IEEE Transactions on Information Theory

Maximum distance separable 2D convolutional codes

Journal:	*IEEE Transactions on Information Theory*
Manuscript ID:	Draft
Manuscript Type:	Regular Manuscript
Date Submitted by the Author:	n/a
Complete List of Authors:	Climent, Joan-Josep; Universitat d'Alacant, Departament d'Estadística i Investigació Operativa Napp, Diego; University of Aveiro, Center for Research and Development in Mathematics and Applications; University of Aveiro, Department of Mathematics Perea, Carmen; Universidad Miguel Hernández de Elche, Centro de Investigación Operativa; Universidad Miguel Hernández de Elche, Departamento de Estadística, Matemáticas e Informática Pinto, Raquel; University of Aveiro, Center for Research and Development in Mathematics and Applications; University of Aveiro, Department of Mathematics
Keywords:	2D convolutional code, generalized Singleton bound, maximum distance separable code, superregular matrix, circulant Cauchy matrix

Maximum distance separable 2D convolutional codes

Joan-Josep Climent Diego Napp Carmen Perea Raquel Pinto

Abstract

Maximum Distance Separable (MDS) block codes and MDS one-dimensional (1D) convolutional codes are the most robust codes for error correction within the class of block codes of a fixed rate and 1D convolutional codes of a certain rate and degree, respectively. In this paper we generalize this concept to the class of two-dimensional (2D) convolutional codes. For that we introduce a natural bound on the distance of a 2D convolutional code of rate k/n and degree δ, which generalizes the Singleton bound for block codes and the generalized Singleton bound for 1D convolutional codes. Then we prove the existence of 2D convolutional codes of rate k/n and degree δ that reach such bound when $n \geq k\frac{(\lfloor \frac{\delta}{k} \rfloor+2)(\lfloor \frac{\delta}{k} \rfloor+3)}{2}$ if $k \nmid \delta$, or $n \geq k\frac{(\frac{\delta}{k}+1)(\frac{\delta}{k}+2)}{2}$ if $k \mid \delta$, by presenting a concrete constructive procedure.

Index Terms

2D convolutional code, generalized Singleton bound, maximum distance separable code, superregular matrix, circulant Cauchy matrix.

I. Introduction

One of the most important requirements for the construction of powerful codes is that they must have good error correcting properties, i.e., as large (free) distance as possible. The codes that have the largest possible distance among all codes with the same parameters are called maximum distance separable (MDS). In the context of block

This paper was presented in part at the 20th International Symposium on Mathematical Theory of Networks and Systems (MTNS2012). Melbourne, Australia. July 9-13, 2012.

Joan-Josep Climent is with Departament d'Estadística i Investigació Operativa. Universitat d'Alacant. Campus de Sant Vicent del Raspeig. Apartat de correus 99, E–03080 Alacant. Spain.

Diego Napp and Raquel Pinto are with CIDMA – Center for Research and Development in Mathematics and Applications. Department of Mathematics. University of Aveiro. Campus Universitario de Santiago, 3810-193 Aveiro, Portugal

Carmen Perea is with Centro de Investigación Operativa. Departamento de Estadística, Matemáticas e Informática. Universidad Miguel Hernández. Av. Universidad s/n, E-03202 Elche, Spain

This work was partially supported by Spanish grant MTM2011-24858 of the Ministerio de Economía y Competitividad of the Gobierno de España. The work of the second and fourth authors was partially supported by *FEDER* founds through *COMPETE*–Operational Programme Factors of Competitiveness ("Programa Operacional Factores de Competitividade") and by Portuguese founds through the *Center for Research and Development in Mathematics and Applications* and the Portuguese Foundation for Science and Technology ("FCT–Fundação para a Ciência e a Tecnologia"), within project PEst-C/MAT/UI4106/2011 with COMPETE number FCOMP-01-0124-FEDER-022690.

codes, MDS codes are very well understood. It is well-known that the distance of a block code of rate k/n is always upper-bounded by the Singleton bound $n-k+1$. The class of Reed-Solomon codes is a good example of block codes that achieve this bound, i.e., are MDS (see, for example, [22]).

The convolutional case is more complex. It was shown in [25] that the distance of a 1D convolutional code of rate k/n and degree δ is always upper-bounded by the generalized Singleton bound $(n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1$. Later, concrete constructions of MDS 1D convolutional codes for all rates and degrees have been introduced [30], [31].

Roughly speaking 1D convolutional codes can be seen as a generalization of block codes in the sense that a block code is a convolutional code with no delay, i.e., block codes are basically 0D convolutional codes. In this way, multi-dimensional convolutional codes (nD convolutional codes where n stands for the dimension) extend the notion of block codes and 1D convolutional codes. These codes have a practical potential in applications as they are very suitable to encode data recorded in n dimensions, e.g., pictures, videos, storage media, wireless applications, etc. [14], [29], [35]. However, in comparison to 1D convolutional codes, little research has been done in the area of nD convolutional codes and much more needs to be done to make it attractive for real life applications.

The algebraic theory of 2D and nD convolutional codes has been laid out by Fornasini and Valcher in [6], Weiner *et al* in [8], [33] and recently by Lomadze in [21]. Several attempts aiming at the construction and implementation of this type of codes have been presented in [1], [2], [4], [11], [17], [19], [20], [24], [34].

Nonetheless, despite its fundamental relevance, very little is known about their distance properties. We mention [5], [24] for results on the distance properties of 2D convolutional codes in some particular cases. Still the general case is unexplored: no general bound on the distance has been derived and, consequently, the existence of multidimensional MDS convolutional codes is not known.

In this paper we investigate these issues for 2D convolutional codes. The paper contains two major results. First, we derive an upper bound on the distance of 2D convolutional codes (Section III). This bound can be regarded as the generalization to the 2D case of the generalized Singleton bound for 1D convolutional codes. Hence, this bound is called generalized 2D Singleton bound and the 2D convolutional codes that achieve such a bound are called MDS 2D convolutional codes. Second, we show that this bound is tight, i.e., we prove that there exist MDS 2D convolutional codes (Section IV). More concretely, we present a construction of an MDS 2D convolutional code of rate k/n and degree δ with $n \geq k\frac{\left(\left\lfloor \frac{\delta}{k} \right\rfloor+2\right)\left(\left\lfloor \frac{\delta}{k} \right\rfloor+3\right)}{2}$, if $k \nmid \delta$, or $n \geq k\frac{\left(\frac{\delta}{k}+1\right)\left(\frac{\delta}{k}+2\right)}{2}$, if $k \mid \delta$. For these constructions we make use of the so-called superregular matrices. Our construction is valid for any field on which we can construct superregular matrices with the required properties. However, to illustrate the results of the paper we also show (in Section V) how to use a circulant Cauchy matrix over a finite field with an odd number of elements to construct an MDS 2D convolutional code and we provide some examples.

