A novel criterion for the construction of MDS convolutional codes of rate $1/n$

Zita Abreu[1,2], Julia Lieb[2], Raquel Pinto[1], Joachim Rosenthal[2]
University of Aveiro[1], University of Zurich[2]

Abstract

Maximum-distance separable (MDS) convolutional codes are characterized by the property that their free distance reaches the generalized Singleton bound. In this paper, a new criterion to construct MDS convolutional codes of rank 1 is presented. This criterion allows to relate the construction of MDS convolutional codes to the construction of reverse superregular Toeplitz matrices. Additionally, we present some construction examples for small code parameters over small finite fields.

1 Introduction

Communication systems that work with digitally represented data use error correction codes because all real communication channels are noisy. One type of error-correcting codes are convolutional codes. The distance of a convolutional code provides a means to assess its capability to protect data from errors. Codes with larger distance are better because they allow correcting more errors. One type of distance for convolutional codes is the free distance, which is considered for decoding when the codeword is fully received. Convolutional codes with maximal free distance are called Maximum Distance Separable Codes (MDS).
There are some known constructions of MDS convolutional codes. The first construction was obtained by Justesen in [Jus75] for codes of rate $1/n$ with restricted degrees. In [SR98] Smarandache and Rosenthal presented constructions of convolutional codes of rate $1/n$ and arbitrary degree δ. However, these constructions require a larger field size than the one obtained by Justesen. Later, Gluesing-Luerssen and Langfeld presented in [GLL06] a construction of convolutional codes of rate $1/n$ with the same field size as the one obtained by Justesen but also with a restriction on the degree of the code. Thereafter, Gluesing-Luerssen, Smarandache and Rosenthal [SGLR01] constructed MDS convolutional codes for arbitrary parameters (n, k, δ) but with a restriction on the size of the underlying finite field. Lieb and Pinto [LP20] presented a new way of constructing MDS convolutional codes of any degree and sufficiently low rate using superregular matrices.
In contrast to MDS block codes, there is no algebraic criterion to check whether a convolutional code is MDS. In [LP20] a criterion for MDS convolutional codes was presented, which however only works if the length n of the code is sufficiently large with respect to rank k and degree δ.
In this paper, a new method for constructing MDS convolutional codes of rank 1 will be presented. In particular, we will relate these codes to reverse superregular Toeplitz matrices. Additionally, the field size in code constructions is an is an important factor to be considered since it is straightly related to the computational efficiency of the encoding and decoding algorithms and the complexity of the decoding algorithms. Therefore, we intend to construct codes over fields of small size and in order to achieve this, we present some construction examples for small code parameters over small finite fields.

1.1 Preliminaries

A **convolutional code** $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[z]$-submodule of $\mathbb{F}_q^n[z]$ of rank k, where $\mathbb{F}_q[z]$ is the ring of polynomials with coefficients in the field $\mathbb{F}_q$. A matrix $G(z) \in \mathbb{F}_q[z]^{k\times n}$ whose rows constitute a basis of $\mathcal{C}$ is called a **generator matrix** for $\mathcal{C}$. It is a full row rank matrix such that:

$$\mathcal{C} = \operatorname{Im}_{\mathbb{F}_q[z]} G(z) = \{v(z) \in \mathbb{F}_q^n[z] : v(z) = u(z)G(z) \text{ with } u(z) \in \mathbb{F}_q^k[z]\}.$$

The maximum degree of the full-size minors of a generator matrix of $\mathcal{C}$ is called the **degree** δ of $\mathcal{C}$. A convolutional code of rate k/n and degree δ is also denoted as (n, k, δ) convolutional code.

The **free distance** of a convolutional code measures its capability of detecting and correcting errors introduced during information transmission through a noisy channel and it is defined by

$$d_{free}(\mathcal{C}) = \min\{wt(v(z))|v(z) \in \mathcal{C}, v(z) \neq 0\},$$

where $wt(v(z)) = \sum_{t=0}^{\deg(v(z))} wt(v_t)$ is the Hamming weight of $v(z) = \sum_{t=0}^{\deg(v(z))} v_t z^t \in \mathbb{F}_q^n[z]$ and the weight $wt(v)$ of $v \in \mathbb{F}_q^n$ is the number of nonzero components of v. In [RS99], the authors obtained an upper bound for the free distance of an (n, k, δ) convolutional code $\mathcal{C}$ given by

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

This bound is called **generalized Singleton bound**. An (n, k, δ) convolutional code with free distance equal to this bound is called **Maximum Distance Separable (MDS)** convolutional code. Note that an MDS $(n, 1, \delta)$ convolutional code has free distance $n(\delta + 1)$.

