A new class of superregular matrices and MDP convolutional codes

P. Almeida[*,a], D. Napp[b], R. Pinto[a]

[a]CIDMA - Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Portugal.
[b]Departament de Matemàtiques Universitat Jaume I Campus de Riu Sec E-12071 Castelló de la Plana Espanya (Spain).

Abstract

This paper deals with the problem of constructing superregular matrices that lead to MDP convolutional codes. These matrices are a type of lower block triangular Toeplitz matrices with the property that all the square submatrices that can possibly be nonsingular due to the lower block triangular structure are nonsingular. We present a new class of matrices that are superregular over a sufficiently large finite field $\mathbb{F}$. Such construction works for any given choice of characteristic of the field $\mathbb{F}$ and code parameters (n, k, δ) such that $(n-k)|\delta$. We also discuss the size of $\mathbb{F}$ needed so that the proposed matrices are superregular.

1. Introduction

In recent years, renewed efforts have been made to further analyze the distance properties of convolutional codes [2, 4, 5, 6, 9, 13, 14, 15]. Convolutional codes with the maximum possible distance (for a given choice of parameters) are called maximum distance separable (MDS). However, for error control purposes it is also important to consider codes with large column distances.

The convolutional codes whose column distances increase as rapidly as possible for as long as possible are called maximum distance profile (MDP) codes. These codes are specially appealing for the performance of sequential decoding algorithms as they have the potential to have a maximum number of errors corrected per time interval. In [10] a non-constructive proof of the existence of such codes (for all transmission rates and all degrees) was given. However, the problem of how to construct MDP codes is far from being solved and very little is known about the minimum field size required for doing so. It turns out that this issue has been connected to the construction of a particular type of *superregular* matrices. In [2] a concrete construction of superregular matrices is given for all parameters (n, k, δ) although over a field with a large characteristic and size. In [6] the size of the field needed to have a superregular matrix is studied. They provide a bound on this size and conjecture the existence of a much tighter bound based on examples and computer searches.

In this paper, we will address these issues and present a new class of matrices that are superregular over a sufficiently large finite field $\mathbb{F}$ of any characteristic. We also provide a bound on the required field size needed for such matrices to be superregular.

*Corresponding author

2. Preliminaries: MDP convolutional codes and superregular matrices

In this section, we recall basic material from the theory of convolutional codes that is relevant to the presented work and link it to the notion of superregular matrices.

Let $\mathbb{F}$ be a finite field and $\mathbb{F}[z]$ the ring of polynomials with coefficients in $\mathbb{F}$. A **convolutional code** $\mathcal{C}$ of rate k/n is a $\mathbb{F}[z]$-submodule of $\mathbb{F}[z]^n$ of rank k of the form

$$\mathcal{C} = \mathrm{im}_{\mathbb{F}[z]} G(z) = \{G(z)u(z) : \ u(z) \in \mathbb{F}^k[z]\},$$

where $G(z) \in \mathbb{F}[z]^{n\times k}$ is a right-invertible matrix over $\mathbb{F}[z]$. For every convolutional code $\mathcal{C}$ there exists a matrix, called the parity check matrix, $H(z) \in \mathbb{F}[z]^{(n-k)\times n}$ such that

$$\mathcal{C} = \ker_{\mathbb{F}[z]} H(z) = \{v(z) \in \mathbb{F}[z]^n : \ H(z)v(z) = 0\}. \tag{1}$$

The *degree* of $\mathcal{C}$, denoted by δ, is defined as the maximum degree of the full size minors of $G(z)$. Note that we can also choose $H(z)$ to be left invertible over $\mathbb{F}[z]$, and in this case δ will also be equal to the maximum degree of the full size minors of $H[z]$. A convolutional code of rate k/n and degree δ is called an (n, k, δ) convolutional code.

The most important property of a code is its distance, defined as follows: The weight of a polynomial vector $v(z) = \sum_{i\in\mathbb{N}} v_i z^i \in \mathbb{F}[z]^n$ is given by $\mathrm{wt}(v) = \sum_{i\in\mathbb{N}} \mathrm{wt}(v_i)$, where $\mathrm{wt}(v_i)$ is the number of nonzero elements of v_i. The **distance** of a convolutional code $\mathcal{C}$ is defined as

$$\mathrm{d}(\mathcal{C}) = \min\{\mathrm{wt}(v(z)) \,|\, v(z) \in \mathcal{C}, v(z) \neq 0\}.$$

If $\mathcal{C} = \ker_{\mathbb{F}[z]} H(z)$, where $H(z) = \sum_{i=0}^{\nu} H_i z^i$, for some $\nu \in \mathbb{N}$, then the j-th **column distance** of $\mathcal{C}$ is defined as

$$\begin{aligned} d_j^c(\mathcal{C}) &= \min\{wt(v_{[0,j]}) = wt(v_0 + v_1 z + \cdots + v_j z^j) : \ v(z) = \sum_{i\in\mathbb{N}} v_i z^i \in \mathcal{C} \text{ and } \ v_0 \neq 0\} \\ &= \min\{wt(\vec{v}_j) : \vec{v}_j = [v_0 \dots v_j] \in \mathbb{F}^{(j+1)n}, \mathcal{H}(H_0, \dots, H_j)\vec{v}_j^{\top} = 0, v(z) = \sum_{i\in\mathbb{N}} v_i z^i \in \mathcal{C}, v_0 \neq 0\}. \end{aligned}$$

where

$$\mathcal{H}(H_0, \dots, H_j) = \begin{pmatrix} H_0 & 0 & 0 & \cdots & 0 \\ H_1 & H_0 & 0 & \cdots & 0 \\ H_2 & H_1 & H_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ H_j & H_{j-1} & \cdots & \cdots & H_0 \end{pmatrix} \in \mathbb{F}^{(j+1)(n-k)\times(j+1)n}, \tag{2}$$

and $H_j = 0$ for $j > \nu$.

In this paper we focus on this important notion of column distance. This notion is closely related to the notion of optimum distance profile (ODP), see [7, pp.112]. The following results about column distances are proved in [2].

Proposition 2.1. *Let $\mathcal{C}$ be an (n, k, δ) convolutional code and $L = \lfloor \delta/k \rfloor + \lfloor \delta/(n-k) \rfloor$. Then*

i) $d_j^c(\mathcal{C}) \leq (j+1)(n-k)+1$, $\forall j \in \mathbb{N}_0$;

ii) if there exists $j \leq L$ such that $d_j^c(\mathcal{C}) = (j+1)(n-k)+1$, then $d_i^c(\mathcal{C}) = (i+1)(n-k)+1$, for all $i \leq j$.

