy matrices (see [31]).

Theorem 4.2. *Let $\mathbb{F}$ be the Galois field of q elements. Let δ and n be any positive integers with $\delta \geq 2$, $n \geq \delta + 1$ and $q \geq n + \delta - 1$. Let $C(A, B, C, D)$ be an $(n, 1, \delta)$-code described by the matrices*

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \quad C = \begin{pmatrix} c_{11} & \cdots & c_{1\delta} \\ c_{21} & \cdots & c_{2\delta} \\ \vdots & & \\ c_{(n-1)1} & \cdots & c_{(n-1)\delta} \end{pmatrix} \quad D = \begin{pmatrix} c_{1\delta-1} \\ c_{2\delta-1} \\ \vdots \\ c_{(n-1)\delta-1} \end{pmatrix}$$

of sizes $\delta \times \delta$, $\delta \times 1$, $(n-1) \times \delta$ and $(n-1) \times 1$ respectively and where C is a extended Cauchy matrix with the first column $\vec{c}_1 = (c_{11}, c_{21}, ldots, c_{(n-1),1})$ of ones. Then we have that

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

Moreover, the value of $\mathrm{z}_{\min}(C)$ is reached in a finite code word of minimum length $\gamma = \delta$ and it is calculate as

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

Proof. The proof is analogous of Theorem 4.1. □

Example 4.2. Let $\mathbb{F}$ be the Galois field of 5 elements and let $C(A, B, C, D)$ be an $(4, 1, 2)$-code described by the matrices

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

It is easy to see that the the $(4, 1, 2)$-code described by the above matrices A, B, C and D satisfy the hypothesis of Theorem 4.2. Then we know that the

$$\begin{aligned} \mathrm{z}_{\min}(C) = {} & \mathrm{wt}(D) + \mathrm{wt}(CB - D) + \mathrm{wt}(CAB - CB) \\ = {} & \mathrm{wt}(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}) + \mathrm{wt}(\begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}) + \mathrm{wt}(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}) = 9 \end{aligned}$$

That is in this case also the code attains the maximal value.

5. Conclusions and future work

In this work we study the lowest Hamming weight of the parity vectors generated by information sequences of weight two, that is, $\mathrm{z}_{\min}$, of a $1/n$ convolutional code $C(A, B, C, D)$ represented in terms of the input-state-output representation. We analyze how one can reduce the computations to derive this value which is, in general, difficult to compute as it is the minimum over the large set of codeword with inputs of weight two. In this work we reduce this set by studying the structure of the codewords produced by the input-state-output system. This will lead to reduce the compute search to obtain the exact value of $\mathrm{z}_{\min}(C)$. We also presented a class of convolutional codes for which we know the form of the codewords that lead to the computation of $\mathrm{z}_{\min}$ and therefore allow us to determine its exact value up to a difference of one unit.

It is left as an open problem to provide a specific lower and upper bounds on $\mathrm{z}_{\min}(C)$, and consequently, lower and upper bounds on the effective free distance over general finite fields. Also it would be interesting to show that this hypothetical upper bound it tight by presenting a concrete construction of a Turbo Code whose effective free distance reaches this bound. Also interesting it would be to derive different constructions to the one given in Section 4 having better bounds.

Acknowledgments

The authors would like to thank the anonymous reviewers for the their comments. The research of the second author was supported by Spanish I+D+i project PID2019-108668GB-I00 of MCIN/AEI/10.13039/501100011033.

Conflict of interest

The authors declare that there is no conflict of interests in this paper.

References

1. S. Benedetto, G. Montorsi, Design of parallel concatenated convolutional codes, *IEEE T. Commun.*, **44** (1996), 591–600. https://doi.org/10.1109/26.494303
2. C. Berrou, A. Glavieux, P. Thitimajshima, Near Shannon limit error-correcting coding and decoding: Turbo Codes (1), *Proc. of IEEE ICC 93– IEEE International Conference on Communications*, **2** (1993), 1064–1070. https://doi.org/10.1109/ICC.1993.397441
3. R. Bru, R. Cantó, B. Ricarte, V. Rumchev, A Basic Canonical Form of Discrete-time Compartmental Systems, *Int. J. Contemp. Math. Sciences*, **2** (2007), 261–273. http://dx.doi.org/10.12988/ijcms.2007.07020
4. P. Campillo, A. Devesa, V. Herranz, C. Perea, Modelization of turbo encoder from linear system point of view, *Proceedings of the 10th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2010)*, (2010), 314–317.
5. B. Cantó, C. Coll, E. Sánchez, On positive behaviour of periodic control systems, *Appl. Math. Comput.*, **161** (2005), 779–786. https://doi.org/10.1016/j.amc.2003.03.001
6. M. V. Carriegos, N. De Castro-García, Partitions of elements in a monoid and its applications to systems theory, *Linear Algebra Appl.*, **491** (2016), 161–170. https://doi.org/10.1016/j.laa.2015.05.034
7. N. De Castro-García, M. V. Carriegos, A. L. Muñoz Castañeda, A characterization of von Neumann rings in terms of linear systems, *Linear Algebra Appl.*, **494** (2016), 236–244. https://doi.org/10.1016/j.laa.2016.01.019

