Advances in Mathematics of Communications
Volume 10, No. 2, 2016, 275–290

doi:10.3934/amc.2016005

CONSTRUCTING STRONGLY-MDS CONVOLUTIONAL CODES WITH MAXIMUM DISTANCE PROFILE

Diego Napp

CIDMA - Center for Research and Development in Mathematics and Applications
Department of Mathematics, University of Aveiro, Portugal

Roxana Smarandache

Departments of Mathematics, and of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46566, USA

(Communicated by Heide Gluesing-Luerssen)

Abstract. This paper revisits strongly-MDS convolutional codes with maximum distance profile (MDP). These are (non-binary) convolutional codes that have an optimum sequence of column distances and attains the generalized Singleton bound at the earliest possible time frame. These properties make these convolutional codes applicable over the erasure channel, since they are able to correct a large number of erasures per time interval. The existence of these codes have been shown only for some specific cases. This paper shows by construction the existence of convolutional codes that are both strongly-MDS and MDP for all choices of parameters.

1. Introduction

In recent literature on convolutional codes, several new classes of codes with good distance properties have been introduced. These classes of codes are known as maximum distance separable (MDS) codes, maximum distance profile (MDP) codes, and strongly MDS (sMDS) codes [10–13, 20, 21]. MDS codes are characterized by the property that they have the maximum possible free distance for a given rate and degree. sMDS codes are a subclass of MDS codes having the property that the free distance is attained at the earliest possible time step. Finally, MDP codes are characterized by the property that their column distances grow at a maximum possible rate.

The existence of MDP convolutional codes was first discussed in [12], and in [10], it was shown how to construct them when $n-k$ divides δ. In this paper, we solve the problem of constructing MDP convolutional codes in the general case where $n-k$ does not necessarily divide δ. Apart from solving a theoretical question, this construction also has a practical purpose, as we explain below. Recently, a number

2010 *Mathematics Subject Classification:* Primary: 94B10, 11T71.

Key words and phrases: Convolutional codes, maximum distance separable (MDS) convolutional codes, maximum distance profile (MDP) convolutional codes, erasure channel.

The first author's research has been supported in part by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2013 and the research of the second has been supported by the NSF Grants CCF 1252788 and DMS 1313221.

of papers [24–27] considered the use of MDP convolutional codes over the erasure channel, where the symbols sent either arrive correctly or they are erased. The Internet is such an example; here the packet sizes are upper bounded by 12,000 bits - the maximum that the Ethernet protocol allows. Each packet can be modeled as an element or a sequence of elements from a large alphabet, for example $\mathbb{F} := \mathbb{F}_{2^{1,000}}$. Packets sent over the Internet are protected by a cyclic redundancy check (CRC) code. If the CRC check fails, the receiver knows that a packet is in error or has not arrived [18]; it then declares an erasure. With or without interleaving, such an encoding scheme results in the property that errors tend to occur in bursts, and this is a phenomenon observed over many channels modeled via the erasure channel. When transmitting over an erasure channel like the Internet, one of the problems encountered is the delay experienced on the received information due to the possible re-transmission of lost packets. One way to eliminate these delays is by using forward error correction. Commonly, block codes have been used for such a task, see, e.g., [7, 15] and the references therein. The use of convolutional codes over the erasure channel has been proposed in Epstein [6], Arai et al. [4], and more recenty [27] in which a subclass of MDP codes was used over the erasure channel. The advantage that convolutional codes have over block codes, exploited in their decoding algorithms, is the flexibility obtained through the "sliding window" feature of convolutional codes. The received information can be grouped in appropriate ways, depending on the erasure bursts, and then be decoded by decoding the "easy" blocks first. This flexibility in grouping information brings certain freedom in the handling of sequences. This "sliding window" property of convolutional codes allows for more erasures to be corrected in a given block than a block code of that same length could correct. In addition, the algebraic properties of maximum distance profile (MDP) convolutional codes allow these codes to correct the largest amount of errors possible for a given window, making them powerful encoding schemes over the erasure channel (see [27] for details).

The paper is organized as follows. In Section 2, we introduce the background necessary for the development of the paper: it includes the necessary introductory material on convolutional codes and on MDP convolutional codes, in particular. In Section 3, we include the main result of the paper: for each parameter n, k, δ, and, in particular, for the open problem case of $(n-k) \nmid \delta$, we show how to construct (n, k, δ) convolutional codes that are MDP (our codes will also be sMDS). At the end of Section 3, we formulate this constructive algorithm, and in Section 4 we conclude our paper.

2. Preliminaries

This section contains the mathematical background needed for the development of our results. Note that throughout the paper, vectors of length n will be viewed as $n \times 1$ matrices, i.e., as column vectors.

Let $\mathbb{F}$ be a finite field and $\mathbb{F}[D]$ be the ring of polynomials with coefficients in $\mathbb{F}$.

A *convolutional code* $\mathcal{C}$ of rate k/n is an $\mathbb{F}[D]$-submodule of $\mathbb{F}[D]^n$ of rank k given by a *basic* and *minimal* full-rank polynomial *encoder matrix* $G(D) \in \mathbb{F}[D]^{k \times n}$ through

$$\mathcal{C} = \mathrm{Im}_{\mathbb{F}[D]} G(D) = \left\{ G(D)^\top u(D) : \, u(D) \in \mathbb{F}^k[D] \right\},$$

where *basic* means that $G(D)$ has a polynomial right inverse, and *minimal* means that the sum of the row degrees of $G(D)$ attains its minimal possible value δ, called the *degree* of $\mathcal{C}$.*

A rate k/n convolutional code $\mathcal{C}$ of degree δ is called an (n,k,δ) convolutional code [17].

A dual description of a convolutional code $\mathcal{C}$ can be given through one of its *parity-check* matrices which are $(n-k)\times n$ full rank polynomial matrices $H(D)$ such that

$$\mathcal{C} = \ker H(D) = \left\{ v(D) \in \mathbb{F}[D]^n \;\mid\; H(D)v(D) = 0 \in \mathbb{F}[D]^{n-k} \right\}.$$

If $v(D) \in \mathbb{F}[D]^n$ has degree $l \geq 0$, $v(D) = v_0 + v_1 D + \ldots + v_l D^l$, and

$$H(D) = H_0 + H_1 D + \cdots + H_m D^m,$$

where $H_m \neq 0$ and $H_i = 0$, for $i > m$, the above kernel representation can be expanded as

$$(1) \qquad \begin{bmatrix} H_0 & & & & \\ \vdots & \ddots & & & \\ H_m & \cdots & H_0 & & \\ & \ddots & \vdots & \ddots & \\ & & H_m & \cdots & H_0 \\ & & & \ddots & \vdots \\ & & & & H_m \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_l \end{bmatrix} = 0.$$

An important distance measure for a convolutional code $\mathcal{C}$ is its *free distance* $d_{\text{free}}(\mathcal{C})$ defined as

$$d_{\text{free}}(\mathcal{C}) \triangleq \min\left\{ \text{wt}(v(D)) \;\mid\; v(D) \in \mathcal{C} \quad \text{and} \quad v(D) \neq 0 \right\},$$

where $\text{wt}(v(D))$ is the Hamming weight of a polynomial vector

$$v(D) = \sum_{i\in\mathbb{N}} v_i D^i \in \mathbb{F}[D]^n,$$

defined as

$$\text{wt}(v(D)) \triangleq \sum_{i\in\mathbb{N}} \text{wt}(v_i),$$

where $\text{wt}(v_i)$ is the number of the nonzero components of v_i.