A convolutional code $\mathcal{C}$ is called **maximum distance profile** (**MDP**) if its column distances achieve the maximum possible values (for a given choice of parameters), *i. e.*, if $\mathcal{C}$ has rate k/n and degree δ, then $d_L^c(\mathcal{C}) = (L+1)(n-k)+1$, for $L = \lfloor \delta/k \rfloor + \lfloor \delta/(n-k) \rfloor$ and so $d_j^c(\mathcal{C}) = (j+1)(n-k)+1$, for $j \leq L$. In order to characterize MDP codes we need to introduce the notion of superregular matrices.

Let $A = [\mu_{ij}]$ be a square matrix of order m over $\mathbb{F}$ and S_m the symmetric group of order m. Recall that the determinant of A is given by

$$|A| = \sum_{\sigma \in S_m} (-1)^{\mathrm{sgn}(\sigma)} \mu_{1\sigma(1)} \cdots \mu_{m\sigma(m)}. \tag{3}$$

Whenever we use the word *term*, we will be considering one product of the form $\mu_{1\sigma(1)} \cdots \mu_{m\sigma(m)}$, with $\sigma \in S_m$, and the word *component* will be reserved to refer to each of the $\mu_{i\sigma(i)}$, with $1 \leq i \leq m$, in a term.

A *trivial term* of the determinant is a term of (3), $\mu_{1\sigma(1)} \cdots \mu_{m\sigma(m)}$, such that exists $1 \leq i \leq m$ with $\mu_{i\sigma(i)} = 0$. If A is a square submatrix of a matrix B, with entries in $\mathbb{F}$, and all the terms of the determinant of A are trivial we say that $|A|$ is a **trivial minor** of B. We say that B is **superregular** if all its non-trivial minors are different from zero.

It is important to remark here that there exist several related, but different, notions of superregular matrices in the literature. Unfortunately, all these notions are only particular cases of the more general definition given above. Frequently, see for instance [11], a superregular matrix is defined to be a matrix for which every square submatrix is nonsingular. Obviously all the entries of these matrices must be nonzero. Also, in [1, 8, 12], several examples of triangular matrices were constructed in such a way that all submatrices inside this triangular configuration were nonsingular. However, all these notions do not apply to our case as they do not consider submatrices that contain zeros. The more recent contributions [2, 4, 6, 14, 15] consider the same notion of superregularity as us, but defined only for lower triangular matrices.

Next theorem shows how MDP (n, k, δ) convolutional codes with $(n-k)|\delta$ can be characterized by superregular matrices (see [2, Theorem 3.1]).

Theorem 2.1. *Let $\mathcal{C}$ be an (n, k, δ) convolutional code such that $(n-k)|\delta$ and represented as*

$$\mathcal{C} = \ker_{\mathbb{F}[z]}[A(z)\ B(z)],$$

where $A(z) = \sum_{i=0}^{\nu} A_i z^i \in \mathbb{F}[z]^{(n-k)\times(n-k)}$, $B(z) = \sum_{i=0}^{\nu} B_i z^i \in \mathbb{F}[z]^{(n-k)\times k}$ and $\nu = \frac{\delta}{(n-k)}$. We can assume without lost of generality that $A_0 = I_{n-k}$. Furthermore, let

$$A(z)^{-1}B(z) = \sum_{i=0}^{\infty} \bar{H}_i z^i \in \mathbb{F}((z))^{(n-k)\times k}$$

be the Laurent expansion of $A(z)^{-1}B(z)$ over the field $\mathbb{F}((z))$ of Laurent series. Define $L = \lfloor \delta/k \rfloor + \delta/(n-k)$ and

$$\widehat{\bar{H}} = [I_{(L+1)(n-k)}\ \bar{\mathcal{H}}(\bar{H}_0, \ldots, \bar{H}_L)] \text{ where}$$

$$\bar{\mathcal{H}}(\bar{H}_0, \ldots, \bar{H}_L) = \begin{pmatrix} \bar{H}_0 & 0 & 0 & \cdots & 0 \\ \bar{H}_1 & \bar{H}_0 & 0 & \cdots & 0 \\ \bar{H}_2 & \bar{H}_1 & \bar{H}_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \bar{H}_L & \bar{H}_{L-1} & \cdots & \cdots & \bar{H}_0 \end{pmatrix} \in \mathbb{F}^{(L+1)(n-k)\times(L+1)k}. \tag{4}$$

The following are equivalent:

1. $\mathcal{C}$ *is MDP.*
2. $\bar{\mathcal{H}}(\bar{H}_0, \ldots, \bar{H}_L)$ *is superregular.*

Hence, the problem of constructing an MDP convolutional code relies on the problem of constructing superregular lower block triangular Toeplitz matrices of the form (4). This problem is addressed in the next section.

For the case where $(n-k) \nmid \delta$, similar results were obtained using different methods from systems theory, see [4, 5, 6] for more details. We will not consider this case in this paper.

3. A new class of MDP codes and superregular matrices

In this section, we introduce a new class of matrices of the form (4) and show that they are superregular matrices over a sufficiently large field $\mathbb{F}$. First, we recall previous contributions on superregular matrices.

It is a common practice in building the matrix $\bar{\mathcal{H}}(\bar{H}_0, \ldots, \bar{H}_L)$ of Theorem 2.1 to first construct a large lower triangular superregular matrix in such a way that it contains the lower block triangular Toeplitz matrix $\bar{\mathcal{H}}(\bar{H}_0, \ldots, \bar{H}_L)$ as a submatrix. In [2], it was shown that for every positive integer r there exists a prime $p = p(r)$ such that

$$S_r = \begin{pmatrix} \binom{r-1}{0} & 0 & 0 & \cdots & 0 \\ \binom{r-1}{1} & \binom{r-1}{0} & 0 & \cdots & 0 \\ \binom{r-1}{2} & \binom{r-1}{1} & \binom{r-1}{0} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \binom{r-1}{r-1} & \binom{r-1}{r-2} & \cdots & \cdots & \binom{r-1}{0} \end{pmatrix} \tag{5}$$

is superregular over $\mathbb{F}_p$. Moreover, the authors proposed the first rough bound on the size of a field $\mathbb{F}$ for a lower triangular Toeplitz matrix A to be superregular over $\mathbb{F}$. Namely if we consider c to be the largest magnitude among the entries of A and if $|\mathbb{F}| > c^r r^{r/2}$, then there exists a superregular lower triangular Toeplitz matrix $A \in \mathbb{F}^{r \times r}$. Later, in [6], the following more refined bound was presented: If $|\mathbb{F}| > B_r$ then there exists a superregular lower triangular Toeplitz matrix $A \in \mathbb{F}^{r \times r}$, where

$$B_r = \frac{1}{2}\left(\frac{1}{r}\binom{2(r-1)}{r-1} + \binom{r-1}{\lfloor \frac{r-1}{2} \rfloor}\right). \tag{6}$$

Moreover, based on examples and computer searches, it was conjectured in [2, 6] that for $\ell \geq 5$ there exists a superregular lower triangular Toeplitz matrix of order ℓ over the field $\mathbb{F}_{2^{\ell-2}}$. If true, it would considerably improve the bound given above. This remains an open problem.