Besides the free distance, for convolutional codes one usually also considers its column distances. Even if in this paper, we focus only on obtaining an optimal free distance, we need the concept of column distances for the proof of our main theorem and thus, we will introduce it in the following.

Definition 1. *For a polynomial vector $v(z) = \sum_{j\in\mathbb{N}_0} v_j z^j \in \mathbb{F}_q^n[z]$, the **$j$-th truncation** of $v(z)$ is defined as*

$$v_{[0,j]}(z) = v_0 + v_1 z + \cdots + v_j z^j.$$

*For $j \in \mathbb{N}_0$, the **j-th column distance** of a convolutional code $\mathcal{C}$ is defined as*

$$d_j^c(\mathcal{C}) := \min\left\{wt(v_{[0,j]}(z)) \mid v(z) \in \mathcal{C} \text{ and } v_0 \neq \mathbf{0}\right\}.$$

Theorem 1. *[GLRS06] Let $\mathcal{C}$ be an (n, k, δ) convolutional code. Then, $d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1$.*

In order to present a criterion for how to check if the column distances reach their upper bound, we first need to introduce the following definition.

Definition 2. *For $r \in \mathbb{N}$, let $A \in \mathbb{F}_q^{r\times r}$ be a matrix with (i, j)-entry denoted by a_{ij}. Define $X = \{x_{ij} : i, j \in \{1, \ldots, r\}\}$ and let $\mathbb{F}_q[X]$ be the set of polynomials in the indeterminates x_{ij}. Then, define $\overline{A} \in \mathbb{F}_q[X]^{r\times r}$ as the matrix with (i, j)-entry equal to*

$$\overline{a}_{ij} = \begin{cases} 0 & \text{for } a_{ij} = 0 \\ x_{ij} & \text{for } a_{ij} \neq 0 \end{cases}$$

*The determinant of A is called **trivially zero** if the determinant of $\overline{A}$ is equal to the zero polynomial. Otherwise, this determinant is called **non trivially zero**.*

Theorem 2 ([GLRS06])**.** *Let $\mathcal{C}$ be a convolutional code with generator matrix $G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}_q[z]^{k\times n}$ with G_0 full rank and $0 \leq j \leq L := \lfloor \frac{\delta}{k} \rfloor + \lfloor \frac{\delta}{n-k} \rfloor$. The following statements are equivalent:*

(a) $d_j^c(\mathcal{C}) = (n-k)(j+1)+1$.

(b) Every full size minor of $G_j^c = \begin{pmatrix} G_0 & \cdots & G_j \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix}$ that is non trivially zero is nonzero.

The following lemmata will be needed to prove our main statement in the next section.

Lemma 1 ([GLRS06])**.** *Let $\mathcal{C}$ be an (n, k, δ) convolutional code with generator matrix $G(z)$ and G_0 full rank. If $d_j^c(\mathcal{C}) = (n-k)(j+1)+1$ for some $j \in \{1, \ldots, L\}$, then $d_i^c(\mathcal{C}) = (n-k)(i+1)+1$ for all $i \leq j$.*

Lemma 2. *Let $A \in \mathbb{F}_q^{r\times s}$ with $r \leq s$ be such that all its fullsize minors are nonzero. Then, each vector which is a linear combination of the r rows of A has at most $r-1$ zeros.*

In the next section, we will relate MDS convolutional codes with codes that have the property that the code itself as well as the so-called reverse code, as introduced in the next definition, reach the upper bound for their $(\delta-1)$-th column distance.

Definition 3 ([Hut08])**.** *Let $\mathcal{C}$ be an (n, k, δ) convolutional code with generator matrix $G(z)$, which has entries $g_{ij}(z)$. Set $\overline{g}_{ij}(z) := z^{\nu_i} g_{ij}(z^{-1})$ where ν_i is the i-th row degree of $G(z)$. Then, the code $\overline{\mathcal{C}}$ with generator matrix $\overline{G}(z)$, which has $\overline{g}_{ij}(z)$ as entries, is called the **reverse code** to $\mathcal{C}$.*

1.2 Criteria and Construction of MDS convolutional codes of rate $1/n$

In the following, we present our main theorem, which provides a criterion for the construction of MDS convolutional codes with $k = 1$.