In [20], Rosenthal and Smarandache showed that the free distance of an (n,k,δ) convolutional code is upper bounded by

$$(2) \qquad d_{\text{free}}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) + \delta + 1.$$

This bound was called the *generalized Singleton bound* since it generalizes in a natural way the Singleton bound for block codes (when $\delta = 0$). An (n,k,δ) convolutional code with its free distance equal to the generalized Singleton bound was called a *maximum distance separable* (MDS) code [20]. It was also observed in [20] that if $\mathcal{C}$ is an MDS convolutional code, then all the row-reduced encoders of $\mathcal{C}$ have $\ell := \delta - k\left\lfloor \frac{\delta}{k} \right\rfloor$ rows of degree $\left\lfloor \frac{\delta}{k} \right\rfloor$ and $k-\ell$ rows of degree $\left\lfloor \frac{\delta}{k} \right\rfloor + 1$. Equivalent result holds for minimal basic parity-check matrices $H(D)$ and hence all row degrees of $H(D)$ are upper bounded by $m \triangleq \left\lceil \frac{\delta}{n-k} \right\rceil$ and the degree δ is the sum of the row degrees of $H(D)$.

*Therefore, the *degree* δ of a convolutional code $\mathcal{C}$ is the sum of the row degrees of one, and hence any, minimal basic encoder.

Another important distance measure for a convolutional code is the *jth column distance* $d_j^c(\mathcal{C})$, given by the equivalent expressions

$$\begin{aligned} d_j^c(\mathcal{C}) &\triangleq \min\left\{\mathrm{wt}(v_{[0,j]}(D)) \;\mid\; v(D) \in \mathcal{C} \;\text{ and }\; v_0 \neq 0\right\} \\ &\triangleq \min\left\{\mathrm{wt}(\hat{v}) \;\mid\; \hat{v} = (v_0, \dots, v_j)^\top \in \ker H_j^c \subset \mathbb{F}^{(j+1)n},\; v_0 \neq 0\right\} \end{aligned} \tag{3}$$

where $v_{[0,j]}(D) = v_0 + v_1 D + \ldots + v_j D^j$ represents the j-th truncation of the codeword $v(D) \in \mathcal{C}$ and

$$H_j^c \triangleq \begin{bmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \cdots & H_0 \end{bmatrix} \in \mathbb{F}^{(j+1)(n-k)\times(j+1)n}, \tag{4}$$

where $H_j = 0$, for $j > m$. This notion is related to the free distance $d_{\mathrm{free}}(\mathcal{C})$ in the following way

$$d_{\mathrm{free}}(\mathcal{C}) = \lim_{j\to\infty} d_j^c(\mathcal{C}). \tag{5}$$

The j-th column distance is upper bounded as following

$$d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1, \tag{6}$$

and the maximality of any of the jth column distances implies the maximality of all the previous ones, [10, 12], *i.e.*,

$$d_j^c(\mathcal{C}) = (n-k)(j+1)+1 \Longrightarrow d_i^c(\mathcal{C}) = (n-k)(i+1)+1, \quad \forall i \leq j.$$

Since no column distance can achieve a value greater than the generalized Singleton bound, there must exist an integer L for which the bound (6) could be attained for all $j \leq L$ and it is a strict inequality for $j > L$ [10]; this value is

$$L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor. \tag{7}$$

An (n, k, δ) convolutional code $\mathcal{C}$ with every $d_j^c(\mathcal{C})$ maximal, for each $j \leq L$, is called a *maximum distance profile* (MDP) code [10, 12]. Therefore, the column distances of MDP codes increase as rapidly as possible for as long as possible. In contrast, an (n, k, δ) convolutional code $\mathcal{C}$ is called a *strongly-MDS* code if the generalized Singleton bound is attained as early as possible [10]. We state these two definitions formally.

Definition 1 ([10])**.** Let $\mathcal{C}$ be a convolutional code of rate k/n and degree δ.

1. $\mathcal{C}$ is said to have a maximum distance profile (MDP) if

   $$d_j^c = (n-k)(j+1)+1, \;\text{ for } j = 0, \dots, L,$$

   where $L = \lfloor \frac{\delta}{k} \rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$, or, equivalently (see [10, Remark 2.10]), if

   $$d_L^c = (n-k)(L+1)+1.$$

2. $\mathcal{C}$ is called a *strongly MDS* (sMDS) code if

   $$d_M^c = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1, \;\text{ for } M = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lceil \frac{\delta}{n-k} \right\rceil,$$

   where M is the minimum instance j such that $d_j^c = d_{\mathrm{free}}(\mathcal{C})$.

Remark 1. Note that, in general, neither MDP implies sMDS, nor sMDS implies MDP. However, for $n-k \mid \delta$ the two notions MDP and sMDS are equivalent. This is what makes this case simpler to address, see [10].

Remark 2. Note that MDP convolutional codes are similar to MDS block codes within windows of size $(L+1)n$. Indeed, if we truncate a codeword with its first component nonzero at any j component, with $j \leq L$, it will have weight higher or equal than the bound (6), which is the Singleton bound for block codes with the given parameters.

The next definition is essential for our construction of MDP codes; it gives a description of these codes using the "superregularity" of a certain matrix associated to a given parity-check matrix, as Theorem 1 below, taken from [10], will formally state.

Let $\theta = (\theta_{ij})$ be a square matrix of order m over $\mathbb{F}$ (or $\mathbb{Z}$) and let S_m be the symmetric group of order m. The determinant $\det(\theta)$ of θ is given by

$$\det(\theta) \triangleq \sum_{\sigma \in S_m} (-1)^{\operatorname{sgn}(\sigma)} \theta_{1\sigma(1)} \cdots \theta_{m\sigma(m)}, \tag{8}$$

where $\operatorname{sgn}(\sigma)$ is the signature of the permutation σ.

Definition 2. If $\theta = (\theta_{ij})$ is a square submatrix of a matrix γ over $\mathbb{F}$ (or $\mathbb{Z}$) with $\theta_{1\sigma(1)} \cdots \theta_{m\sigma(m)} = 0$, for all $\sigma \in S_m$, we say that $\det(\theta)$ is a *trivial minor* of γ. Let $\{M_{ij}\}$ be a set of matrices of the same size and $\gamma = (M_{ij})$ be a lower triangular block matrix, *i.e.*, $M_{ij} = 0$ for $i < j$. We say that γ is a *superregular* matrix if all entries of M_{ij}, $i \geq j$, are different from zero and all the non-trivial minors of γ are non-zero.

Observe that the trivial minors of a superregular matrix come from submatrices that contain a zero in their diagonal, or equivalent, submatrices that contain an $s \times t$ zero block for some s, t such that $s + t - 1$ is equal to or larger than its order.