We propose a new type of superregular matrices with the form of (4). Of course, this will bring about a new class of MDP codes. Let (n, k, δ) be given such that $(n-k)|\delta$. Let $M = \max\{n-k, k\}$

and $L = \lfloor \delta/k \rfloor + \delta/(n-k)$. Let α be a primitive element of a finite field $\mathbb{F} = \mathbb{F}_{p^N}$ and define

$$[T_0|\ T_1\ |\dots\ |T_L] =$$
$$= \left[\begin{array}{cccc|ccc|c|ccc} \alpha^{2^0} & \alpha^{2^1} & \cdots & \alpha^{2^{M-1}} & \alpha^{2^M} & \cdots & \alpha^{2^{2M-1}} & & \alpha^{2^{ML}} & \cdots & \alpha^{2^{M(L+1)-1}} \\ \alpha^{2^1} & \alpha^{2^2} & \cdots & \alpha^{2^M} & \alpha^{2^{M+1}} & \cdots & \alpha^{2^{2M}} & & \alpha^{2^{ML+1}} & \cdots & \alpha^{2^{M(L+1)}} \\ \alpha^{2^2} & \alpha^{2^3} & \cdots & \alpha^{2^{M+1}} & \alpha^{2^{M+2}} & \cdots & \alpha^{2^{2M+1}} & \cdots & \alpha^{2^{ML+2}} & \cdots & \alpha^{2^{M(L+1)+1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ \alpha^{2^{M-1}} & \alpha^{2^M} & \cdots & \alpha^{2^{2M-2}} & \alpha^{2^{2M-1}} & \cdots & \alpha^{2^{3M-2}} & & \alpha^{2^{M(L+1)-1}} & \cdots & \alpha^{2^{M(L+2)-2}} \end{array}\right]. \quad (7)$$

Define also, $\mathcal{T}(T_0, T_1, \dots, T_L) \in \mathbb{F}^{(L+1)M \times (L+1)M}$ by

$$\mathcal{T}(T_0, \dots, T_L) = \begin{pmatrix} T_0 & 0 & 0 & \cdots & 0 \\ T_1 & T_0 & 0 & \cdots & 0 \\ T_2 & T_1 & T_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ T_L & T_{L-1} & \cdots & \cdots & T_0 \end{pmatrix}. \quad (8)$$

We are going to prove that if N is sufficiently large then $\mathcal{T}(T_0, T_1, \dots, T_L)$ is superregular. First, we need the following well known result.

Theorem 3.1 ([3]). *Let $\mathbb{F}$ be a finite field with p^N elements. Let α be a primitive element of $\mathbb{F}$ and $\rho(z)$ be the minimal polynomial of α (*i. e., *$\mathbb{F} = \mathbb{F}_p[z]/(\rho(z))$ and deg $\rho(z) = N$). If $f(z) \in \mathbb{F}_p[z]$ with $f(\alpha) = 0$ then $\rho(z) \mid f(z)$.*

Theorem 3.2. *Let $L, M \in \mathbb{N}$, α be a primitive element of a finite field $\mathbb{F}$ of characteristic p, $\rho(z)$ be the minimal polynomial of α and consider $\mathcal{T}(T_0, T_1, \dots, T_L) \in \mathbb{F}^{(L+1)M \times (L+1)M}$. If $|\mathbb{F}| \geq p^{(2^{M(L+2)-1})}$ then the matrix $\mathcal{T}(T_0, T_1, \dots, T_L)$ is superregular (over $\mathbb{F}$).*

Proof: Let $[t_{L1}\ \cdots\ t_{LM}|\cdots|t_{11}\ \cdots\ t_{1M}|t_{01}\ \cdots\ t_{0M}]$ denote the columns of $\mathcal{T}(T_0, \dots, T_L)$ and define $\overline{\mathcal{T}}(T_0, \dots, T_L) = [t_{01}\ \cdots\ t_{0M}|t_{11}\ \cdots\ t_{1M}|\cdots|t_{L1}\ \cdots\ t_{LM}]$, *i. e.*, set

$$\overline{\mathcal{T}}(T_0, \dots, T_L) =$$
$$\left[\begin{array}{ccc|c|ccc|ccc} 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \alpha^{2^0} & \cdots & \alpha^{2^{M-1}} \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \alpha^{2^1} & \cdots & \alpha^{2^M} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & \alpha^{2^{M-1}} & \cdots & \alpha^{2^{2M-2}} \\ \hline 0 & \cdots & 0 & \cdots & \alpha^{2^0} & \cdots & \alpha^{2^{M-1}} & \alpha^{2^M} & \cdots & \alpha^{2^{2M-1}} \\ 0 & \cdots & 0 & \cdots & \alpha^{2^1} & \cdots & \alpha^{2^M} & \alpha^{2^{M+1}} & \cdots & \alpha^{2^{2M}} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & \alpha^{2^{M-1}} & \cdots & \alpha^{2^{2M-2}} & \alpha^{2^{2M-1}} & \cdots & \alpha^{2^{3M-2}} \\ \hline \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \hline \alpha^{2^0} & \cdots & \alpha^{2^{M-1}} & \cdots & \alpha^{2^{M(L-1)}} & \cdots & \alpha^{2^{ML-1}} & \alpha^{2^{ML}} & \cdots & \alpha^{2^{M(L+1)-1}} \\ \alpha^{2^1} & \cdots & \alpha^{2^M} & \cdots & \alpha^{2^{M(L-1)+1}} & \cdots & \alpha^{2^{ML}} & \alpha^{2^{ML+1}} & \cdots & \alpha^{2^{M(L+1)}} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{2^{M-1}} & \cdots & \alpha^{2^{2M-2}} & \cdots & \alpha^{2^{ML-1}} & \cdots & \alpha^{2^{M(L+1)-2}} & \alpha^{2^{M(L+1)-1}} & \cdots & \alpha^{2^{M(L+2)-2}} \end{array}\right].$$

We show that $\overline{\mathcal{T}}(T_0,\ldots,T_L)$ is superregular. Obviously, this readily implies that $\mathcal{T}(T_0,\ldots,T_L)$ is superregular as well.