Theorem 3. *Consider an $(n, 1, \delta)$ convolutional code $\mathcal{C}$ with $n = 2$ and $\delta \leq 4$ or $n \geq 3$ and δ arbitrary and generator matrix $G(z) = \sum_{i=0}^{\delta} G_i z^i$. Assume that all non trivially zero fullsize minors of the following matrices are nonzero:*

$$\begin{pmatrix} G_0 & \cdots & G_{\delta-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix} \text{ and } \begin{pmatrix} G_\delta & \cdots & G_1 \\ & \ddots & \vdots \\ 0 & & G_\delta \end{pmatrix} \text{ and } \begin{pmatrix} G_\ell & \cdots & G_\delta \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\delta-\ell} \end{pmatrix} \text{ for } 0 \leq \ell < min\left(\delta - 1, \frac{n(\delta+2)}{n+1}\right).$$

Then, $\mathcal{C}$ is an MDS convolutional code.

Proof. Let $u(z) \in \mathbb{F}_q[z]$ be a message with $\deg(u) = \ell$ and let $v(z) = u(z)G(z)$ be the corresponding codeword, i.e. $\deg(v) = \delta + \ell$. Then, one obtains $(v_0\ v_1\ \cdots\ v_{\delta+\ell}) = (u_0\ v_1\ \cdots\ v_\ell)\mathcal{G}$, where

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_\delta & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & G_0 & \cdots & G_\delta \end{pmatrix} \qquad \text{for} \quad \ell \geq \delta$$

$$\mathcal{G} = \begin{pmatrix} G_0 & \cdots & G_\ell & \cdots & G_\delta & & 0 \\ & \ddots & \vdots & & \vdots & \ddots & \\ 0 & & G_0 & \cdots & G_{\ell-\delta} & \cdots & G_\delta \end{pmatrix} \qquad \text{for} \quad \ell < \delta$$

For estimating the free distance we will split $\mathcal{G}$ into several matrices in different ways.

Case 1: $\ell \geq \delta - 1 > 0$

$$wt(v(z)) \geq wt\left((u_0\ \cdots\ u_{\delta-1}) \begin{pmatrix} G_0 & \cdots & G_{\delta-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix}\right) + wt\left((u_{\ell-\delta+1} \cdots u_\ell) \begin{pmatrix} G_\delta & & 0 \\ \vdots & \ddots & \\ G_1 & \cdots & G_\delta \end{pmatrix}\right)$$

Through row and column permutations the matrix $\begin{pmatrix} G_\delta & & 0 \\ \vdots & \ddots & \\ G_1 & \cdots & G_\delta \end{pmatrix}$ can be transformed into $\bar{G}^c_{\delta-1}$ and therefore all fullsize minors of both matrices are nonzero. Since $k = 1$, we have $L \geq \delta - 1$. Because all non trivially zero fullsize minors of $G^c_{\delta-1} = \begin{pmatrix} G_0 & \cdots & G_{\delta-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix}$ and $\bar{G}^c_{\delta-1} = \begin{pmatrix} G_\delta & \cdots & G_1 \\ & \ddots & \vdots \\ 0 & & G_\delta \end{pmatrix}$ are nonzero, which implies that G_0 and G_δ are full rank, and we can apply Theorem 2 to $\mathcal{C}$ and $\overline{\mathcal{C}}$, respectively. As $u_0 \neq 0 \neq u_\ell$, we can conclude

$$wt(v(z)) \geq 2\big((n-1)\delta + 1\big) = n(\delta+1) + n(\delta-1) - 2(\delta-1) \geq n(\delta+1).$$

Case 2: $1 \leq \ell < \delta - 1$

In this case, we have

$$wt(v(z)) \geq wt\left((u_0\ \cdots\ u_{\ell-1}) \begin{pmatrix} G_0 & \cdots & G_{\ell-1} \\ & \ddots & \vdots \\ 0 & & G_0 \end{pmatrix}\right) + wt\left((u_0\ \cdots\ u_\ell) \begin{pmatrix} G_\ell & \cdots & G_\delta \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\delta-\ell} \end{pmatrix}\right) +$$
$$+ wt\left((u_1\ \cdots\ u_\ell) \begin{pmatrix} G_\delta & & 0 \\ \vdots & \ddots & \\ G_{\delta-\ell+1} & \cdots & G_\delta \end{pmatrix}\right).$$