II. 2D CONVOLUTIONAL CODES

In this section we recall the basic background on 2D finite support convolutional codes. We denote the ring of polynomials in the two indeterminates, z_1 and z_2, with coefficients in the finite field $\mathbb{F}$ by $\mathbb{F}[z_1, z_2]$.

Definition 1: A *2D finite support convolutional code* $\mathcal{C}$ of rate k/n is a free $\mathbb{F}[z_1, z_2]$-submodule of $\mathbb{F}[z_1, z_2]^n$, where k is the rank of $\mathcal{C}$. A full column rank matrix $\widehat{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ whose columns constitute a basis for $\mathcal{C}$, i.e., such that

$$\begin{aligned}\mathcal{C} &= \mathrm{Im}_{\mathbb{F}[z_1,z_2]}\, \widehat{G}(z_1, z_2)\\ &= \left\{\widehat{\boldsymbol{v}}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^n \mid \widehat{\boldsymbol{v}}(z_1, z_2) = \widehat{G}(z_1, z_2)\widehat{\boldsymbol{u}}(z_1, z_2) \text{ with } \widehat{\boldsymbol{u}}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k\right\},\end{aligned}$$

is called an *encoder* of $\mathcal{C}$. The elements $\widehat{\boldsymbol{v}}(z_1, z_2)$ of $\mathcal{C}$ are called *codewords* and $\widehat{\boldsymbol{u}}(z_1, z_2)$ are the *information vectors*.

We consider a 2D finite support convolutional code as a free submodule of $\mathbb{F}[z_1, z_2]^n$, and not as a general submodule of $\mathbb{F}[z_1, z_2]^n$ like in [33], in order to avoid the lack of injectivity, i.e., that two different sequences produce the same codeword.

Two full column rank matrices $\widehat{G}(z_1, z_2), \widehat{G}'(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ are *equivalent encoders* if they generate the same 2D finite support convolutional code, i.e., if

$$\mathrm{Im}_{\mathbb{F}[z_1,z_2]}\, \widehat{G}(z_1, z_2) = \mathrm{Im}_{\mathbb{F}[z_1,z_2]}\, \widehat{G}'(z_1, z_2),$$

which happens if and only if there exists a unimodular matrix $\widehat{U}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times k}$ (see [33]) such that $\widehat{G}(z_1, z_2)\widehat{U}(z_1, z_2) = \widehat{G}'(z_1, z_2)$.

From now on we will refer to 2D finite support convolutional codes simply as 2D convolutional codes.

The complexity and the degree of a 1D convolutional code are equivalent and crucial notions. They are one of the parameters of the generalized Singleton bound on the distance of these codes. To define similar notions for 2D convolutional codes, we need to consider first the usual notion of (total) degree of a polynomial matrix

$$\widehat{G}(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}_0^2} G(i, j) z_1^i z_2^j \in \mathbb{F}[z_1, z_2]^{n\times k},$$

with $G(i, j) \in \mathbb{F}^{n\times k}$, defined as $\deg(\widehat{G}(z_1, z_2)) = \max\{i + j \mid G(i, j) \neq 0\}$. Here, and in the rest of the paper, $\mathbb{N}_0$ denotes the set of nonnegative integers. We can define the total degree of a polynomial vector or just of a polynomial in the same way.

Moreover, given a polynomial matrix $\widehat{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ we define the internal degree of $\widehat{G}(z_1, z_2)$, denoted by $\delta_i(\widehat{G}(z_1, z_2))$, as the maximal degree of its full size minors. Note that since equivalent encoders differ by unimodular matrices, their full size minors differ by a nonzero constant. We can now introduce the notion of complexity of a 2D convolutional code as follows.

Definition 2 ([24]): Let $\mathcal{C}$ be a 2D convolutional code. The *complexity* of $\mathcal{C}$, represented by $\widehat{\delta}_{\mathcal{C}}$, is defined as the internal degree of any encoder of $\mathcal{C}$.

We define the degree of a 2D convolutional code in a similar way as it is defined for 1D convolutional codes.

Definition 3: Let $\mathcal{C}$ be a 2D convolutional code, $\widehat{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ an encoder of $\mathcal{C}$ and ν_i the column degree of the ith column of $\widehat{G}(z_1, z_2)$, i.e, the maximum degree of the entries of the ith column of $\widehat{G}(z_1, z_2)$. The *external degree* of $\widehat{G}(z_1, z_2)$, denoted by $\delta_e(\widehat{G}(z_1, z_2))$, is defined as

$$\delta_e(\widehat{G}(z_1, z_2)) = \sum_{i=1}^{k} \nu_i$$

and the *degree* of $\mathcal{C}$, denoted by $\delta_{\mathcal{C}}$, is defined as the minimum of the external degrees of all the encoders of $\mathcal{C}$.

Since $\nu = \max\{\nu_i \mid i = 1, 2, \ldots, k\}$ is the total degree of $\widehat{G}(z_1, z_2)$, it follows then that

$$\widehat{G}(z_1, z_2) = \sum_{0\leq i+j\leq \nu} G(i, j) z_1^i z_2^j, \quad \text{with } G(i, j) \in \mathbb{F}^{n\times k} \text{ and } G(i, j) \neq O \text{ for some } i + j = \nu. \tag{1}$$

Note that when $\delta_{\mathcal{C}} = 0$, then $\widehat{G}(z_1, z_2)$ is a constant matrix and therefore yields a block code. So, from now on we always assume that $\delta_{\mathcal{C}} > 0$.

Remark 1: If $\widehat{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ is an encoder of a 2D convolutional code $\mathcal{C}$, then

$$\delta_i(\widehat{G}(z_1, z_2)) \leq \delta_e(\widehat{G}(z_1, z_2)).$$

Moreover, if there exists an encoder $\widehat{G}(z_1, z_2)$ of $\mathcal{C}$, such that $\delta_e(\widehat{G}(z_1, z_2)) = \widehat{\delta}_{\mathcal{C}}$, then $\widehat{\delta}_{\mathcal{C}} = \delta_{\mathcal{C}}$.