Let $A=[\mu_{ij}]$ be a square submatrix of $\overline{\mathcal{T}}(T_0,\ldots,T_L)$ of size $m\leq M(L+1)$, such that $|A|$ is a nontrivial minor of $\overline{\mathcal{T}}(T_0,\ldots,T_L)$.

If $\mu_{ij}\neq 0$ then μ_{ij} is a power of α. Let $\nu_{ij}\in\mathbb{N}$ such

$$\alpha^{\nu_{ij}}=\mu_{ij}.$$

Note that each term of the determinant of A given by (3) is zero or a power of α. Given $\sigma\in S_m$ such that $\mu_{1\sigma(1)}\cdots\mu_{m\sigma(m)}\neq 0$, let ν_σ such that

$$\alpha^{\nu_\sigma}=\mu_{1\sigma(1)}\cdots\mu_{m\sigma(m)}.$$

Consider $m>1$ otherwise the proof is trivial. First we show that the exponents of α appearing in any nontrivial term of $|A|$ are all smaller than $2^{M(L+2)-1}$.

From the particular structure of the matrix $\overline{\mathcal{T}}(T_0,\ldots,T_L)$, it follows that

$$2\nu_{ij'}\leq\nu_{ij}\quad\text{and}\quad 2\nu_{i'j}\leq\nu_{ij}\quad\text{if}\quad i'<i\quad\text{and}\quad j'<j. \tag{9}$$

Let $\sigma\in S_m$ and suppose $\mu_{1\sigma(1)}\mu_{2\sigma(2)}\cdots\mu_{m\sigma(m)}\neq 0$. Define

$$R_k=\{(i,j)\in\mathbb{N}^2\mid 1\leq i,j\leq k\text{ and }i=k\text{ or }j=k\}$$

and

$$R(\sigma)=\{(i,j)\in\mathbb{N}^2\mid (i,j)=(t,\sigma(t))\text{ for some }t\in\{1,2,\ldots,m\}\}.$$

It follows from (9) that

$$\sum_{(i,j)\in R_k\cap R(\sigma)}\nu_{ij}\leq 2^{M(L+2)-2(m-k+1)}$$

for $1\leq k\leq m$. Hence,

$$\begin{aligned}\nu_\sigma &= \sum_{k=1}^{m}\sum_{(i,j)\in R_k\cap R(\sigma)}\nu_{ij}\leq 2^{M(L+2)-2}+2^{M(L+2)-4}+\cdots 2^{M(L+2)-2m}\\ &< 2^{M(L+2)-2}\sum_{i=0}^{\infty}4^{-i}\\ &= 2^{M(L+2)-2}\frac{4}{3}\\ &< 2^{M(L+2)-1}.\end{aligned}$$

So the exponent of α on any nonzero term is smaller than $2^{M(L+2)-1}$. Next, we will prove the following result:

> Statement 1: If there are nontrivial terms, then there exists a *unique* term α^β with highest exponent β.

Since $\rho(z)$ has degree greater than β, if Statement 1 holds true then the uniqueness of β will imply that $|A|=f(\alpha)=\pm\alpha^\beta+\gamma(\alpha)$, where $\gamma(z)$ is a polynomial of degree smaller than β. This would immediately imply that $|A|\neq 0$ since otherwise, by theorem 3.1, one would have that $\rho(z)\mid f(z)$, which contradicts the fact that the degree o $f(z)$ is less than $2^{M(L+2)-1}$. Therefore, we will obtain that $\overline{\mathcal{T}}(T_0,\ldots,T_L)$ is superregular, which will conclude the proof.

The idea of the proof of Statement 1 is to define recursively a permutation $\overline{\sigma}$ of S_m such that the corresponding term will have the highest exponent. We will show that, whenever possible, $\overline{\sigma}(m) = m$, *i. e.*, the term defined by $\overline{\sigma}$ contains the component at the bottom-right corner, namely μ_{mm}. However, this is not always possible as the terms corresponding to permutations σ, with $\sigma(m) = m$, can all be zero. For this reason, we divide our proof in two cases. First we study the case when it is possible to have a nontrivial term, where the corresponding permutation σ satisfies $\sigma(m) = m$, and we prove that, for any term $\alpha^{\widehat{\beta}}$ without this property, there is one term with this property which has an exponent of α larger than $\widehat{\beta}$. In the second case, all the terms having $\sigma(m) = m$ are trivial, so we construct a new matrix A' of size $l < m$ having the last l rows and the first l columns of the matrix A and where it is possible to have a nontrivial term of $|A'|$ with the associated permutation σ satisfying $\sigma(l) = l$. We then use the first case to get $\overline{\sigma}(m) = l$.

After establishing the value of $\overline{\sigma}(m)$ we construct a submatrix A_1 of A obtained by the elimination of the last row and the $\overline{\sigma}(m)$ column of A and repeat the process for the matrix A_1, obtaining the value of $\overline{\sigma}(m-1)$. Proceeding in this way, we recursively define a sequence of matrices $A_0 = A, A_1, \dots A_{m-1}$ where, for each $0 \leq i \leq m-1$, A_i is a square matrix of size $m-i$ and, using cases 1 or 2 applied to the matrix A_i, we define $\overline{\sigma}(m-i)$. Thus, we define a unique permutation $\overline{\sigma}$ whose corresponding term has the highest exponent.

As the construction of a new permutation in the first case is hard to follow, we will illustrate the process with an example.

Write A as a block matrix in the following form

$$A = \left[\begin{array}{ccc|c} & O_1 & & \\ \hline & O_2 & & \\ \hline & \vdots & & B_1 \\ \hline O_h & & \cdots & \\ \hline B_h & & & \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ \\ B_0 \end{array}\right], \tag{10}$$

where, for each $1 \leq i \leq h$, O_i is a null matrix with l_i columns and, for each $0 \leq j \leq h$, B_j is a matrix with k_j rows and no entry equal to zero. We have $l_1 > \cdots > l_h$ and $m = k_0 > k_1 > \cdots > k_h$. The minor $|A|$ being nontrivial means that we cannot have a row with more zeros than the number of rows below it. Therefore, we have $k_i \geq l_i$ for any $1 \leq i \leq h$.

If $h = 0$ then $A = B_0$ and all entries of A are nonzero. Note that if all the elements just above the main antidiagonal of A are zero (*i. e.*, $k_i = l_i$ for all $1 \leq i \leq h$) then there exists a unique term of $|A|$ which is nonzero, namely, the one constituted by the elements of the main antidiagonal of A and therefore μ_{mm} is not a component in such a term. Moreover, if any $k_i = l_i$, for some $1 \leq i \leq h$, then, the components that correspond to the first l_i columns of a nontrivial term of $|A|$ must be selected within the last k_i rows, *i. e.* we must have $\sigma(j) \leq l_i$, for $j \in \{m - l_i + 1, \cdots, m\}$ and consequently, we cannot have $\sigma(m) = m$. Roughly speaking, in this case, to obtain a nontrivial term of $|A|$ we are *forced* to pick up l_i of its components in the $l_i \times l_i$ submatrix of A located in the lower left corner.