It is important to remark here that there are several related but different notions of superregular matrices in the literature. Frequently, see for instance [22], a superregular matrix is defined to be a matrix (not necessarily lower block triangular) with the property that *all* of its square submatrices are nonsingular, implying that such a matrix must have all its entries nonzero. Also, in [1, 16, 23], several examples of triangular matrices were constructed in such a way that all submatrices inside this triangular configuration were nonsingular. These notions however, do not apply to the case we consider; we will consider matrices that allow zero entries. The more recent contributions [10, 11, 13, 24, 25] consider the same notion of superregularity but defined only for lower triangular matrices. The notion we consider comprises, however, a larger set, e.g., apart from lower triangular matrices, it also includes block triangular matrices.

Theorem 1. *Let $\mathcal{C} = \{v(D) \in \mathbb{F}((D))^n \mid H(D)v(D) = 0\}$ be a (n, k, δ) convolutional code with a minimal basic parity-check matrix $H(D)$ and let*

$$A(D) = \sum_{i=0}^{m} A_i D^i \in \mathbb{F}[D]^{(n-k)\times(n-k)},$$

$$B(D) = \sum_{i=0}^{m} B_i D^i \in \mathbb{F}[D]^{(n-k)\times k}, \tag{9}$$

such that

$$H(D)=\sum_{i=0}^{m} H_i D^i=\sum_{i=0}^{m}\begin{bmatrix}A_i & B_i\end{bmatrix} D^i=\begin{bmatrix}A(D) & B(D)\end{bmatrix}\in \mathbb{F}[D]^{(n-k)\times n}, \tag{10}$$

where $m \triangleq \lfloor\frac{\delta}{n-k}\rfloor+1=\lceil\frac{\delta}{n-k}\rceil$ *(we assume* $n-k\nmid\delta$*). Assume in addition that* A_0 *is invertible and let*

$$A(D)^{-1}B(D)=\sum_{i=0}^{\infty} P_i D^i\in\mathbb{F}((D))^{(n-k)\times k} \tag{11}$$

be the Laurent expansion of $A(D)^{-1}B(D)$ *over the field* $\mathbb{F}((D))$ *of Laurent series. For all* $j\ge 0$*, define*

$$\widehat{H}_j^c \triangleq \begin{bmatrix}I_{(j+1)(n-k)} & P_j^c\end{bmatrix}, \tag{12}$$

where the matrix $I_{(j+1)(n-k)}$ *is the identity matrix of size* $(j+1)(n-k)$ *and*

$$P_j^c \triangleq \begin{bmatrix}P_0 & 0 & \cdots & 0\\ P_1 & P_0 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ P_j & P_{j-1} & \cdots & P_0\end{bmatrix}. \tag{13}$$

Then, the following conditions are equivalent, for all $j\in\{1,\dots,L\}$*:*

1. $d_j^c=(n-k)(j+1)+1$*;*
2. *every nontrivial* $(n-k)(j+1)\times(n-k)(j+1)$ *full-size minor of* H_j^c *is nonzero.*
3. P_j^c *is superregular;*

Proof. The proof follows directly from [10, Theorem 2.4 & Theorem 3.1] and the definition of superregular matrix. □

3. Constructing MDP convolutional codes

Given the parameters $n,k,\delta\in\mathbb{N}$, $k<n$, such that $(n-k)\nmid\delta$, our goal is to construct an (n,k,δ) convolutional code with the MDP property.[†] In fact, we will construct an sMDS code with the MDP property, *i.e.*, by Definition 1, we search for an (n,k,δ) code such that

$$d_L^c=(n-k)(L+1)+1 \qquad \text{(MDP)}$$
$$d_M^c=(n-k)\left(\left\lfloor\frac{\delta}{k}\right\rfloor+1\right)+\delta+1 \qquad \text{(sMDS)}.$$

We aim to construct a matrix $H(D)=\begin{bmatrix}A(D) & B(D)\end{bmatrix}\in\mathbb{F}[D]^{(n-k)\times n}$, as in Theorem 1 that satisfy the MDP and sMDS properties, or equivalently, such that the matrix P_L^c defined through (11) and (13) (for $j=L$) is superregular and such that

$$d_M^c=(n-k)\left(\left\lfloor\frac{\delta}{k}\right\rfloor k+1\right)+\delta+1.$$

[†] The case $(n-k)\mid\delta$ has been addressed successfully in [10, Theorem 3.1]. The remaining case $(n-k)\nmid\delta$ is still unsolved and was left as an open problem in [10–12].

To this end, we construct a matrix

$$P_M^c = \begin{bmatrix} P_0 & 0 & \cdots & 0 \\ P_1 & P_0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ P_M & P_{M-1} & \cdots & P_0 \end{bmatrix}, \tag{14}$$

such that its submatrix P_L^c is superregular. We will show that this matrix defines a unique code $\mathcal{C} = \ker \begin{bmatrix} A(D) & B(D) \end{bmatrix}$ through

$$A(D)^{-1}B(D) \triangleq \sum_{i=0}^{M} P_i D^i + \mathcal{O}(D^{M+1}) \in \mathbb{F}((D))^{(n-k)\times k}, \tag{15}$$

where, for all $i \in \{0,\dots,M\}$, P_i are the block entries of the matrix P_M^c. The superegularity of P_L^c will guarantee that the code $\mathcal{C} = \ker H(D)$ has $d_L^c = (n-k)(L+1)+1$. The choice of the remaining part of P_M^c will ensure that $d_M^c = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor k + 1\right) + \delta + 1$ and that the code $\mathcal{C}$ has rate k/n and degree δ.

Let

$$T_M^c = \begin{bmatrix} T_0 & 0 & \cdots & 0 \\ T_1 & T_0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ T_M & T_{M-1} & \cdots & T_0 \end{bmatrix} \in \mathbb{F}^{(n-k)(M+1)\times k(M+1)} \tag{16}$$

be a superregular matrix and let $P_i \triangleq T_i$, for $i \in \{0,\dots,L\}$, and

$$P_L^c \triangleq \begin{bmatrix} P_0 & 0 & \cdots & 0 \\ P_1 & P_0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ P_L & P_{L-1} & \cdots & P_0 \end{bmatrix} = \begin{bmatrix} T_0 & 0 & \cdots & 0 \\ T_1 & T_0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ T_L & T_{L-1} & \cdots & T_0 \end{bmatrix} \triangleq T_L^c. \tag{17}$$

For issues concerning the existence and constructions of such superregular matrices see [2, 10].

It might seem natural to choose $P_M \triangleq T_M$. Since T_M^c is superregular, this choice would seem to ensure also the maximality of the Mth column distance of the code $\mathcal{C}$, i.e.,

$$d_M^c = (n-k)(M+1)+1.$$

However, if the code has rate k/n and degree δ,

$$(n-k)(M+1)+1 > (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1 \geq d_{\text{free}},$$

where the second inequality holds because the middle expression is the generalized Singleton bound for the given parameters. This yields that

$$d_M^c > d_{\text{free}} = \lim_{j\to\infty} d_j^c \geq d_M^c,$$

since d_j^c is increasing in j, which leads to a contradiction. Therefore, P_M has to be chosen differently.

Note that, when $(n-k) \nmid \delta$, which is the case we consider here, we have that

$$\left\lceil \frac{\delta}{n-k} \right\rceil - 1 = \left\lfloor \frac{\delta}{n-k} \right\rfloor \qquad \text{and}$$

$$(n-k) = \delta - \left\lfloor \frac{\delta}{n-k} \right\rfloor (n-k) + \left\lceil \frac{\delta}{n-k} \right\rceil (n-k) - \delta .$$

For simplicity, we denote $\overline{\delta} \triangleq \delta - \left\lfloor \frac{\delta}{n-k} \right\rfloor (n-k)$ and $\underline{\delta} \triangleq \left\lceil \frac{\delta}{n-k} \right\rceil (n-k) - \delta$, and obtain, therefore, that $(n-k) = \underline{\delta} + \overline{\delta}$.