If no confusion arises we write δ and $\widehat{\delta}$ for $\delta_{\mathcal{C}}$ and $\widehat{\delta}_{\mathcal{C}}$, respectively. Note that the degree of a 1D convolutional code equals its complexity, since a 1D convolutional code always admits column reduced encoders whose external degree equals their internal degree (see [12], [23]). However, for 2D convolutional codes such encoders do not always exist and there are therefore codes such that $\widehat{\delta} < \delta$. The following simple example illustrates this fact.

Example 1: For any finite field, let $\mathcal{C}$ be a 2D convolutional code with encoder

$$\widehat{G}(z_1, z_2) = \begin{bmatrix} 1 & 0 \\ z_1 & z_2 \\ 1 & 1 \end{bmatrix}.$$

It is easy to check that $\mathcal{C}$ has complexity 1 but degree 2. □

Remark 2: Note that the complexity and the degree of a 2D convolutional code are directly connected with the notion of degree of a 2D polynomial, which means that different notions of complexity and degree could be considered. We opted to use the "total degree" of a 2D polynomial since, similarly to the 1D case, the corresponding notion of complexity gives a lower bound on the dimension of the input-state-output representations of such codes (see [24]).

We finish this section by introducing the support and the weight of a word. Given a word

$$\widehat{\boldsymbol{v}}(z_1, z_2) = \sum_{(i,j)\in\mathbb{N}_0^2} \boldsymbol{v}(i, j) z_1^i z_2^j \in \mathbb{F}[z_1, z_2]^n,$$

with $\boldsymbol{v}(i,j) \in \mathbb{F}^n$ for $(i,j) \in \mathbb{N}_0^2$, we define the *support* of $\widehat{\boldsymbol{v}}(z_1,z_2)$ as

$$\mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right) = \left\{(i,j) \in \mathbb{N}_0^2 \mid \boldsymbol{v}(i,j) \neq \boldsymbol{0}\right\}$$

and the *weight* of $\widehat{\boldsymbol{v}}(z_1,z_2)$ as

$$\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right) = \sum_{(i,j)\in\mathbb{N}_0^2} \mathrm{wt}\left(\boldsymbol{v}(i,j)\right) = \sum_{(i,j)\in\mathrm{Supp}(\widehat{\boldsymbol{v}}(z_1,z_2))} \mathrm{wt}\left(\boldsymbol{v}(i,j)\right),$$

where $\mathrm{wt}\left(\boldsymbol{v}(i,j)\right)$ is the number of nonzero entries of $\boldsymbol{v}(i,j)$.

Moreover, if $\widehat{G}(z_1,z_2) \in \mathbb{F}[z_1,z_2]^{n\times k}$ is the polynomial matrix given by expression (1),

$$\widehat{\boldsymbol{u}}(z_1,z_2) = \sum_{(r,s)\in\mathbb{N}_0^2} \boldsymbol{u}(r,s) z_1^r z_2^s \in \mathbb{F}[z_1,z_2]^k,$$

is the information vector, and $\widehat{\boldsymbol{v}}(z_1,z_2) = \widehat{G}(z_1,z_2)\widehat{\boldsymbol{u}}(z_1,z_2)$, is the corresponding codeword, then

$$\widehat{\boldsymbol{v}}(z_1,z_2) = \sum_{(a,b)\in\mathbb{N}_0^2} \boldsymbol{v}(a,b) z_1^a z_2^b,$$

where

$$\boldsymbol{v}(a,b) = \sum_{\substack{0\leq i+j\leq \nu \\ i+r=a \\ j+s=b}} G(i,j)\boldsymbol{u}(r,s) = \sum_{r+s\leq a+b\leq \nu+r+s} G(a-r,b-s)\boldsymbol{u}(r,s) \tag{2}$$

III. 2D GENERALIZED SINGLETON BOUND

It is well-known that an important measure of robustness of a code is its distance (see [12], [22]). We define the notion of distance of a 2D convolutional code as in [33]. The *distance* between two words

$$\widehat{\boldsymbol{v}}_1(z_1,z_2), \widehat{\boldsymbol{v}}_2(z_1,z_2) \in \mathbb{F}[z_1,z_2]^n$$

is then given by $\mathrm{dist}\left(\widehat{\boldsymbol{v}}_1(z_1,z_2), \widehat{\boldsymbol{v}}_2(z_1,z_2)\right) = \mathrm{wt}\left(\widehat{\boldsymbol{v}}_1(z_1,z_2) - \widehat{\boldsymbol{v}}_2(z_1,z_2)\right)$.

Definition 4: Given a 2D convolutional code $\mathcal{C}$, the *distance* of $\mathcal{C}$ is defined as

$$\mathrm{dist}\left(\mathcal{C}\right) = \min\left\{\mathrm{dist}\left(\widehat{\boldsymbol{v}}_1(z_1,z_2), \widehat{\boldsymbol{v}}_2(z_1,z_2)\right) \mid \widehat{\boldsymbol{v}}_1(z_1,z_2), \widehat{\boldsymbol{v}}_2(z_1,z_2) \in \mathcal{C}, \text{ with } \widehat{\boldsymbol{v}}_1(z_1,z_2) \neq \widehat{\boldsymbol{v}}_2(z_1,z_2)\right\}.$$

Note that the linearity of $\mathcal{C}$ implies that

$$\mathrm{dist}\left(\mathcal{C}\right) = \min\left\{\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right) \mid \widehat{\boldsymbol{v}}(z_1,z_2) \in \mathcal{C}, \text{ with } \widehat{\boldsymbol{v}}(z_1,z_2) \neq \boldsymbol{0}\right\}.$$

In this section, we give an upper bound on the distance of 2D convolutional codes of rate k/n and degree δ. For that we need the following result. Here, and in the rest of the paper, we write $\#S$ to refer to the number of elements in a set S.

Lemma 1: *Let $\widehat{G}(z_1,z_2) \in \mathbb{F}[z_1,z_2]^{n\times k}$ be a full column rank matrix such that all its column degrees are equal to ν, and let $\mathcal{C}$ be the 2D convolutional code generated by $\widehat{G}(z_1,z_2)$. Then*

$$\mathrm{dist}\left(\mathcal{C}\right) \leq n\frac{(\nu+1)(\nu+2)}{2} - k + 1.$$

Proof: Since ν is the total degree of $\widehat{G}(z_1, z_2)$ we can consider expression (1). Let $\boldsymbol{u} \in \mathbb{F}^k$ be a nonzero vector such that $G(0,0)\boldsymbol{u}$ has its first $k-1$ entries equal to zero. Thus, $\mathrm{wt}\,(G(0,0)\boldsymbol{u}) \leq n-k+1$.