Let us denote the highest possible exponent in α of a nontrivial term of $|A|$ as

$$\beta = \max_{b \in \mathbb{N}} \{b : \alpha^b = \mu_{1\sigma(1)} \cdots \mu_{m\sigma(m)}, \text{ for some } \sigma \in S_m\}.$$

Thus, it is enough to show that there is a unique $\overline{\sigma} \in S_m$ such that

$$\alpha^\beta = \mu_{m\overline{\sigma}(m)} \mu_{m-1\overline{\sigma}(m-1)} \cdots \mu_{1\overline{\sigma}(1)}. \tag{11}$$

Let $\sigma \in S_m$ such that $\alpha^\beta = \mu_{1\sigma(1)} \cdots \mu_{m\sigma(m)}$ then the following statements are true:

Case 1: If $h = 0$ or $l_i < k_i$ for any $1 \leq i \leq h$, then $\sigma(m) = m$.

Case 2: If $l_i = k_i$ for some $i \in \{1, \ldots, h\}$, then $\sigma(m) = l_{\overline{i}}$, where $\overline{i}$ is the maximum $i \in \{1, \ldots, h\}$ such that $l_i = k_i$.

Note that, by the way β is defined, it could be the exponent of α of more than one term. We prove that, whenever one permutation does not satisfy the conditions in cases 1 and 2, then the corresponding term will have an exponent of α smaller than β. Therefore, we will be able to prove that only one permutation $\overline{\sigma}(m)$, defined recursively by the conditions in cases 1 and 2, satisfies (11).

Proof Case 1: First we are going to prove that if $h = 0$ or $l_i < k_i$ for all $1 \leq i \leq h$, then the entries of A just above the main antidiagonal are nonzero, *i. e.*,

$$\mu_{(m-i)i} \neq 0 \quad \text{for any} \quad i \in \{1, \ldots, m-1\}. \tag{12}$$

If $h = 0$ then all entries of A are nonzero, in particular $\mu_{(m-i)i} \neq 0$ for any $1 \leq i \leq m-1$.

Now, suppose $l_j < k_j$ for all $1 \leq j \leq h$. If, for some $i \in \{1, \ldots, m-1\}$, we have $\mu_{(m-i)i} = 0$ then there exists $j \in \{1, \ldots, h\}$ such that $l_j \geq i$, but then $k_j \leq m - (m-i)$, so $k_j \leq l_j$ which contradicts our hypothesis. Therefore, we obtain (12).

Take $\widehat{\sigma} \in S_m$ with

$$\mu_{m\widehat{\sigma}(m)}\mu_{m-1\widehat{\sigma}(m-1)} \cdots \mu_{1\widehat{\sigma}(1)} \neq 0,$$

and $\mu_{m\widehat{\sigma}(m)} \neq \mu_{mm}$. Such a permutation always exists, because, for example, the elements of the antidiagonal are nonzero, i. e. $\mu_{i(m-i+1)} \neq 0$ for $1 \leq i \leq m$.

Let $\nu_{\widehat{\sigma}} \in \mathbb{N}$, such that

$$\alpha^{\nu_{\widehat{\sigma}}} = \mu_{m\widehat{\sigma}(m)}\mu_{m-1\widehat{\sigma}(m-1)} \cdots \mu_{1\widehat{\sigma}(1)}.$$

We prove the statement of Case 1 by constructing a permutation $\widetilde{\sigma} \in S_m$, obtained from $\widehat{\sigma}$ by multiplying $\widehat{\sigma}$ by a product of transpositions, with the following properties

1. $\widetilde{\sigma}(m) = m$;
2. $\mu_{i\widetilde{\sigma}(i)} \neq 0$, for any $1 \leq i \leq m$;
3. The exponent of the term corresponding to $\widetilde{\sigma}$ is larger than the exponent of the term corresponding to $\widehat{\sigma}$.

We start by giving some intuition of how the permutation $\widetilde{\sigma}$ is obtained, then we formally construct $\widetilde{\sigma}$ satisfying the three properties mentioned above, and in the end, we illustrate this construction with an example.

Suppose that $\widehat{\sigma}(m) = j$ and $\widehat{\sigma}(i_1) = m$ with $1 \leq i_1, j \leq m-1$, if $\mu_{i_1 j} \neq 0$ (this always happens if $h = 0$) then it is enough to take $\widetilde{\sigma} = \widehat{\sigma} \cdot (jm)$, where (jm) is the transposition that takes j to m and m to j . That is, $\widetilde{\sigma}$ is defined by

1. $\widetilde{\sigma}(m) = m$;
2. $\widetilde{\sigma}(i_1) = j$;
3. $\widetilde{\sigma}(k) = \widehat{\sigma}(k)$, for any $k \neq m$ and $k \neq i_1$.

But if $\mu_{i_1 j} = 0$, then we define $\widetilde{\sigma}(i_1) = \delta_1$, for a chosen $\delta_1 \geq m - i_1$ (so that $\mu_{i_1\delta_1} \neq 0$, by (12)) and for i_2 defined by $\widehat{\sigma}(i_2) = \delta_1$, we check if $\mu_{i_2 j}$ is different from zero, in which case, we define $\widetilde{\sigma} = \widehat{\sigma} \cdot (jm)(\delta_1 j)$. If $\mu_{i_2 j} = 0$, then we proceed in a similar manner obtaining in the end

$$\widetilde{\sigma} = \widehat{\sigma} \cdot (jm)(\delta_r \delta_{r-1})(\delta_{r-1}\delta_{r-2}) \cdots (\delta_2\delta_1)(\delta_1 j), \tag{13}$$

for some $r \leq m$.

Formally, we construct $\widetilde{\sigma} \in S_m$ recursively, as follows:
Define $\delta_0 = m$ and while $\mu_{\widehat{\sigma}^{-1}(\delta_i)\widehat{\sigma}(m)} = 0$, define

$$\delta_{i+1} = \widehat{\sigma}\left(\max_{j \geq m - \widehat{\sigma}^{-1}(\delta_i)} \widehat{\sigma}^{-1}(j)\right),$$

and let r be the first integer such that $\mu_{\widehat{\sigma}^{-1}(\delta_r)\widehat{\sigma}(m)} \neq 0$. The permutation $\widetilde{\sigma} \in S_m$ will be defined by the following

1. $\widetilde{\sigma}(m) = m$ and $\widetilde{\sigma}(\widehat{\sigma}^{-1}(\delta_r)) = \widehat{\sigma}(m)$;
2. For $0 \leq i < r$, $\widetilde{\sigma}(\widehat{\sigma}^{-1}(\delta_i)) = \delta_{i+1}$;
3. For $i \notin I = \{\widehat{\sigma}^{-1}(\delta_i) \mid 0 \leq i \leq r\}$, $\widetilde{\sigma}(i) = \widehat{\sigma}(i)$.