We partition T_M in the following way. Let

$$T_M \triangleq \left[\begin{array}{c} \overline{T}_M \\ \hline \underline{T}_M \end{array} \right] \triangleq \left[\begin{array}{c|c} \overline{T}_M^{(1)} & \overline{T}_M^{(2)} \\ \hline \underline{T}_M^{(1)} & \underline{T}_M^{(2)} \end{array} \right] \in \mathbb{F}^{(n-k)\times k} \tag{18}$$

where

$$\overline{T}_M \in \mathbb{F}^{\overline{\delta}\ \times\ k}, \qquad \underline{T}_M \in \mathbb{F}^{\underline{\delta}\ \times\ k}$$

and

$$\overline{T}_M^{(1)} \in \mathbb{F}^{\overline{\delta}\ \times\ \delta - \lfloor \frac{\delta}{k} \rfloor k}\ , \quad \underline{T}_M^{(1)} \in \mathbb{F}^{\underline{\delta}\ \times\ \delta - \lfloor \frac{\delta}{k} \rfloor k}\ ,$$

$$\overline{T}_M^{(2)} \in \mathbb{F}^{\overline{\delta}\ \times\ \left(\lfloor \frac{\delta}{k} \rfloor + 1\right)k - \delta}\ , \quad \underline{T}_M^{(2)} \in \mathbb{F}^{\underline{\delta}\ \times\ \left(\lfloor \frac{\delta}{k} \rfloor + 1\right)k - \delta}\ .$$

Analogously,

$$P_M \triangleq \left[\begin{array}{c} \overline{P}_M \\ \hline \underline{P}_M \end{array} \right] \triangleq \left[\begin{array}{c|c} P_M^{(1)} & P_M^{(2)} \end{array} \right] \triangleq \left[\begin{array}{c|c} \overline{P}_M^{(1)} & \overline{P}_M^{(2)} \\ \hline \underline{P}_M^{(1)} & \underline{P}_M^{(2)} \end{array} \right] \tag{19}$$

and define

$$\overline{P}_M^{(1)} \triangleq \overline{T}_M^{(1)}\ , \quad \overline{P}_M^{(2)} \triangleq \overline{T}_M^{(2)}\ , \quad \underline{P}_M^{(1)} \triangleq \underline{T}_M^{(1)},$$

i.e.,

$$P_M \triangleq \left[\begin{array}{c|c} \overline{P}_M^{(1)} & \overline{P}_M^{(2)} \\ \hline \underline{P}_M^{(1)} & \underline{P}_M^{(2)} \end{array} \right] = \left[\begin{array}{c|c} \overline{T}_M^{(1)} & \overline{T}_M^{(2)} \\ \hline \underline{T}_M^{(1)} & X \end{array} \right], \tag{20}$$

where the matrix $\underline{P}_M^{(2)} \triangleq X$ is still to be determined. Nevertheless, we can already derive, independently of the choice of $\underline{P}_M^{(2)}$, the following result which will lead us to the desired construction.

Lemma 1. *Let (n,k,δ) be given such that $n-k \nmid \delta$. Let T_M^c as in (16) be a superregular matrix and select $P_i \triangleq T_i$, $i = 0, \dots, M-1$, and P_M such that $\overline{P}_M^{(1)} \triangleq \overline{T}_M^{(1)}$, $\overline{P}_M^{(2)} \triangleq \overline{T}_M^{(2)}$, $\underline{P}_M^{(1)} \triangleq \underline{T}_M^{(1)}$, $\underline{P}_M^{(2)} \triangleq X$ as in (20) with X variable. Let $\mathcal{C} = \ker H(D)$, A_i and B_i satisfying equations (10) and (15). If A_0 is invertible then, for any matrix X, the following hold:*

1. $d_L^c = (n-k)(L+1)+1$;
2. $d_M^c \geq (n-k)\left(\lfloor \frac{\delta}{k} \rfloor + 1\right) + \delta + 1$.

Proof. Statement 1. follows directly from Theorem 1.

Statement 2: From (3), it follows that

$$d_M^c \quad = \quad \min \left\{ \mathrm{wt}(\hat{v}) \,|\, \hat{v} = (\hat{v}_0, \hat{v}_1, \dots, \hat{v}_M)^\top \in \ker H_M^c \subset \mathbb{F}^{(M+1)n}\ , \hat{v}_0 \neq 0 \right\}.$$

It is easy to see that after a column permutation the sliding parity-check matrix H_M^c in (4) of $\mathcal{C}$ has the form

$$H_M^{c'} \triangleq \left[\begin{array}{cccc|cccc} A_0 & 0 & \cdots & 0 & B_0 & 0 & \cdots & 0 \\ A_1 & A_0 & \cdots & 0 & B_1 & B_0 & \cdots & 0 \\ A_2 & A_1 & \cdots & 0 & B_2 & B_1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_M & A_{M-1} & \cdots & A_0 & B_M & B_{M-1} & \cdots & B_0 \end{array}\right]$$

and using that A_0 is invertible we can left multiply $H_M^{c'}$ by the inverse of the first block to obtain $\widehat{H}_M^c$ (defined in (12)). Hence,

$$\begin{aligned} d_M^c &= \min\left\{ \mathrm{wt}(\bar{v}) \,|\, \bar{v} = (\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{2M+2})^\top \in \ker H_M^{c'} \subset \mathbb{F}^{(M+1)n} \,, (\bar{v}_0, \bar{v}_{M+2}) \neq 0 \right\} \\ &= \min\left\{ \mathrm{wt}(\bar{v}) \,|\, \bar{v} = (\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{2M+2})^\top \in \ker \widehat{H}_M^{c} \subset \mathbb{F}^{(M+1)n} \,, \bar{v}_{M+2} \neq 0 \right\}, \end{aligned}$$

where the vector $\bar{v} = (\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{2M+1})$ is divided according to $H_M^{c'}$ (or $\widehat{H}_M^c$). Note that when considering $\ker \widehat{H}_M^c$, the condition $(\bar{v}_0, \bar{v}_{M+2}) \neq 0$ is equivalent to $\bar{v}_{M+2} \neq 0$. On the other hand, let

$$\widehat{H}_M^{trunc} \triangleq \left[\begin{array}{c|c} I_{(n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta} & \underbrace{\begin{array}{ccccc} P_0 & 0 & \cdots & \cdots & 0 \\ P_1 & P_0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ P_L & P_{L-1} & \cdots & P_0 & 0 \\ \overline{P}_M & \overline{P}_L & \cdots & \overline{P}_1 & \overline{P}_0 \end{array}}_{\triangleq \widehat{P}_M^{trunc}} \end{array}\right]$$

be the submatrix of $\widehat{H}_M^c$ obtained by discarding its last $\underline{\delta}$ rows while keeping the first $\overline{\delta}$ rows of $[P_M \; P_{M-1} \cdots P_0]$, denoted by $[\overline{P}_M \; \overline{P}_L \dots \overline{P}_0]$. Then,

$$\begin{aligned} &\min\left\{ \mathrm{wt}(\bar{v}) \,|\, \bar{v} = (\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{2M+2})^\top \in \ker \hat{H}_M^{c} \subset \mathbb{F}^{(M+1)n} \,, \bar{v}_{M+2} \neq 0 \right\} \geq \\ &\min\left\{ \mathrm{wt}(\bar{v}) \,|\, \bar{v} = (\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{2M+2})^\top \in \ker \hat{H}_M^{trunc} \subset \mathbb{F}^{(M+1)n} \,, \bar{v}_{M+2} \neq 0 \right\} \end{aligned}$$