Notice that since $\mathrm{wt}\,(G(i,j)\boldsymbol{u}) \leq n$, for $1 \leq i+j \leq \nu$, and

$$\#\{(i,j) \in \mathbb{N}_0^2 \mid 1 \leq i+j \leq \nu\} = \frac{(\nu+1)(\nu+2)}{2} - 1,$$

we have that

$$\begin{aligned}
\mathrm{dist}\,(\mathcal{C}) &\leq \mathrm{wt}\left(\widehat{G}(z_1,z_2)\boldsymbol{u}\right) = \sum_{0\leq i+j\leq \nu} \mathrm{wt}\,(G(i,j)\boldsymbol{u}) \\
&= \mathrm{wt}\,(G(0,0)\boldsymbol{u}) + \sum_{1\leq i+j\leq \nu} \mathrm{wt}\,(G(i,j)\boldsymbol{u}) \\
&\leq (n-k+1) + n\left(\frac{(\nu+1)(\nu+2)}{2} - 1\right) = n\frac{(\nu+1)(\nu+2)}{2} - k + 1.
\end{aligned}$$

■

The above result allows us to obtain an upper bound on the distance of a general 2D convolutional code of rate k/n and degree δ, as stated in the next theorem.

Theorem 1: *Let $\mathcal{C}$ be a 2D convolutional code of rate k/n and degree δ. Then*

$$\mathrm{dist}\,(\mathcal{C}) \leq n\frac{\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right)}{2} - k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{3}$$

Proof: Let $\widehat{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ be an encoder of $\mathcal{C}$ with column degrees $\nu_1, \nu_2, \ldots, \nu_k$ and external degree δ (i.e., $\nu_1 + \nu_2 + \cdots + \nu_k = \delta$).

Assume first that $\nu_1 = \nu_2 = \cdots = \nu_k$. Then, from Lemma 1

$$\mathrm{dist}\,(\mathcal{C}) \leq n\frac{(\nu_k+1)(\nu_k+2)}{2} - k + 1.$$

and taking into account that $k\nu_k = \delta$, it follows that

$$n\frac{(\nu_k+1)(\nu_k+2)}{2} - k + 1 = n\frac{\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right)}{2} - k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1$$

and therefore, expression (3) holds.

Assume now that

$$\nu_1 \geq \nu_2 \geq \cdots \geq \nu_t > \nu_{t+1} = \nu_{t+2} = \cdots = \nu_k$$

for some t with $1 \leq t < k$. It follows then that $\delta \geq t(\nu_k+1) + (k-t)\nu_k$. So, $\delta - k\nu_k \geq t$ and $\left\lfloor \frac{\delta}{k} \right\rfloor \geq \nu_k$.

Let $\widehat{\boldsymbol{u}}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k$ be a nonzero vector whose first t entries are zero. Then, it follows from Lemma 1 that

$$\mathrm{dist}\,(\mathcal{C}) \leq n\frac{(\nu_k+1)(\nu_k+2)}{2} - (k-t) + 1.$$

This upper bound is larger if ν_k and t are as large as possible. Since the largest possible values for ν_k and t are $\nu_k = \left\lfloor \frac{\delta}{k} \right\rfloor$ and $t = \delta - k\left\lfloor \frac{\delta}{k} \right\rfloor$, substituting this values in the above upper bound, inequality (3) holds. ■

The upper bound given by the above theorem is the extension to 2D convolutional codes of the generalized Singleton bound for 1D convolutional codes (see [25], [31]).

Definition 5: We call the upper bound in expression (3) the 2*D generalized Singleton bound*. Moreover, we say that a 2D convolutional code of rate k/n and degree δ is a *Maximum Distance Separable* (MDS) 2D convolutional code if its distance equals the 2D generalized Singleton bound.

There could be other expressions for the 2D generalized Singleton bound as there is not a unique obvious way to define the "degree" δ of a 2D convolutional code (see Remark 2).

Finally, note that in the proof of Theorem 1, $t = \delta - k\nu_k$, implies that $\nu_1 = \nu_2 = \cdots = \nu_t = \nu_k + 1$. Thus, the existence of an encoder with column degrees

$$\nu_1 = \nu_2 = \cdots = \nu_t = \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \quad \text{and} \quad \nu_{t+1} = \nu_{t+2} = \cdots = \nu_k = \left\lfloor \frac{\delta}{k} \right\rfloor$$

is a necessary condition for a 2D convolutional code to be MDS.

IV. MDS 2D CONVOLUTIONAL CODES

In this section we present a construction of MDS 2D convolutional codes of rate k/n and degree δ. To this end we need to consider superregular matrices.

Definition 6 ([26]): Let A be an $n \times \ell$ matrix over a finite field $\mathbb{F}$. We say that A is a *superregular* matrix if every square submatrix of A is nonsingular.

See [9], [15], [16], [18], [22], [26], [28] for different constructions of superregular matrices. Superregular matrices are also called MDS matrices [13] or hyper-invertible matrices [3].

Note that every submatrix of a superregular matrix is also a superregular matrix. In particular, all the entries of a superregular matrix are nonzero. We will use these facts several times throughout the paper.

It is worth mentioning that some authors have used the term *superregular* to define a related but different type of matrices, see for instance [7], [10], [32]. So,

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{2\times 2} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix} \in \mathbb{F}_3^{3\times 3}$$

are superregular matrices within the meaning of [7], [10], [32], but they are not superregular matrices within the meaning of Definition 6.

The following lemma is an immediate consequence of Definition 6 and it gives a lower bound on the weight of a linear combination of columns of a superregular matrix.

Lemma 2: *Let A be a superregular matrix of size $n \times \ell$ over a finite field $\mathbb{F}$, with $n \geq \ell$. It follows that any nontrivial linear combination of m different columns of A cannot have more than $m-1$ entries equal to zero.*

Next, for positive integers n, k and δ, we construct a 2D convolutional code $\mathcal{C}$ of rate k/n and degree δ whose distance achieves the upper bound of expression (3).