By definition, $\widehat{\sigma}^{-1}(\delta_{i+1})$ is the maximum of $\widehat{\sigma}^{-1}(\delta_i) + 1$ values, so since we cannot have two components of a term in the same row, we must have $\widehat{\sigma}^{-1}(\delta_{i+1}) > \widehat{\sigma}^{-1}(\delta_i)$. So,

$$\nu_{m\widehat{\sigma}(m)} + \sum_{i=1}^{r} \nu_{\widehat{\sigma}^{-1}(\delta_i)\delta_i} \leq \sum_{i=0}^{r} \nu_{(m-i)\,(m-r+i)}.$$

By (9), we have

$$\nu_{(m-i)\,(m-r+i)} \leq 2^{-i} 2^{-r+i} \nu_{mm},$$

then

$$\nu_{m\widehat{\sigma}(m)} + \sum_{i=1}^{r} \nu_{\widehat{\sigma}^{-1}(\delta_i)\delta_i} \leq \sum_{i=0}^{r} 2^{-r} \nu_{mm} \leq \nu_{mm}.$$

Therefore

$$\begin{aligned}
\nu_{\widehat{\sigma}} &= \sum_{i \in I} \nu_{i\widehat{\sigma}(i)} + \sum_{i \notin I} \nu_{i\widehat{\sigma}(i)} \\
&\leq \nu_{mm} + \sum_{i \notin I \cup \{m\}} \nu_{i\widehat{\sigma}(i)} \\
&< \nu_{m\widetilde{\sigma}(m)} + \sum_{i \notin I \cup \{m\}} \nu_{i\widetilde{\sigma}(i)} + \sum_{i \in I} \nu_{i\widetilde{\sigma}(i)} \\
&= \nu_{\widetilde{\sigma}}
\end{aligned}$$

which implies that $\nu_{\widehat{\sigma}}$ is not a maximum, that is $\nu_{\widehat{\sigma}} < \beta$.

Hence, in order to achieve the greatest possible exponent, we need to consider $\sigma(m) = m$.

In order to illustrate how the construction of $\widetilde{\sigma}$ works, consider the following matrix,

0	0	0	0	0	0	0	0	0	0	0	0	0	×		
0	0	0	0	0	0	0	0	0	0	0				□	×
0	0	0	0	0	0	0	0	0	0	×					
0	0	0	0	0	0	0	0	0	0		×				
0	0	0	0	0	0	0						□		×	
0	0	0	0	0	0				□			×			
0	0	0	0	0	0			□	×						
0	0	0	0	0	0	×									
0	0	0					□	×							
0	0	0		×											
0	0	0			×										
0	×														
0			□				×								
		×													
□			×												
×															□

We have $h = 7$, $(l_1, \ldots, l_7) = (13, 11, 10, 7, 6, 3, 1)$, $(k_0, \ldots, k_7) = (16, 15, 14, 12, 11, 8, 5, 3)$, so we have $l_i < k_i$ for $1 \leq i \leq h$. The $\times$ symbols denote the permutation

$$\widehat{\sigma} = (1\ 14\ 3\ 11\ 6\ 13\ 8\ 7\ 10\ 5\ 15\ 4\ 12\ 2\ 16)(9),$$

and the $\square$ symbols denote the positions where the computed permutation $\widetilde{\sigma}$ is different from $\widehat{\sigma}$. Effectively, one can compute $\widetilde{\sigma}$ following the steps described above as follows:

$\delta_0 = m = 16$ and $\mu_{\widehat{\sigma}^{-1}(16)\widehat{\sigma}(16)} = \mu_{2\ 1} = 0$. Then

$$\begin{aligned} \delta_1 &= \widehat{\sigma}\left(\max_{j \geq 16 - \widehat{\sigma}^{-1}(\delta_0)} \widehat{\sigma}^{-1}(j)\right) \\ &= \widehat{\sigma}\left(\max\{1, 2, 5\}\right) \\ &= 15. \end{aligned}$$

Next, since $\mu_{\widehat{\sigma}^{-1}(15)\widehat{\sigma}(16)} = \mu_{5\ 1} = 0$, we define

$$\delta_2 = \widehat{\sigma}\left(\max\{1, 2, 3, 4, 5, 6\}\right) = 13.$$

In the end we obtain the sequences

$$(\delta_1, \delta_2, \ldots, \delta_6) = (15, 13, 10, 9, 8, 4)$$

and

$$\left(\widehat{\sigma}^{-1}(\delta_0), \widehat{\sigma}^{-1}(\delta_1), \ldots, \widehat{\sigma}^{-1}(\delta_6)\right) = (2, 5, 6, 7, 9, 13, 15).$$

Since $\mu_{\widehat{\sigma}^{-1}(4)\widehat{\sigma}(16)} = \mu_{15\ 1} \neq 0$, we define $\widetilde{\sigma}$ by

1. $\widetilde{\sigma}(16) = 16$ and $\widetilde{\sigma}\left(\widehat{\sigma}^{-1}(4)\right) = \widetilde{\sigma}(15) = 1$;
2. $\widetilde{\sigma}(2) = 15, \widetilde{\sigma}(5) = 13, \widetilde{\sigma}(6) = 10, \widetilde{\sigma}(7) = 9, \widetilde{\sigma}(9) = 8$ and $\widetilde{\sigma}(13) = 4$;
3. For $i \in \{1, 3, 4, 8, 10, 11, 12, 14\}$, $\widetilde{\sigma}(i) = \widehat{\sigma}(i)$.