Since $\widehat{P}_M^{trunc} \in \mathbb{F}^{(n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta \, \times \, k(M+1)}$ is a superregular matrix, then every $\left((n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta\right) \times \left((n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta\right)$ full-size minor of $\widehat{H}_M^{trunc}$ is nonzero and therefore we obtain that

$$\begin{aligned} &\min\left\{ \mathrm{wt}(\bar{v}) \,|\, \bar{v} = (\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{2M+2})^\top \in \ker \hat{H}_M^{trunc} \subset \mathbb{F}^{(M+1)n} \,, \bar{v}_{M+2} \neq 0 \right\} = \\ &(n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \end{aligned}$$

Hence,

$$d_M^c \geq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{21}$$

□

We can now prove the existence of a convolutional codes with sMDS and MDP properties.

Theorem 2. *Given any set of parameters (n, k, δ), there exists an (n, k, δ) convolutional code that is both sMDS and MDP.*

Proof. It is well-known that a convolutional code of rate k/n and degree δ cannot have free distance larger than the Singleton bound $(n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1$. The previous Lemma shows that a code $\mathcal{C} = \ker H(D)$ with A_i, B_i and the P_i related via equation (15) and P_i chosen as in (17) and (20), has d^c_M equal to or larger than the Singleton bound of an (n,k,δ) code. We still do not know the rate and degree of $\mathcal{C}$ but if $\mathcal{C}$ had rate k/n and degree δ, then its free distance must satisfy the Singleton bound for these parameters, i.e., $d_{\text{free}} \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1$. Since $d^c_M \leq d_{\text{free}}$ and from (21) we obtain that

$$d_{\text{free}} = d^c_M = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1,$$

i.e., $\mathcal{C}$ is an sMDS (n,k,δ) code. Since $\mathcal{C}$ also has the MDP property ($d^c_L = (n-k)(L+1)+1$) this construction would produce the desired (n,k,δ)-code that is sMDS and has the MDP property.

Hence, we will choose $\underline{P}^{(2)}_M$ based on the following criteria:

1. The constructed matrix P^c_M should generate, via equation (15), the matrices A_i and B_i, such that the code $\mathcal{C}$ is an (n,k,δ) code.
2. A_0 is invertible (we can apply Theorem 1 and Lemma 1).

For this purpose we make the following partition:

$$A_i = \begin{bmatrix} \overline{A}_i \\ \underline{A}_i \end{bmatrix} \in \mathbb{F}^{(n-k)\times(n-k)}\ , \qquad B_i = \begin{bmatrix} \overline{B}_i \\ \underline{B}_i \end{bmatrix} \in \mathbb{F}^{(n-k)\times k},$$

where,

$$\begin{aligned} &\overline{A}_i \in \mathbb{F}^{\overline{\delta}\ \times\ (n-k)}\ , \quad \overline{B}_i \in \mathbb{F}^{\overline{\delta}\ \times\ k}\ , \\ &\underline{A}_i \in \mathbb{F}^{\underline{\delta}\ \times\ (n-k)}\ , \quad \underline{B}_i \in \mathbb{F}^{\underline{\delta}\ \times\ k}\ , \quad i \in \{0,\dots,m\}. \end{aligned}$$

The freedom to choose $\underline{P}^{(2)}_M$ also gives some freedom in choosing the A_i's and B_i's. Making use of this freedom we shall impose the conditions:

1. $\underline{A}_m = 0\ , \quad \underline{B}_m = 0\ ,$
2. A_0 invertible,

and show that these conditions ensure that the above mentioned criteria are satisfied[‡].

Recall that $m = \lceil \frac{\delta}{n-k} \rceil$,

$$A(D) = \sum_{i=0}^{m} A_i D^i \in \mathbb{F}[D]^{(n-k)\times(n-k)}, \quad B(D) = \sum_{i=0}^{m} B_i D^i \in \mathbb{F}[D]^{(n-k)\times k}$$

and

$$B(D) = A(D)\left(\sum_{i=0}^{M} P_i D^i + \text{higher terms}\right). \tag{22}$$

Equating the coefficients of $D^m,\ D^{m+1},\dots,D^M$, it follows that

$$[A_m \dots A_0] \begin{bmatrix} P_0 & \cdots & P_{M-m} \\ \vdots & \ddots & \vdots \\ P_m & \cdots & P_M \end{bmatrix} = [B_m\ 0 \dots 0].$$

[‡] In the case $(n-k) \mid \delta$, the matrices above are simply $\overline{A}_i = A_i$, $\overline{B}_i = B_i$, $\underline{A}_i = 0$, $\underline{B}_i = 0$, for all $i \in \{0,\dots,m\}$. This fact makes this case easier to address, see [10].

Using the partition of the A_i's and B_i's and imposing the conditions $\underline{A}_m = 0$, $\underline{B}_m = 0$, we obtain that

$$[\underline{A}_{m-1} \cdots \underline{A}_0] \begin{bmatrix} P_1 & \cdots & P_{M-m+1} \\ \vdots & \ddots & \vdots \\ P_m & \cdots & P_M \end{bmatrix} = [0 \dots 0] \tag{23}$$

and

$$[\overline{A}_m \dots \overline{A}_0] \begin{bmatrix} P_1 & \cdots & P_{M-m} \\ \vdots & \ddots & \vdots \\ P_{m+1} & \cdots & P_M \end{bmatrix} = [0 \dots 0]. \tag{24}$$

Consider first

$$\widehat{P} \triangleq \begin{bmatrix} P_1 & \cdots & P_{M-m} & P^{(1)}_{M-m+1} \\ \vdots & \ddots & \vdots & \vdots \\ P_m & \cdots & P_{M-1} & P^{(1)}_M \end{bmatrix} \in \mathbb{F}^{(n-k)m \times \delta} \tag{25}$$

where $\begin{bmatrix} P^{(1)}_{M-m+1} \\ \vdots \\ P^{(1)}_M \end{bmatrix}$ are the first $\delta - \left\lfloor \frac{\delta}{k} \right\rfloor k$ columns of $\begin{bmatrix} P_{M-m+1} \\ \vdots \\ P_M \end{bmatrix}$. Note that $\widehat{P}$ is completely determined by (17) and (20).

A parity-check matrix of the block code having the full rank matrix $\widehat{P}^\top$ as generator matrix, is a matrix with $(n-k)m$ columns and $(n-k)m - \delta = \underline{\delta}$ rows. Let $[\underline{A}_{m-1} \dots \underline{A}_0] \in \mathbb{F}^{\underline{\delta} \times (n-k)m}$ be such parity-check matrix, *i.e.*, $\mathrm{Im}_{\mathbb{F}} \widehat{P}^\top = \ker_{\mathbb{F}} [\underline{A}_{m-1} \dots \underline{A}_0]$.