Throughout the paper, we denote

$$t = \delta - k \left\lfloor \frac{\delta}{k} \right\rfloor .$$

For notational reasons we assume first that $k \nmid \delta$, i.e., $0 < t < k$. The case $k \mid \delta$ is simpler and it will be briefly considered at the end of this section.

Using superregular matrices we will construct an encoder $\widehat{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n \times k}$ of an MDS 2D convolutional code of rate k/n and degree δ, with column degrees $\nu_1, \nu_2, \ldots, \nu_k$, given by

$$\nu_r = \begin{cases} \lfloor \frac{\delta}{k} \rfloor + 1, & \text{for } r = 1, 2, \ldots, t, \\ \lfloor \frac{\delta}{k} \rfloor, & \text{for } r = t+1, t+2, \ldots, k. \end{cases} \tag{4}$$

Let us define

$$\ell_1 = \frac{(\lfloor \frac{\delta}{k} \rfloor + 2)(\lfloor \frac{\delta}{k} \rfloor + 3)}{2} \qquad \text{and} \qquad \ell_2 = \frac{(\lfloor \frac{\delta}{k} \rfloor + 1)(\lfloor \frac{\delta}{k} \rfloor + 2)}{2}.$$

Hence, ℓ_1 and ℓ_2 represent the maximum number of nonzero coefficient vectors in $\mathbb{F}^n$ that a polynomial vector in $\mathbb{F}[z_1, z_2]^n$ of degrees $\lfloor \frac{\delta}{k} \rfloor + 1$ and $\lfloor \frac{\delta}{k} \rfloor$, respectively, may have.

For a sufficient large field $\mathbb{F}$ consider matrices

$$A_r = \begin{bmatrix} \boldsymbol{g}_0^r & \boldsymbol{g}_1^r & \cdots & \boldsymbol{g}_{\ell_2-1}^r \end{bmatrix} \in \mathbb{F}^{n \times \ell_2} \quad \text{for} \quad r = 1, 2, \ldots, t, t+1, \ldots, k$$

and

$$B_r = \begin{bmatrix} \boldsymbol{g}_{\ell_2}^r & \boldsymbol{g}_{\ell_2+1}^r & \cdots & \boldsymbol{g}_{\ell_1-1}^r \end{bmatrix} \in \mathbb{F}^{n \times (\ell_1 - \ell_2)} \quad \text{for} \quad r = 1, 2, \ldots, t,$$

such that

$$\begin{aligned} \mathfrak{G} &= \begin{bmatrix} A_1 & B_1 & A_2 & B_2 & \cdots & A_t & B_t & A_{t+1} & A_{t+2} & \cdots & A_k \end{bmatrix} \in \mathbb{F}^{n \times (k\ell_2 + t(\ell_1 - \ell_2))}, \\ \mathcal{G}_1 &= \begin{bmatrix} \operatorname{rsh}(A_1) & \operatorname{rsh}(A_2) & \cdots & \operatorname{rsh}(A_t) & \operatorname{rsh}(A_{t+1}) & \cdots & \operatorname{rsh}(A_k) \end{bmatrix} \in \mathbb{F}^{n\ell_2 \times k}, \\ \mathcal{G}_2 &= \begin{bmatrix} \operatorname{rsh}(B_1) & \operatorname{rsh}(B_2) & \cdots & \operatorname{rsh}(B_t) \end{bmatrix} \in \mathbb{F}^{n(\ell_1 - \ell_2) \times t} \end{aligned} \tag{5}$$

are superregular matrices, where

$$\operatorname{rsh}(A_r) = \begin{bmatrix} \boldsymbol{g}_0^r \\ \boldsymbol{g}_1^r \\ \vdots \\ \boldsymbol{g}_{\ell_2-1}^r \end{bmatrix} \quad \text{for} \quad r = 1, 2, \ldots, t, t+1, \ldots, k$$

and

$$\operatorname{rsh}(B_r) = \begin{bmatrix} \boldsymbol{g}_{\ell_2}^r \\ \boldsymbol{g}_{\ell_2+1}^r \\ \vdots \\ \boldsymbol{g}_{\ell_1-1}^r \end{bmatrix} \quad \text{for} \quad r = 1, 2, \ldots, t,$$

are the reshapes of the matrices A_r and B_r, respectively. Further, we define the matrix

$$\mathcal{G} = \begin{bmatrix} \mathcal{G}_1 \\ \bar{\mathcal{G}}_2 \end{bmatrix}, \quad \text{with} \quad \bar{\mathcal{G}}_2 = \begin{bmatrix} \mathcal{G}_2 & O \end{bmatrix} \in \mathbb{F}^{n(\ell_1-\ell_2)\times k}. \tag{6}$$

Note that we can obtain the matrices $\mathcal{G}_1$ and $\mathcal{G}_2$ from matrix $\mathfrak{G}$ and vice-versa. In Section V we will present a method to obtain superregular matrices $\mathfrak{G}$, $\mathcal{G}_1$, and $\mathcal{G}_2$.

Now, let us construct polynomial vectors $\widehat{G}_r(z_1, z_2) \in \mathbb{F}[z_1, z_2]^n$ as follows

$$\widehat{G}_r(z_1, z_2) = \begin{cases} \displaystyle\sum_{0\le i+j\le \lfloor \frac{\delta}{k} \rfloor + 1} \boldsymbol{g}^r_{\mu(i,j)} z_1^i z_2^j, & \text{for } r = 1, 2, \ldots, t, \\ \displaystyle\sum_{0\le i+j\le \lfloor \frac{\delta}{k} \rfloor} \boldsymbol{g}^r_{\mu(i,j)} z_1^i z_2^j, & \text{for } r = t+1, t+2, \ldots, k, \end{cases} \tag{7}$$

where $\mu : \mathbb{N}_0^2 \to \mathbb{N}_0$ is the map defined by

$$\mu(i, j) = j + \frac{(i+j)(i+j+1)}{2}, \quad \text{for all} \quad (i, j) \in \mathbb{N}_0^2. \tag{8}$$

This is a well-known function (one of the Cantor's pairing functions) commonly used to show that $\mathbb{N}_0^2$ and $\mathbb{N}_0$ have the same cardinality; i.e., μ is a bijection. Moreover, $\mu(r_1, s_1) < \mu(r_2, s_2)$ if and only if $r_1 + s_1 < r_2 + s_2$, or $r_1 + s_1 = r_2 + s_2$ and $s_1 < s_2$.