In other words, taking $j = \widehat{\sigma}^{-1}(16) = 1$ in equation (13), we have

$$\begin{aligned} \widetilde{\sigma} &= \widehat{\sigma} \cdot (1\ 16)(4\ 8)(8\ 9)(9\ 10)(10\ 13)(13\ 15)(15\ 1) \\ &= (1\ 14\ 3\ 11\ 6\ 10\ 5\ 13\ 4\ 12\ 2\ 15)(7\ 9\ 8)(16). \end{aligned}$$

Proof Case 2: Let $\widehat{\sigma} \in S_m$ with

$$\mu_{m\widehat{\sigma}(m)}\mu_{m-1\widehat{\sigma}(m-1)}\cdots\mu_{1\widehat{\sigma}(1)} \neq 0,$$

Since $k_{\overline{i}} = l_{\overline{i}}$, then, in any nontrivial term of $|A|$, we must have $\widehat{\sigma}(j) \leq l_{\overline{i}}$ for $j \in \{m-l_{\overline{i}}+1, \ldots, m\}$, which amounts to saying that in order to obtain a nontrivial term of $|A|$ one must pick up $l_{\overline{i}}$ of its components in a matrix A' obtained from A by picking the rows with indices $m - l_{\overline{i}} + 1, \ldots, m$ and the columns with indices $1, \ldots, l_{\overline{i}}$. Obviously, if $\widehat{\sigma}$ gives rise to a term of $|A|$ with the highest exponent, then the corresponding term of $|A'|$ must also have the highest exponent among all terms of $|A'|$. In order to know which term of $|A'|$ has the highest possible exponent in α one can apply the statement of Case 1 for $|A'|$ instead of $|A|$ to conclude that $\mu_{m\sigma(m)} = \mu_{ml_{\overline{i}}}$.

In this way we have shown that if $\overline{\sigma} \in S_m$ satisfies

$$\alpha^{\beta} = \mu_{m\overline{\sigma}(m)}\mu_{m-1\overline{\sigma}(m-1)}\cdots\mu_{1\overline{\sigma}(1)},$$

then $\overline{\sigma}(m) = m$ when the matrix A satisfies the conditions of Case 1 or $\overline{\sigma}(m) = l_{\overline{i}}$ when the matrix A satisfies the conditions of Case 2.

Once $\overline{\sigma}(m)$ has been uniquely determined, we can remove from A its m-th row and its $\overline{\sigma}(m)$-th column to obtain a new square matrix A_1 of order $m-1$. We follow the same previous arguments applied to A_1 instead of to A to determine $\overline{\sigma}(m-1)$. In this way, we define recursively a sequence of matrices $A = A_0, A_1, A_2, \ldots A_{m-1}$, and for each A_i we uniquely define $\overline{\sigma}(m-i)$ using one of the two Cases. Hence there is only one permutation, namely $\overline{\sigma}$, satisfying equation (11) and therefore we prove the existence of a unique maximum in the exponents of the terms of $|A|$. □

We illustrate the whole process of deriving the permutation $\overline{\sigma}$ that gives rise to the *unique* term with highest exponent in α with the following example.

Example 3.1. *Let*

$$A = \left[\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ \hline
0 & 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ \hline
0 & 0 & 0 & & & & & & & & & & & \\ \hline
0 & 0 & 0 & & & & & & & & & & & \\ \hline
0 & 0 & 0 & & & & & & & & & & & \\ \hline
0 & & & & & & & & & & & & & \\ \hline
0 & & & & & & & & & & & & & \\ \hline
 & & & & & & & & & & & & & \\ \hline
\end{array}\right].$$

We have $h = 7$, $(l_1, \ldots, l_7) = (12, 11, 10, 7, 6, 3, 1)$, $(k_0, \ldots, k_7) = (14, 13, 12, 10, 9, 6, 3, 1)$, *so the largest* i *for which* $l_i = k_i$ *is* $\overline{i} = 7$ *and* $l_{\overline{i}} = 1$. *So, for the matrix* A' *obtained from* A *by picking the row with index* m *and the column with index* 1, *we have* $h = 0$, *so* $\overline{\sigma}(m) = 1$. *The new square matrix*

A_1 will be

$$A_1 = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & & & & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ \hline 0 & 0 & & & & & & & & & & & \\ \hline 0 & 0 & & & & & & & & & & & \\ \hline 0 & 0 & & & & & & & & & & & \\ \hline & & & & & & & & & & & & \\ \hline & & & & & & & & & & & & \end{array}\right]$$

Now, $\bar{i} = 6$ and $l_{\bar{i}} = 2$, so $\overline{\sigma}(m) = 3$ (the second column in the matrix A_1 is the third column in the matrix A).

In the end we obtain

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \square & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \square & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \square & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \square \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & \square & & & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & \square & & & & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & & & \square & & & & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & & & & \square & & & & \\ \hline 0 & 0 & 0 & \square & & & & & & & & & & \\ \hline 0 & 0 & 0 & & \square & & & & & & & & & \\ \hline 0 & 0 & 0 & & & \square & & & & & & & & \\ \hline 0 & \square & & & & & & & & & & & & \\ \hline 0 & & \square & & & & & & & & & & & \\ \hline \square & & & & & & & & & & & & & \end{array}\right]$$

The $\square$ symbols denote the permutation $\overline{\sigma}$.

It is well-known that if N is an integer and p a prime number then there exists a finite field $\mathbb{F}$ with p^N elements and therefore there exists a finite field $\mathbb{F}$ such that $|\mathbb{F}| = p^{(2^{M(L+2)-1})}$. However, it follows from the proof of Theorem 3.2 that it is enough to have $|\mathbb{F}| > p^{((2^{M(L+2)-2})(\frac{4}{3}))}$ in order to $\mathcal{T}(T_0, T_1, \ldots, T_L)$ to be superregular. It can be checked using computer algebra programs that there are particular examples (for small values of (n, k, δ)) of superregular matrices that require a much smaller field size, see for instance [2, Example 3.10]. However, the proposed superregular matrices can be constructed for any given characteristic p and parameters (n, k, δ) and therefore provides a general construction. Note that the superregular matrix S_r given in (5) requires, in general, a large characteristic $p(r)$.

We are now in the position to present a new class of MDP convolutional codes. The result easily follows from Theorem 2.1, Theorem 3.2 and the fact that submatrices of a superregular matrix inherit the superregularity property.