Note that if we partition

$$\underline{A}_0 = [\underline{A}^{(1)}_0 \mid \underline{A}^{(2)}_0], \text{ with } \underline{A}^{(2)}_0 \in \mathbb{F}^{\underline{\delta} \times \underline{\delta}}, \tag{26}$$

then $\underline{A}^{(2)}_0$ is nonsingular as its determinant corresponds to a full size minor of the superregular matrix $\widehat{P}$, see for instance [10, Lemma A.1], [9] or [8].

Once $[\underline{A}_{m-1} \dots \underline{A}_0]$ is fixed (as being a parity-check matrix of the code with generator matrix $\widehat{P}$) and it satisfies the matrix equation

$$[\underline{A}_{m-1} \dots \underline{A}_0] \; \widehat{P} = 0,$$

we aim at deriving $\underline{P}^{(2)}_M$ such that (23) is also satisfied, *i.e.*, $\underline{P}^{(2)}_M$ must be defined such that

$$[\underline{A}_{m-1} \cdots \underline{A}_0] \begin{bmatrix} P^{(2)}_{M-m+1} \\ \vdots \\ P^{(2)}_M \end{bmatrix} = 0, \tag{27}$$

$$\text{with } P^{(2)}_M = \left[\begin{array}{c} \overline{P}^{(2)}_M \\ \hline \underline{P}^{(2)}_M \end{array} \right] \text{ and} \tag{28}$$

$\begin{bmatrix} P^{(2)}_{M-m+1} \\ \vdots \\ \overline{P}^{(2)}_M \end{bmatrix}$ are the last $\left(\left\lfloor \dfrac{\delta}{k} \right\rfloor + 1 \right) k - \delta$ columns of $\begin{bmatrix} P_{M-m+1} \\ \vdots \\ \overline{P}_M \end{bmatrix} \in \mathbb{F}^{\delta \times k}$.

Imposing conditions (27) and using the partitions (26) and (28), we can complete the undetermined part $\underline{P}_M^{(2)}$ of P_M as

$$\underline{P}_M^{(2)} \triangleq -(A_0^{(2)})^{-1} \cdot [\underline{A}_{m-1} \cdots \underline{A}_1 \ \underline{A}_0^{(1)}] \begin{bmatrix} P^{(2)}_{M-m+1} \\ \vdots \\ \overline{P}^{(2)}_M \end{bmatrix}, \tag{29}$$

in order to have that equation (23) holds.

Next, as $\underline{A}_0$ has full row rank, one can select $\overline{A}_0$ such that

$$A_0 = \begin{bmatrix} \overline{A}_0 \\ \underline{A}_0 \end{bmatrix} \tag{30}$$

is nonsingular.

Finally, the matrix equation (24) can be written as

$$\begin{bmatrix} \overline{A}_m & \cdots & \overline{A}_1 \end{bmatrix} \begin{bmatrix} P_1 & \cdots & P_{M-m} \\ \vdots & \ddots & \vdots \\ P_m & \cdots & P_{M-1} \end{bmatrix} = -\overline{A}_0 \begin{bmatrix} P_{m+1} & \cdots & P_M \end{bmatrix}. \tag{31}$$

This equation has at least one solution for the to-be-determined matrix

$$\begin{bmatrix} \overline{A}_m \cdots \overline{A}_1 \end{bmatrix}$$

as the matrix occurring in the left-hand side is an $m(n-k) \times (M-m)k$ superregular matrix that has full column rank since

$$m(n-k) = \left\lceil \frac{\delta}{n-k} \right\rceil (n-k) \geq \delta \geq \left\lfloor \frac{\delta}{k} \right\rfloor k = (M-m)k.$$

Therefore, so far, we have shown how to calculate the matrices A_i and P_i, for $i = 0, \ldots, m$. Matrices B_i can be subsequently computed via equation (22). Note that the resulting matrix $\underline{B}_m$ is zero as needed in the case we are considering.

Since A_0 is nonsingular, the matrix $\begin{bmatrix} A(D) & B(D) \end{bmatrix}$ has full rank. Therefore, the rate of $\mathcal{C}$ is k/n. To see that the degree is indeed δ, let $\widehat{\delta}$ be the degree of $\mathcal{C} = \ker H(D)$. Then, $\widehat{\delta}$ satisfies $\widehat{\delta} \leq \sum_{i=1}^{n-k} \delta_i$, where δ_i is the i-th row degree of $H(D)$. Due to the imposed structure on A_m and B_m, *i.e.*, $\underline{A}_m = 0$ and $\underline{B}_m = 0$, we also have that $\sum_{i=1}^{n-k} \delta_i \leq \delta$ and, therefore, $\widehat{\delta} \leq \delta$. On the other hand, since $(n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1$ is the Singleton bound for an (n, k, δ) code, it implies that $\mathcal{C}$ must have at least degree δ, *i.e.*, $\widehat{\delta} \geq \delta$. Thus, $\widehat{\delta} = \delta$, and the proof of the theorem is completed. □

Theorem 2 is equivalent to the main result presented in [11]. Unfortunately the proof in [11] gives no clues on how one can actually construct such sMDS codes with the MDP property. In contrast, our method gives a concrete construction of sMDS codes with maximum distance profile. The algorithm to construct such a code is summarized in the next subsection.

Constructive algorithm The following steps can be followed in order to derive matrices A_i and B_i that give rise to the desired sMDP code with maximum distance profile.

1. Select a superregular matrix T_M^c as in (16). For this task one can make use of the existing constructions of superregular matrices in [10, Example 3.10,(2)] and [2].
2. Take $P_i = T_i$, for $i \in \{0, \dots, L\}$, and P_M as in (20) with the sub-matrix $\underline{P}_M^{(2)}$ unknown.
3. Compute a minimal parity-check matrix of the code with generator matrix $\widehat{P}$ given in (25) to obtain $[\underline{A}_{m-1} \cdots \underline{A}_0]$.
4. Obtain the matrix $\underline{P}_M^{(2)}$ through equation (29) and, therefore, "completing" the matrix P_M.
5. Choose $\overline{A}_0$ such that the matrix in (30) is nonsingular. One can use, for instance, the elements of the canonical basis.
6. Solve the matrix equation (31) to obtain $[\overline{A}_m \cdots \overline{A}_1]$.
7. Compute the matrix $B(D)$ through equation (22).

Remark 3. Although the above algorithm gives a method to construct sMDS convolutional codes with maximum distance profile, it is important to note that the existing constructions of superregular matrices require large field sizes and that the construction of superregular matrices (Step 1) over small finite fields is still an open problem under investigation. Some conjectures and results on the size of the field required for the construction of superregular matrices are still unsolved [10, 13].

We illustrate the algorithm with an example.

Example 1. Let, for example, $(n, k, \delta) = (5, 2, 2)$. Then, $m = 1$, $M = 2$. We need to construct a parity-check matrix $H(D) \in \mathbb{F}[D]^{3\times 5}$.