Applying Lemma 2, we obtain

$$wt\left((u_0 \ \cdots \ u_\ell)\begin{pmatrix} G_\ell & \cdots & G_\delta \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\delta-\ell} \end{pmatrix}\right) \geq n(\delta-\ell+1)-(\ell+1)+1.$$

Using Lemma 1, one gets as in the previous case that all nontrivial fullsize minors of $G^c_{\ell-1}$ and $\bar{G}^c_{\ell-1}$ are nonzero. Finally,

$$wt(v(z)) \geq 2\big((n-1)\ell+1\big)+n(\delta-\ell+1)-(\ell+1)+1 = n(\delta+1)+n\ell-3\ell+2 \geq n(\delta+1)$$

for $n \geq 3$ or $n = 2$ and $\ell \leq \delta - 2 \leq 4$.

If $n(\delta-\ell+1)-(\ell+1)+1 < 0$, the middle part of the weight and thus the condition on the matrix depending on ℓ is not needed. This explains the upper bound on ℓ in the assumptions of the theorem.

Case 3: $\ell = 0$

In this case, $wt(v(z)) = wt(u_0(G_0 \cdots G_\delta)) = n(\delta+1)$. □

To find constructions for generator matrices that fulfill the properties of the preceding theorem we can make use of so-called reverse superregular matrices as defined in the following.

Definition 4. *Let $r, n, m \in \mathbb{N}$ and consider a Toeplitz matrix $A \in \mathbb{F}_q^{(r+1)n\times(r+1)m}$ of the form $A = \begin{pmatrix} A_0 & \cdots & A_r \\ & \ddots & \vdots \\ 0 & & A_0 \end{pmatrix}$ with $A_i \in \mathbb{F}_q^{n\times m}$ for $i \in \{0,\dots,r\}$. A is called **(reverse) superregular Toeplitz matrix** if all non trivially zero minors (of any size) of the matices A and $A_{rev} = \begin{pmatrix} A_r & \cdots & A_0 \\ & \ddots & \vdots \\ 0 & & A_r \end{pmatrix}$ are nonzero.*

As all the matrices of the form $\begin{pmatrix} G_\ell & \cdots & G_\delta \\ \vdots & & \vdots \\ G_0 & \cdots & G_{\delta-\ell} \end{pmatrix}$ with $0 \leq \ell \leq \delta-2$ are submatrices of G^c_δ, all conditions of Theorem 3 are fulfilled if G^c_δ is a reverse superregular Toeplitz matrix. Hence, we can use existing constructions for reverse superregular Toeplitz matrices to construct MDS convolutional codes. Such constructions can e.g. be found in [Tom10] or [Lie18]. However, the field sizes obtained from these constructions are rather large. In the following section, we will present some examples for small code parameters over small finite fields using Theorem 3 directly.

1.3 Construction examples for small code parameters

In the following, we give some examples for small code parameters, where the criterion of Theorem 3 allows the construction of MDS convolutional codes over smaller fields than required for already existing constructions (up to our knowledge).

Example 1. *If $\delta = 1$ and n arbitrary, all conditions of Theorem 3 are fulfilled if and only if all fullsize minors of $(G_0 \ G_1)$ are nonzero. This means $G_0 = G_1 = (1 \ \cdots \ 1)$ defines an MDS convolutional code over any field. Obviously, the condition of Theorem 1 is sharp in this case.*

Example 2. *For $n = 2$, our criterion says that all non trivially zero fullsize minors of $(G_0 \ G_1 \ G_2)$, $\begin{pmatrix} G_0 & G_1 \\ 0 & G_0 \end{pmatrix}$ and $\begin{pmatrix} G_2 & G_1 \\ 0 & G_2 \end{pmatrix}$ have to be nonzero. It is easy to see that also in this case our criterion is not only sufficient but also necessary and an $(n,1,2)$ MDS convolutional code exists if and only if $q \geq n+1$, e.g. $G_0 = G_2 = (1 \ \cdots \ 1)$ and $G_1 = (1 \ \alpha \ \cdots \alpha^{n-1})$ with α primitive element of $\mathbb{F}_q$. For $n = 2$ this field size is smaller than in existing constructions, for $n \geq 3$ it is equal to the best existing construction [GLL06].*