Note that the superregularity of the matrix $\mathfrak{G}$ (also the superregularity of the matrices $\mathcal{G}_1$ and $\mathcal{G}_2$) implies that all the entries in the polynomial vector $\widehat{G}_r(z_1, z_2)$, for $r = 1, 2, \ldots, t, t+1, t+2, \ldots, k$, are nonzero. Moreover, $\widehat{G}_r(z_1, z_2)$ has degree $\lfloor \frac{\delta}{k} \rfloor + 1$, for $r = 1, 2, \ldots, t$, and degree $\lfloor \frac{\delta}{k} \rfloor$, for $r = t+1, t+2, \ldots, k$.

Finally, we define the encoder

$$\widehat{G}(z_1, z_2) = \begin{bmatrix} \widehat{G}_1(z_1, z_2) & \widehat{G}_2(z_1, z_2) & \cdots & \widehat{G}_t(z_1, z_2) & \cdots & \widehat{G}_k(z_1, z_2) \end{bmatrix} \in \mathbb{F}[z_1, z_2]^{n\times k}, \tag{9}$$

for which the column degrees of the first t columns are $\lfloor \frac{\delta}{k} \rfloor + 1$ and the column degrees of the last $k - t$ columns are $\lfloor \frac{\delta}{k} \rfloor$, that is, expression (4) holds. Now, since $t = \delta - k\lfloor \frac{\delta}{k} \rfloor$ it follows that $\nu_1 + \nu_2 + \cdots + \nu_k = \delta$, i.e., $\delta_e(\widehat{G}(z_1, z_2)) = \delta$.

Note that $\lfloor \frac{\delta}{k} \rfloor + 1$ is the total degree of $\widehat{G}(z_1, z_2)$; therefore, according to expressions (1) and (7) we can write expression (9) as

$$\widehat{G}(z_1, z_2) = \sum_{0\le i+j\le \lfloor \frac{\delta}{k} \rfloor + 1} G(i, j) z_1^i z_2^j \tag{10}$$

where

$$G(i, j) = \begin{cases} \begin{bmatrix} \boldsymbol{g}^1_{\mu(i,j)} & \boldsymbol{g}^2_{\mu(i,j)} & \cdots & \boldsymbol{g}^t_{\mu(i,j)} & \boldsymbol{g}^{t+1}_{\mu(i,j)} & \cdots & \boldsymbol{g}^k_{\mu(i,j)} \end{bmatrix}, & \text{if } 0 \le i+j \le \lfloor \frac{\delta}{k} \rfloor, \\ \begin{bmatrix} \boldsymbol{g}^1_{\mu(i,j)} & \boldsymbol{g}^2_{\mu(i,j)} & \cdots & \boldsymbol{g}^t_{\mu(i,j)} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}, & \text{if } i+j = \lfloor \frac{\delta}{k} \rfloor + 1, \end{cases} \tag{11}$$

or equivalently

$$\widehat{G}(z_1, z_2) = \begin{bmatrix} \mathcal{I}_0(z_1, z_2) & \mathcal{I}_1(z_1, z_2) & \cdots & \mathcal{I}_{\lfloor \frac{\delta}{k} \rfloor + 1}(z_1, z_2) \end{bmatrix} \mathcal{G}, \tag{12}$$

with

$$\mathcal{I}_\xi(z_1,z_2)=\left[\begin{array}{cccccc} Iz_1^\xi z_2^0 & Iz_1^{\xi-1}z_2^1 & \cdots & Iz_1^1 z_2^{\xi-1} & Iz_1^0 z_2^\xi \end{array}\right], \quad \text{for } \xi=0,1,2,\ldots,\left\lfloor\frac{\delta}{k}\right\rfloor+1,$$

and I is the $n\times n$ identity matrix.

Next result establishes that $\widehat{G}(z_1,z_2)$ is an encoder of a 2D convolutional code of rate k/n and degree δ.

Lemma 3: *Let $\widehat{G}(z_1,z_2)$ be the matrix defined by expression (9). Then $\mathcal{C}=\mathrm{Im}_{\mathbb{F}[z_1,z_2]}\,\widehat{G}(z_1,z_2)$ is a 2D convolutional code of rate k/n and degree δ.*

Proof: Let us show that $\widehat{G}(z_1,z_2)$ is a full column rank matrix and that $\mathcal{C}$ has degree δ.

We need first to prove that $\widehat{G}(z_1,z_2)$ has a nonzero full size minor. Let $\bar{G}(z_1,z_2)$ be the $k\times k$ submatrix of $\widehat{G}(z_1,z_2)$ constituted by the first k rows of $\widehat{G}(z_1,z_2)$. Since $\widehat{G}(z_1,z_2)$ has external degree $\delta_e(\widehat{G}(z_1,z_2))=\delta$, we have that

$$\det(\bar{G}(z_1,z_2))=\sum_{0\leq i+j\leq\delta} m_{ij}z_1^i z_2^j, \quad \text{where} \quad m_{ij}\in\mathbb{F},$$

i.e., $\det(\bar{G}(z_1,z_2))$ is a polynomial of degree less than or equal to δ. Note that $m_{0\delta}=\det(M_{0\delta})$, where $M_{0\delta}$ is the $k\times k$ submatrix of $\mathfrak{G}$ constituted by the first k rows of the matrix

$$\left[\begin{array}{cccccc} \boldsymbol{g}^1_{\ell_1-1} & \boldsymbol{g}^2_{\ell_1-1} & \cdots & \boldsymbol{g}^t_{\ell_1-1} & \boldsymbol{g}^{t+1}_{\ell_2-1} & \cdots & \boldsymbol{g}^k_{\ell_2-1} \end{array}\right].$$

The superregularity of $\mathfrak{G}$ implies that $m_{0\delta}\neq 0$, consequently $\det(\bar{G}(z_1,z_2))\neq 0$ and therefore $\widehat{G}(z_1,z_2)$ is a full column rank matrix.

Moreover, it also implies that $\deg\det(\bar{G}(z_1,z_2))=\delta$ and in turn $\delta\leq\delta_i(\widehat{G}(z_1,z_2))$. It follows that the complexity $\widehat{\delta}$ of $\mathcal{C}$ is lower bounded by δ, i.e., $\widehat{\delta}\geq\delta$. In addition, since $\widehat{\delta}\leq\delta$ we obtain that $\widehat{\delta}=\delta$. By Remark 1 we conclude that $\mathcal{C}$ has degree δ. ■

Next we show that $\widehat{G}(z_1,z_2)$ as defined in expression (9) generates a 2D convolutional code with distance equal to the 2D generalized Singleton bound given in expression (3), i.e., that $\widehat{G}(z_1,z_2)$ generates an MDS 2D convolutional code.