8. J.-J. Climent, V. Herranz, C. Perea, A first approximation of concatenated convolutional codes from linear systems theory viewpoint, *Linear Algebra Appl.*, **425** (2007) , 673–699. https://doi.org/10.1016/j.laa.2007.03.017
9. J.-J. Climent, V. Herranz, C. Perea, Linear system modelization of concatenated block and convolutional codes, *Linear Algebra Appl.*, **429** (2008), 1191–1212. https://doi.org/10.1016/j.laa.2007.09.006
10. J.-J. Climent, D. Napp, C. Perea, R. Pinto, Maximum distance separable 2D convolutional codes, *IEEE T. Inform. Theory*, **62** (2016), 669–680. https://doi.org/10.1109/TIT.2015.2509075
11. J. J. Climent, V. Herranz, C. Perea, Parallel concatenated convolutional codes from linear systems theory viewpoint, *Systems and Control Letters*, **96** (2016), 15–22. https://doi.org/10.1016/j.sysconle.2016.06.016
12. D. Divsalar, F. Pollara, Low Rate Turbo Codes for Deep Space Communications, *Proceedings of 1995 IEEE Int. Symp. Info. Theory*, (1995). https://doi.org/10.1109/ISIT.1995.531137
13. D. Divsalar, F. Pollara, Multiple turbo codes for deep-space communications, *The Telecommunications and Data Acquisition Progress Report*, (1995).
14. D. Divsalar, R. J. McEliece, The effective free distance of turbo codes, *Electron. Lett.*, **32** (1996), 445–446. https://doi.org/10.1049/el:19960321
15. D. Divsalar, R. J. McEliece, 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. M. I. García-Planas, E. M. Soudit, L. E. Um, Convolutional codes under linear systems point of view. Analysis of output-controllability, *WSEAS Press. World Scientific and Engineering Academy and Society*, **11** (2012), 2224–2880.
17. M. I. García-Planas, N. deCastro, Concatenated linear systems over rings and their application to construction of concatenated families of convolutional codes, *Linear algebra appl.*, **542** (2017), 624–647. https://doi.org/10.1016/j.laa.2017.12.009
18. V. Herranz, D. Napp, C. Perea, Serial concatenation of a block code and a 2D convolutional code, *Multidim. syst. sign. p.*, **30** (2019), 1113–1127. https://doi.org/10.1007/s11045-018-0591-3
19. V. Herranz, D. Napp, C. Perea, $1/n$ Turbo Codes from linear system point of view, *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, **114** (2020). https://doi.org/10.1007/s13398-020-00850-2
20. S. Hong, R. Wu, On deep holes of generalized Reed-Solomon codes, *AIMS Mathematics*, **1** (2016), 96–101. https://doi.org/10.3934/Math.2016.2.96
21. J. Lieb, J. Rosenthal, Erasure decoding of convolutional codes using first order representations, *Math. Control Signal.*, **33** (2021), 499–513. https://doi.org/10.1007/s00498-021-00289-9
22. T. Kailath, *Linear Systems*, Prentice Hall information and system sciences series, Prentice-Hall, 1980.
23. J. L. Massey, M. K. Sain, Codes, automata, and continuous systems: explicit interconnections, *IEEE T. Automat. Contr.*, **12** (1967), 644–650. https://doi.org/10.1109/TAC.1967.1098736
24. R. J. McEliece, The algebraic theory of convolutional codes, *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. North-Holland: Elsevier (1998), 1065–1138.

25. A. L. M. Castañeda, J. M. Muñoz-Porras, F. J. Plaza-Martín, Rosenthal's Decoding Algorithm for Certain 1-Dimensional Convolutional Codes, *IEEE T. Inform. Theory*, **65** (2019), 7736–7741. https://doi.org/10.1109/TIT.2019.2921370

26. D. Napp, R. Pereira, R. Pinto, P. Rocha, Periodic state-space representations of periodic convolutional codes, *Cryptography and Communications*, **11** (2019), 585–595. https://doi.org/10.1007/s12095-018-0313-6

27. B. Ricarte, S. Romero-Vivó, An algebraic approach to the structural properties of positive state control systems, *Math. Method. Appl. Sci.*, **41** (2018), 2370–2378. https://doi.org/10.1002/mma.4351

28. J. Rosenthal, J. M. Schumacher, E. V. York, On behaviors and convolutional codes, *IEEE T. Inform. Theory*, **42** (1996), 1881–1891. https://doi.org/10.1109/18.556682

29. J. Rosenthal, E. V. York, BCH convolutional codes, *IEEE T. Inform. Theory*, **45** (1999), 1833–1844. https://doi.org/10.1109/18.782104

30. J. Rosenthal, 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. New York: Springer-Verlag, **123** (2001), 39–66. https://doi.org/10.1007/978-1-4613-0165-3_2

31. R. M. Roth, A. Lempel, On MDS codes via Cauchy matrices, *IEEE T. Inform. Theory*, **35** (1989), 1314–1319. https://doi.org/10.1109/18.45291

32. R. Smarandache, J. Rosenthal, Construction of Convolutional Codes using Methods from Linear Systems Theory, *Proc. of the 35-th Annual Allerton Conf. on Commun., Control, and Computing*, (1997), 953–960.

33. R. Smarandache, J. Rosenthal, A state space approach for constructing MDS rate $1/n$ convolutional codes, *Proc. of the 1998 IEEE Inform. Theory Workshop (ITW 1998)*, (1998), 116–117. https://doi.org/10.1109/ITW.1998.706461

34. X. F. Xu, Y. C. Xu, S. F. Hong, Some results on ordinary words of standard Reed-Solomon codes, *AIMS Mathematics*, **4** (2019), 1336–1347. https://doi.org/10.3934/math.2019.5.1336