1. We consider the superregular matrices described in [2] for building T_2^c as follows:

$$T_2^c \triangleq \left[\begin{array}{cc|cc|cc}
\alpha^{2^0} & \alpha^{2^1} & 0 & 0 & 0 & 0 \\
\alpha^{2^1} & \alpha^{2^2} & 0 & 0 & 0 & 0 \\
\alpha^{2^2} & \alpha^{2^3} & 0 & 0 & 0 & 0 \\
\hline
\alpha^{2^3} & \alpha^{2^4} & \alpha^{2^0} & \alpha^{2^1} & 0 & 0 \\
\alpha^{2^4} & \alpha^{2^5} & \alpha^{2^1} & \alpha^{2^2} & 0 & 0 \\
\alpha^{2^5} & \alpha^{2^6} & \alpha^{2^2} & \alpha^{2^3} & 0 & 0 \\
\hline
\alpha^{2^6} & \alpha^{2^7} & \alpha^{2^3} & \alpha^{2^4} & \alpha^{2^0} & \alpha^{2^1} \\
\alpha^{2^7} & \alpha^{2^8} & \alpha^{2^4} & \alpha^{2^5} & \alpha^{2^1} & \alpha^{2^2} \\
\alpha^{2^8} & \alpha^{2^9} & \alpha^{2^5} & \alpha^{2^6} & \alpha^{2^2} & \alpha^{2^3}
\end{array}\right],$$

where α is a primitive element of a field $\mathbb{F}$ of characteristic 2 and of size equal to or larger than 2^{512}.

2. Set

$$P_0 \triangleq \begin{bmatrix} \alpha^{2^0} & \alpha^{2^1} \\ \alpha^{2^1} & \alpha^{2^2} \\ \alpha^{2^2} & \alpha^{2^3} \end{bmatrix}, \quad P_1 \triangleq \begin{bmatrix} \alpha^{2^3} & \alpha^{2^4} \\ \alpha^{2^4} & \alpha^{2^5} \\ \alpha^{2^5} & \alpha^{2^6} \end{bmatrix}.$$

Since $\delta - \left\lfloor \frac{\delta}{k} \right\rfloor k = 0$,

$$P_2 \triangleq \left[\begin{array}{c} \overline{P}_2 \\ \hline \underline{P}_2 \end{array}\right] \triangleq \left[\, P_2^{(2)} \,\right] \triangleq \left[\begin{array}{c} \overline{P}_2^{(2)} \\ \hline \underline{P}_2^{(2)} \end{array}\right] \tag{32}$$

and then

$$\overline{P}_2 \triangleq \begin{bmatrix} \alpha^{2^6} & \alpha^{2^7} \\ \alpha^{2^7} & \alpha^{2^8} \end{bmatrix}, \; X = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \text{ and } P_2 = \begin{bmatrix} \alpha^{2^6} & \alpha^{2^7} \\ \alpha^{2^7} & \alpha^{2^8} \\ x_1 & x_2 \end{bmatrix},$$

where the variables x_1 and x_2 have to be computed.

3. To find a solution for the matrix equation (23), *i.e.*, to find $\underline{A}_0$ and the variables x_1 and x_2 in P_2 such that $\underline{A}_0 \begin{bmatrix} P_1 & P_2 \end{bmatrix} = 0$ is satisfied, we first compute $\underline{A}_0$ as the parity check matrix of $\hat{P}$ as in (25). For these parameters $\hat{P} = P_1$ and therefore

$$\underline{A}_0 = \begin{bmatrix} \alpha^{32} + \alpha^{40} & \alpha^{16} + \alpha^{24} + \alpha^{32} & 1 \end{bmatrix}.$$

4. Divide

$$\underline{A}_0 = \left[\begin{array}{c|c} \underline{A}_0^{(1)} & \underline{A}_0^{(2)} \end{array} \right] = \left[\begin{array}{cc|c} a_0 & a_1 & a_2 \end{array} \right]$$

to solve equation (29):

$$\begin{aligned} X = \begin{bmatrix} x_1 & x_2 \end{bmatrix} &= -a_2^{-1} \begin{bmatrix} a_0 \; a_1 \end{bmatrix} \begin{bmatrix} \alpha^{2^6} & \alpha^{2^7} \\ \alpha^{2^7} & \alpha^{2^8} \end{bmatrix} \\ &= \begin{bmatrix} \alpha^{96} + \alpha^{104} + \alpha^{144} + \alpha^{152} + \alpha^{160} & \alpha^{160} + \alpha^{168} + \alpha^{272} + \alpha^{280} + \alpha^{288} \end{bmatrix}. \end{aligned}$$

5. One can choose $\overline{A}_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ such that (30) holds.

6. To complete the values of the matrix $A(D)$ one needs to compute A_1 (or equivalently of $\overline{A}_1$) which is it done by solving the matrix equation (31):

$$\overline{A}_1 P_1 = -\overline{A}_0 P_2 \Rightarrow \overline{A}_1 = \begin{bmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \end{bmatrix},$$

which produces

$$\begin{aligned} y_1 &= \alpha^{104} + \alpha^{96} + \alpha^{88} + \alpha^{80} + \alpha^{72} + \alpha^{64}; \\ y_2 &= \alpha^{96} + \alpha^{88} + \alpha^{80} + \alpha^{72} + \alpha^{64} + \alpha^{56} + \alpha^{48}; \\ y_3 &= 0; \\ y_4 &= \alpha^{232} + \alpha^{224} + \alpha^{216} + \alpha^{208} + \alpha^{200} + \alpha^{192} + \alpha^{184} \\ &\quad + \alpha^{176} + \alpha^{168} + \alpha^{160} + \alpha^{152} + \alpha^{144} + \alpha^{136} + \alpha^{128}; \\ x_5 &= \alpha^{224} + \alpha^{216} + \alpha^{208} + \alpha^{200} + \alpha^{192} + \alpha^{184} + \alpha^{176} \\ &\quad + \alpha^{168} + \alpha^{160} + \alpha^{152} + \alpha^{144} + \alpha^{136} + \alpha^{128} + \alpha^{120} + \alpha^{112}; \\ y_6 &= 0. \end{aligned}$$

7. Finally, once we have obtained $A(D)$ one can easily compute $B(D) = B_0 + B_1 D$ by means of equation (22):

$$B_0 = \begin{bmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \\ b_0 & b_0' \end{bmatrix}$$

with $b_0 = \alpha^{41} + \alpha^{34} + \alpha^{33} + \alpha^{26} + \alpha^{18} + \alpha^4$ and $b_0' = \alpha^{42} + \alpha^{36} + \alpha^{34} + \alpha^{28} + \alpha^{20} + \alpha^8$, and

$$B_1 = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \\ 0 & 0 \end{bmatrix}$$