First we need to consider several technical results. The first one introduces a lower bound on the weight of codewords generated by a single monomial $\boldsymbol{u}z_1^r z_2^s$.

Lemma 4: *Let $\widehat{G}(z_1,z_2)$ be the matrix defined by expression (9) and assume that $\widehat{\boldsymbol{u}}(z_1,z_2)=\boldsymbol{u}z_1^r z_2^s$ for some $\boldsymbol{u}\in\mathbb{F}^k\setminus\{\boldsymbol{0}\}$ and $(r,s)\in\mathbb{N}_0$. If $\widehat{\boldsymbol{v}}(z_1,z_2)=\widehat{G}(z_1,z_2)\widehat{\boldsymbol{u}}(z_1,z_2)$ then*

$$\mathrm{wt}\,(\widehat{\boldsymbol{v}}(z_1,z_2))\geq n\ell_2-(k-t)+1.$$

Proof: Since $\mathrm{wt}\left(\widehat{G}(z_1,z_2)\boldsymbol{u}z_1^r z_2^s\right)=\mathrm{wt}\left(\widehat{G}(z_1,z_2)\boldsymbol{u}\right)$, we can assume, without loss of generality, that $\widehat{\boldsymbol{u}}(z_1,z_2)=\boldsymbol{u}$.

Let us consider the matrix $\mathcal{G}$ of expression (6), $\boldsymbol{u} = \begin{bmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \end{bmatrix}$, with $\boldsymbol{u}_1 \in \mathbb{F}^t$ and $\boldsymbol{u}_2 \in \mathbb{F}^{k-t}$, and assume that $\boldsymbol{v} = \mathcal{G}\boldsymbol{u}$. Then $\boldsymbol{v} = \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \end{bmatrix}$, where $\boldsymbol{v}_1 = \mathcal{G}_1\boldsymbol{u}$ and $\boldsymbol{v}_2 = \mathcal{G}_2\boldsymbol{u}_1$.

Note that $\boldsymbol{v}_1$ is a nontrivial linear combination of columns of an $n\ell_2 \times k$ superregular matrix and $\boldsymbol{v}_2$ is a linear combination of columns of an $n(\ell_1 - \ell_2) \times t$ superregular matrix. We consider two cases.

Case 1: $\boldsymbol{u}_1 = \boldsymbol{0}$. In this case, we have that $\boldsymbol{v} = \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{0} \end{bmatrix}$ where $\boldsymbol{v}_1$ is a nontrivial linear combination of the columns of an $n\ell_2 \times (k-t)$ superregular matrix, with $k - t < n\ell_2$. By Lemma 2, $\mathrm{wt}\,(\boldsymbol{v}) \geq n\ell_2 - (k-t) + 1$.

Case 2: $\boldsymbol{u}_1 \neq \boldsymbol{0}$. Then $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are nontrivial linear combinations of the columns of an $n\ell_2 \times k$ and an $n(\ell_1 - \ell_2) \times t$ superregular matrices, respectively. Further, as $n\ell_2 > k$ and $n(\ell_1 - \ell_2) > t$, it follows from Lemma 2 that $\mathrm{wt}\,(\boldsymbol{v}_1) \geq n\ell_2 - k + 1$ and $\mathrm{wt}\,(\boldsymbol{v}_2) \geq n(\ell_1 - \ell_2) - t + 1$ and consequently we obtain

$$\mathrm{wt}\,(\boldsymbol{v}) = \mathrm{wt}\,(\boldsymbol{v}_1) + \mathrm{wt}\,(\boldsymbol{v}_2) \geq n\ell_1 - k - t + 2 \geq n\ell_2 - (k-t) + 1$$

where the last inequality follows from the fact that $\ell_1 \geq \ell_2 + 2$ and $n > t$.

By expression (12), $\mathrm{wt}\left(\widehat{G}(z_1, z_2)\widehat{\boldsymbol{u}}(z_1, z_2)\right) = \mathrm{wt}\,(\boldsymbol{v})$ and the result follows. ■

Next, we derive a lower bound on the weight of codewords generated by any nonzero polynomial vector $\widehat{\boldsymbol{u}}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k$. We consider the case $\delta < k$ in Lemma 5 and then the case $\delta \geq k$ in Lemma 6.

It will be useful to write the information vector $\widehat{\boldsymbol{u}}(z_1, z_2)$ as the sum of M different monomials

$$\widehat{\boldsymbol{u}}(z_1, z_2) = \sum_{m=1}^{M} \boldsymbol{u}(r_m, s_m) z_1^{r_m} z_2^{s_m}, \tag{13}$$

and consequently, the corresponding codeword $\widehat{\boldsymbol{v}}(z_1, z_2) = \widehat{G}(z_1, z_2)\widehat{\boldsymbol{u}}(z_1, z_2)$ as

$$\widehat{\boldsymbol{v}}(z_1, z_2) = \sum_{m=1}^{M} \widehat{\boldsymbol{v}}_m(z_1, z_2), \tag{14}$$

where, for $m = 1, 2, \ldots, M$,

$$\begin{aligned} \widehat{\boldsymbol{v}}_m(z_1, z_2) &= \widehat{G}(z_1, z_2)\boldsymbol{u}(r_m, s_m) z_1^{r_m} z_2^{s_m} \\ &= \sum_{0 \leq i+j \leq \left\lfloor \frac{\delta}{k} \right\rfloor + 1} G(i, j)\boldsymbol{u}(r_m, s_m) z_1^{i+r_m} z_2^{j+s_m} \end{aligned} \tag{15}$$

and therefore

$$\mathrm{Supp}\,(\widehat{\boldsymbol{v}}_m(z_1, z_2)) \subseteq \left\{ (a, b) \mid r_m + s_m \leq a + b \leq r_m + s_m + \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right\}. \tag{16}$$

We can assume, without loss of generality, that

$$\mu(r_m, s_m) < \mu(r_{m+1}, s_{m+1}), \quad \text{for } m = 1, 2, \ldots, M-1,$$

where μ is the map defined in expression (8). So,

$$r_m + s_m < r_{m+1} + s_{m+1}, \quad \text{or} \quad r_m + s_m = r_{m+1} + s_{m+1} \text{ and } s_m < s_{m+1}. \tag{17}$$

We assume from now on that $n \geq \ell_1 k$. However, we conjecture that the code presented above is an MDS 2D convolutional code for any given parameters n, k, and δ.