Corollary 3.1. *Let (n, k, δ) be given and let $T_\ell = [t_{ij}^\ell]$, $1 \leq i, j \leq m$ and $0 \leq \ell \leq L$ be the entries of the matrix T_ℓ as in (7). Define $\bar{H}_\ell = [t_{ij}^\ell]$ $1 \leq i \leq n-k$, $1 \leq j \leq k$ and $0 \leq \ell \leq L$. Let*

$A(z) = \sum_{i=0}^{\nu} A_i z^i \in \mathbb{F}[z]^{(n-k)\times(n-k)}$ *and* $B(z) = \sum_{i=0}^{\nu} B_i z^i \in \mathbb{F}[z]^{(n-k)\times k}$*, with* $\nu = \frac{\delta}{n-k}$*,* $A_0 = I_{n-k}$*,* $A_i \in \mathbb{F}^{(n-k)\times(n-k)}$*, with* $1 \leq i \leq \nu$ *is obtained by solving the equations*

$$[A_\nu \cdots A_1] \begin{bmatrix} \bar{H}_{L-\nu} & \cdots & \bar{H}_1 \\ \bar{H}_{L-\nu+1} & \cdots & \bar{H}_2 \\ \vdots & & \vdots \\ \bar{H}_{L-1} & \cdots & \bar{H}_\nu \end{bmatrix} = -[\bar{H}_L \cdots \bar{H}_{\nu+1}],$$

and $B_i = A_0\bar{H}_i + A_1\bar{H}_{i-1} + \cdots + A_i\bar{H}_0$*, with* $0 \leq i \leq \nu$*.*

If $|\mathbb{F}| \geq p^{(2^{M(L+1)+n-2})}$ *then the convolutional code* $\mathcal{C} = \ker_{\mathbb{F}[z]}[A(z)\ B(z)]$ *is an MDP convolutional code of rate* k/n *and degree* δ*.*

Remark 3.1. *Details about the construction of the matrices* $A(z)$ *and* $B(z)$ *presented in Corollary 3.1 can be found in [2, Appendix C]*

The following example illustrates the construction of a $(5, 2, 3)$ MDP convolutional code.

Example 3.2. *Since* $n = 5$*,* $k = 2$ *and* $\delta = 3$*, we have that* $L = 2$ *and* $\nu = 1$*. Let us consider* α *a root of the primitive polynomial* $x^{1024} + x^{39} + x^{37} + x^{36} + 1 \in \mathbb{F}_2[x]$*,* i. e.*, a primitive element over the field* $\mathbb{F}_{2^{1024}}$ *and the matrix*

$$[\bar{H}_0\ \bar{H}_1\ \bar{H}_2] = \left[\begin{array}{cc|cc|cc} \alpha^{2^0} & \alpha^{2^1} & \alpha^{2^3} & \alpha^{2^4} & \alpha^{2^6} & \alpha^{2^7} \\ \alpha^{2^1} & \alpha^{2^2} & \alpha^{2^4} & \alpha^{2^5} & \alpha^{2^7} & \alpha^{2^8} \\ \alpha^{2^2} & \alpha^{2^3} & \alpha^{2^5} & \alpha^{2^6} & \alpha^{2^8} & \alpha^{2^9} \end{array}\right]$$

over $\mathbb{F}_{2^{1024}}$*. Considering* $A(z) = I_3 + A_1 z$ *such that* $A_1\bar{H}_1 = -\bar{H}_2$*, where, a possible choice is*

$$\begin{aligned} A(z) \quad = \quad & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \\ & \frac{1}{\alpha^{2^3+2^5} - \alpha^{2^5}} \begin{bmatrix} -\alpha^{2^5+2^6} + \alpha^{2^4+2^7} & -\alpha^{2^5+2^7} + \alpha^{2^4+2^8} & -\alpha^{2^5+2^8} + \alpha^{2^4+2^9} \\ \alpha^{2^4+2^6} - \alpha^{2^3+2^7} & \alpha^{2^4+2^7} - \alpha^{2^3+2^8} & \alpha^{2^4+2^8} - \alpha^{2^4+2^8} - \alpha^{2^3+2^9} \\ 0 & 0 & 0 \end{bmatrix} z, \end{aligned}$$

and $B(z) = B_0 + B_1 z$ *such that* $B_0 = \bar{H}_0$ *and* $B_1 = \bar{H}_1 + A_1\bar{H}_0$*, we have that*

$$\mathcal{C} = \ker_{\mathbb{F}[z]}[A(z)\ B(z)]$$

is a $(5, 2, 3)$ *MDP convolutional code.*

4. Conclusions

There is a type of superregular matrices that are essential for the construction of MDP convolutional codes. However, very little is understood about how to construct these matrices and how large a finite field must be, so that a superregular matrix of a given order can exist over that field. In this paper, we have presented a new class of MDP (n, k, δ) convolutional codes, such that $(n-k)|\delta$, by means of the construction of a novel type of superregular matrices over a field of any characteristic. We also established a bound for the size of the field needed for these matrices to be superregular.

Referências

[1] A. K. Aidinyan. *On Matrices with Nondegenerate Square Submatrices*. Probl. Peredachi Inf., **22** (4): 106-108, 1986.

[2] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache. *Strongly MDS convolutional codes*. IEEE Trans. Inf. Th., **52** (2): 584-598, 2006.

[3] T.W. Hungerford. *Algebra*. Springer-Verlag, New York, 1974.

[4] R. Hutchinson *The Existence of Strongly MDS Convolutional Codes*. SIAM Journal on Control and Optimization, **47** (6): 2812-2826, 2008.

[5] R. Hutchinson, J. Rosenthal and R. Smarandache. *Convolutional codes with maximum distance profile*. Systems & Control Letters, **54** (1): 53-63, 2005.

[6] R. Hutchinson, R. Smarandache and J. Trumpf. *On superregular matrices and MDP convolutional codes*. Linear Algebra and its Applications, **428**: 2585-2596, 2008.

[7] R. Johannesson and K.S. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press Series in Digital and Mobile Comm., 1999.

[8] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II*. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[9] J. M. Muñoz Porras, J. A. Domínguez Pérez, J. I. Iglesias Curto and G. Serrano Sotelo. *Convolutional Goppa codes*. IEEE Trans. Inf. Th., **52** (1), 340-344, 2006.

[10] J. Rosenthal and R. Smarandache. *Maximum distance separable convolutional codes*. Appl. Algebra Engrg. Comm. Comput., **10** (1), 15-32, 1999.

[11] R. M. Roth and A. Lempel. *On MDS codes via Cauchy matrices*. IEEE Trans. Inf. Th., **35** (6), 1314-1319, 1989.

[12] R. M. Roth and G. Seroussi. *On generator matrices of MDS codes*. IEEE Trans. Inf. Th., **31** (6), 826-830, 1985.

[13] R. Smarandache, H. Gluesing-Luerssen and J. Rosenthal. *Constructions of MDS-convolutional codes*. IEEE Trans. Inf. Th., **47** (5), 2045-2049, 2001.

[14] V. Tomás. *Complete-MDP Convolutional Codes over the Erasure Channel*. Departamento de Ciencia de la Computación e Inteligencia Artificial, Universidad de Alicante, Alicante, España. Jul. 2010.

[15] V. Tomás, J. Rosenthal and R. Smarandache. *Decoding of MDP convolutional codes over the erasure channel*. Proceedings of the 2009 IEEE International Symposium on Information Theory (ISIT 2009), 556-560, Seoul, Korea. June 2009. IEEE.