with

$$\begin{aligned}
b_1 &= \alpha^{105}+\alpha^{98}+\alpha^{97}+\alpha^{90}+\alpha^{89}+\alpha^{82}+\alpha^{81}+\alpha^{74}+\alpha^{73}+\alpha^{66}\\
&\quad+\alpha^{65}+\alpha^{58}+\alpha^{50}+\alpha^{8};\\
b_2 &= \alpha^{106}+\alpha^{100}+\alpha^{98}+\alpha^{92}+\alpha^{90}+\alpha^{84}+\alpha^{82}+\alpha^{76}+\alpha^{74}+\alpha^{68}\\
&\quad+\alpha^{66}+\alpha^{60}+\alpha^{52}+\alpha^{16};\\
b_3 &= \alpha^{233}+\alpha^{226}+\alpha^{225}+\alpha^{218}+\alpha^{217}+\alpha^{210}+\alpha^{209}+\alpha^{202}+\alpha^{201}+\alpha^{194}\\
&\quad+\alpha^{193}+\alpha^{186}+\alpha^{185}+\alpha^{178}+\alpha^{177}+\alpha^{170}+\alpha^{169}+\alpha^{162}+\alpha^{161}+\alpha^{154}\\
&\quad+\alpha^{153}+\alpha^{146}+\alpha^{145}+\alpha^{138}+\alpha^{137}+\alpha^{130}+\alpha^{129}+\alpha^{122}+\alpha^{114}+\alpha^{16};\\
b_4 &= \alpha^{234}+\alpha^{228}+\alpha^{226}+\alpha^{220}+\alpha^{218}+\alpha^{212}+\alpha^{210}+\alpha^{204}+\alpha^{202}+\alpha^{196}\\
&\quad+\alpha^{194}+\alpha^{188}+\alpha^{186}+\alpha^{180}+\alpha^{178}+\alpha^{172}+\alpha^{170}+\alpha^{164}+\alpha^{162}+\alpha^{156}\\
&\quad+\alpha^{154}+\alpha^{148}+\alpha^{146}+\alpha^{140}+\alpha^{138}+\alpha^{132}+\alpha^{130}+\alpha^{124}+\alpha^{116}+\alpha^{32}.
\end{aligned}$$

The resulting code

$$\begin{aligned}
\mathcal{C} &= \ker H(D) = \ker \begin{bmatrix} A(D) & B(D) \end{bmatrix}\\
&= \ker \begin{bmatrix} 1+y_1D & y_2D & 0 & \alpha+b_1D & \alpha^2+b_2D\\ y_4D & 1+y_5D & 0 & \alpha^2+b_3D & \alpha^4+b_4D\\ \alpha^{32}+\alpha^{40} & \alpha^{16}+\alpha^{24}+\alpha^{32} & 1 & b_0 & b_0' \end{bmatrix}
\end{aligned}$$

has rate $2/5$, degree 2 and is a sMDS $(5,2,2)$ code with maximum distance profile.

4. Conclusions

A great deal of attention has been devoted in recent years to two new classes of (n,k,δ) convolutional codes called MDP and sMDS due to their optimal distance properties. However, the question of how to construct them has remained open and only the case $(n-k) \mid \delta$ (the case where these two classes coincide) has been solved. In this paper we have filled this gap by presenting an effective method to construct sMDS (n,k,δ)-codes with maximum distance profile for any choice of the parameters (n,k,δ).

Acknowledgments

The authors would like to thank the reviewers for their valuable comments and suggestions that led to a much improved manuscript.

References

[1] A. K. Aidinyan, On matrices with nondegenerate square submatrices, *Probl. Peredachi Inf.*, **22** (1986), 106–108.

[2] P. Almeida, D. Napp and R. Pinto, A new class of superregular matrices and MDP convolutional codes, *Linear Algebra Appl.*, **439** (2013), 2145–2157.

[3] P. Almeida, D. Napp and R. Pinto, Superregular matrices and applications to convolutional codes, *Linear Algebra Appl.*, **499** (2016), 1–25.

[4] M. Arai, A. Yamamoto, A. Yamaguchi, S. Fukumoto and K. Iwasaki, Analysis of using convolutional codes to recover packet losses over burst erasure channels, in *Proc. 2001 Pacific Rim Int. Symp. Dependable Computing*, Washington, DC, 2001, p.258.

[5] J. J. Climent, D. Napp, C. Perea and R. Pinto, Maximum distance separable 2D convolutional codes, *IEEE Trans. Inf. Theory*, **62** (2016), 669–680.

[6] M. A. Epstein, Algebraic decoding for a binary erasure channel, Technical Report 340, MIT, 1958.

[7] S. Fashandi, S. O. Gharan and A. K. Khandani, Coding over an erasure channel with a large alphabet size, in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, 2008, 1053–1057.

[8] E. Fornasini and R. Pinto, Matrix fraction descriptions in convolutional codes, *Linear Algebra Appl.*, **392** (2004), 119–158.

[9] G. D. Forney, Jr., Structural analysis of convolutional codes via dual codes, *IEEE Trans. Inf. Theory*, **19** (1973), 512–518.

[10] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache, Strongly MDS convolutional codes, *IEEE Trans. Inf. Theory*, **52** (2006), 584–598.

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

[12] R. Hutchinson, J. Rosenthal and R. Smarandache, Convolutional codes with maximum distance profile, *Syst. Control Letters*, **54** (2005), 53–63.

[13] R. Hutchinson, R. Smarandache and J. Trumpf, On superregular matrices and MDP convolutional codes, *Linear Algebra Appl.*, **428** (2008), 2585–2596.

[14] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, New York, 1999.

[15] J. Lacan and J. Fimes, Systematic MDS erasure codes based on Vandermonde matrices, *IEEE Commun. Letters*, **8** (2004), 570–572.

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes II*, North-Holland Publishing Co., Amsterdam, 1977.

[17] R. J. McEliece, The algebraic theory of convolutional codes, in *Handbook of Coding Theory* (eds. V. Pless and W.C. Huffman), Elsevier, Amsterdam, 1998, 1065–1138.

[18] V. Paxson, End-to-end internet packet dynamics, *IEEE/ACM Trans. Netw.*, **7** (1999), 277–292.

[19] J. Rosenthal, Connections between linear systems and convolutional codes, in *Codes, Systems and Graphical Models* (eds. B. Marcus and J. Rosenthal), Springer-Verlag, 2001, 39–66.

[20] J. Rosenthal and R. Smarandache, Maximum distance separable convolutional codes, *Appl. Algebra Engrg. Comm. Comput.*, **10** (1999), 15–32.

[21] J. Rosenthal and E. V. York, BCH convolutional codes, *IEEE Trans. Inf. Theory*, **45** (1999), 1833–1844.

[22] R. M. Roth and A. Lempel, On MDS codes via Cauchy matrices, *IEEE Trans. Inf. Theory*, **35** (1989), 1314–1319.

[23] R. M. Roth and G. Seroussi, On generator matrices of MDS codes, *IEEE Trans. Inf. Theory*, **31** (1985), 826–830.

[24] V. Tomás, *Complete-MDP Convolutional Codes over the Erasure Channel*, Ph.D thesis, Univ. Alicante, Spain, 2010.

[25] V. Tomás, J. Rosenthal and R. Smarandache, Decoding of MDP convolutional codes over the erasure channel, in *Proc. 2009 IEEE Int. Symp. Inform. Theory*, Seoul, 2009, 556–560.

[26] V. Tomás, J. Rosenthal and R. Smarandache, Reverse-maximum distance profile convolutional codes over the erasure channel, in *Proc. 19th Int. Symp. Math. Theory Networks Systems – MTNS*, Budapest, 2010, 2121–2127.

[27] V. Tomás, J. Rosenthal and R. Smarandache, Decoding of convolutional codes over the erasure channel, *IEEE Trans. Inf. Theory*, **58** (2012), 90–108.

Received for publication January 2014.

E-mail address: diego@ua.pt
E-mail address: rsmarand@nd.edu