Example 3. *For $n = \delta = 3$, the best existing constructions require $q \geq 10$ (see [Jus75, GLL06]). Using Theorem 3, a $(3,1,3)$ convolutional code over $\mathbb{F}_{16}$ with generator matrix $G(z) = \sum_{i=0}^{3} G_i z^i$, such that $G_0 = (\alpha^2+1 \ \ 1 \ \ \alpha^3+1)$, $G_1 = (\alpha^3+\alpha \ \ \alpha^3+\alpha^2+1 \ \ \alpha^3)$, $G_2 = (\alpha^3+\alpha^2+\alpha+1 \ \ \alpha+1 \ \ \alpha^3+\alpha^2+\alpha)$ and $G_3 = (\alpha^2+1 \ \ \alpha^3+\alpha^2 \ \ \alpha^2+\alpha+1)$, with α as primitive element of $\mathbb{F}_{16}$, is an*

MDS convolutional code.
To improve the field size, we look where in the proof of Theorem 3 our estimations were not sharp and realize that in Case 2 ($\ell = 1$), we get weight 3 from G_1^c and $\bar{G}_1^c$, respectively. Hence, we only need weight 6 coming from the part $\begin{pmatrix} G_1 & G_2 & G_3 \\ G_0 & G_1 & G_2 \end{pmatrix}$. *Lemma 2 tells us that for this it is enough if all fullsize minors of the three separated matrices* $\begin{pmatrix} G_1 \\ G_0 \end{pmatrix}$ *and* $\begin{pmatrix} G_2 \\ G_1 \end{pmatrix}$ *and* $\begin{pmatrix} G_3 \\ G_2 \end{pmatrix}$ *and are nonzero. With this modified version of Theorem 3, we found an* $(3, 1, 3)$ *MDS convolutional code over* $\mathbb{F}_7$ *defined by the generator matrix* $G(z) = \sum_{i=0}^{3} G_i z^i$, *with* $G_0 = (4\ 4\ 5)$, $G_1 = (6\ 5\ 3)$, $G_2 = (3\ 2\ 6)$ *and* $G_3 = (5\ 3\ 4)$.

2 Conclusion

We presented a new criterion for MDS convolutional codes with rate $1/n$ as well as some examples over small finite fields. For future work, we will investigate to which extent we can release the conditions of our main theorem depending on the code parameters to obtain construction examples for MDS convolutional codes over smaller fields. Moreover, we will generalize our results to convolutional codes with $k > 1$ and also cover the case rate $1/2$, $\delta \geq 5$.

Acknowledgements

This work is supported by the Swiss National Science Foundation grant n. 188430 and The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), UIDB/04106/2020 and UIDP/04106/2020. The work of the first author was also supported by FCT grant UI/BD/151186/2021.

References

[GLL06] H. Gluesing-Luerssen and B. Langfeld. A class of one-dimensional mds convolutional codes. *Journal of Algebra and Its Applications*, 5(4):505–520, 2006.

[GLRS06] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. 52(2):584–598, 2006.

[Hut08] R. Hutchinson. The existence of strongly MDS convolutional codes. *SIAM J. Control Optim.*, 47(6):2812–2826, 2008.

[Jus75] J. Justesen. An algebraic construction of rate $1/\nu$ convolutional codes. *IEEE Trans. Inform. Theory*, IT-21(1):577–580, 1975.

[Lie18] J. Lieb. Complete MDP convolutional codes. *Journal of Algebra and Its Applications*, 2018.

[LP20] J. Lieb and R. Pinto. Constructions of mds convolutional codes using superregular matrices. *J. Algebra Comb. Discrete Appl.*, 7(1):71–82, 2020.

[RS99] J Rosenthal and R Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Engineering, Communication and Computing*, 10(1):15–32, 1999.

[SGLR01] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions for MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.

[SR98] R. Smarandache and J. Rosenthal. A state space approach for constructing MDS rate $1/n$ convolutional codes. In *Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory*, pages 116–117, Killarney, Kerry, Ireland, June 1998.

[Tom10] V. Tomás. *Complete-MDP convolutional codes over the erasure channel.* PhD thesis, Departamento de Ciencia de la Computacion e Inteligencia Artificial, Universidad de Alicante, Alicante, Spain, 2010.