Lemma 5: *Assume that $\delta < k$ and $n \geq \ell_1 k$. Let $\widehat{G}(z_1, z_2)$ be the matrix defined by expression (9). If $\widehat{\boldsymbol{u}}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k$ is a nonzero vector and $\widehat{\boldsymbol{v}}(z_1, z_2) = \widehat{G}(z_1, z_2)\widehat{\boldsymbol{u}}(z_1, z_2)$ then*

$$\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right) \geq n - (k - t) + 1.$$

Proof: Since $\delta < k$ we have that $\left\lfloor \frac{\delta}{k} \right\rfloor = 0$ which implies that $\ell_1 = 3$ and $t = \delta$. Moreover, from expression (10) we have that

$$\widehat{G}(z_1, z_2) = G(0,0) + G(1,0)z_1 + G(0,1)z_2 \tag{18}$$

with $G(1,0)$ and $G(0,1)$ having at most t nonzero columns.

Note that if $M = 1$, the result follows from Lemma 4. Hence, assume $M \geq 2$.

From expressions (18) and (13), we have that

$$\widehat{\boldsymbol{v}}(z_1, z_2) = \sum_{m=1}^{M} \left(G(0,0)\boldsymbol{u}(r_m, s_m) z_1^{r_m} z_2^{s_m} + G(1,0)\boldsymbol{u}(r_m, s_m) z_1^{r_m+1} z_2^{s_m} + G(0,1)\boldsymbol{u}(r_m, s_m) z_1^{r_m} z_2^{s_m+1} \right) \tag{19}$$

and from expressions (2), (10), (17) and (19) it follows that $\boldsymbol{v}(r_1, s_1) = G(0,0)\boldsymbol{u}(r_1, s_1)$. Note that the superregularity of $G(0,0)$ and the fact that $\boldsymbol{u}(r_1, s_1) \neq \mathbf{0}$, imply that $\mathrm{wt}\left(\boldsymbol{v}(r_1, s_1)\right) \geq n - k + 1$; so, $\boldsymbol{v}(r_1, s_1) \neq \mathbf{0}$ and therefore $(r_1, s_1) \in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right)$.

If $(r_2, s_2) \notin \{(r_1 + 1, s_1), (r_1, s_1 + 1)\}$, from expressions (10), (18), (13) and (19) we have that $\boldsymbol{v}(r_2, s_2) = G(0,0)\boldsymbol{u}(r_2, s_2)$ and, as in the previous case, $\mathrm{wt}\left(\boldsymbol{v}(r_2, s_2)\right) \geq n - k + 1$. So $\boldsymbol{v}(r_2, s_2) \neq \mathbf{0}$, and therefore, $(r_2, s_2) \in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right)$.

On the other hand, if $(r_2, s_2) \in \{(r_1 + 1, s_1), (r_1, s_1 + 1)\}$, again from expressions (10), (18), (13) and (19) we have that

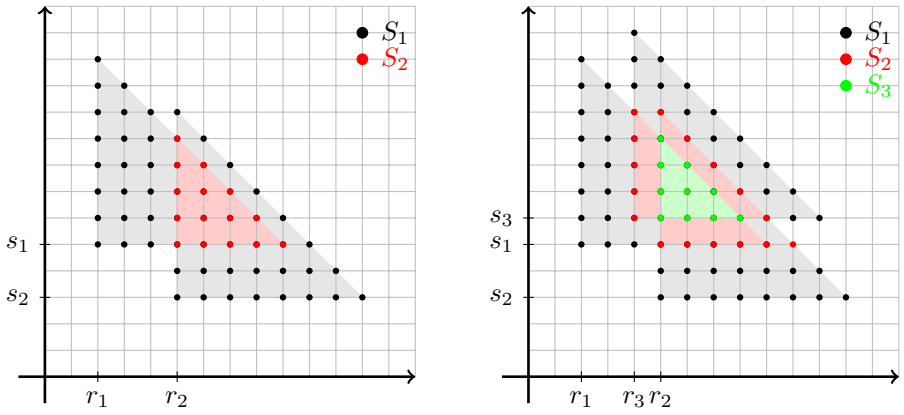
$$\boldsymbol{v}(r_2, s_2) = \begin{cases} G(0,0)\boldsymbol{u}(r_2, s_2) + G(1,0)\boldsymbol{u}(r_1, s_1), & \text{if } (r_2, s_2) = (r_1 + 1, s_1), \\ G(0,0)\boldsymbol{u}(r_2, s_2) + G(0,1)\boldsymbol{u}(r_1, s_1), & \text{if } (r_2, s_2) = (r_1, s_1 + 1), \end{cases}$$

and using the fact that $G(1,0)$ and $G(0,1)$ have at most t nonzero columns it readily follows that $\mathrm{wt}\left(\boldsymbol{v}(r_2, s_2)\right) \geq n - k - t + 1$. So $\boldsymbol{v}(r_2, s_2) \neq \mathbf{0}$, and therefore, $(r_2, s_2) \in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right)$.

Taking into account that $k > t$, $n \geq 3k$, and that in either of the two cases $\mathrm{wt}\left(\boldsymbol{v}(r_2, s_2)\right) \geq n - k - t + 1$, it follows that

$$\begin{aligned} \mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right) &= \sum_{(i,j) \in \mathrm{Supp}(\widehat{\boldsymbol{v}}(z_1, z_2))} \mathrm{wt}\left(\boldsymbol{v}(i,j)\right) \geq \mathrm{wt}\left(\boldsymbol{v}(r_1, s_1)\right) + \mathrm{wt}\left(\boldsymbol{v}(r_2, s_2)\right) \\ &\geq n - k + 1 + n - k - t + 1 > 2n - 3k + 2 \geq n + 2 \geq n - (k - t) + 1. \end{aligned}$$

■



(a) S_1 and S_2 (b) S_1, S_2 and S_3

Fig. 1: The set $\bigcup_{m=1}^{M} S_m$ for $\delta = 7$ and different values of M

Lemma 6: *Assume that $\delta \geq k$ and $n \geq \ell_1 k$. Let $\widehat{G}(z_1, z_2)$ be the matrix defined by expression (9). If $\widehat{\boldsymbol{u}}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^k$ is a nonzero vector and $\widehat{\boldsymbol{v}}(z_1, z_2) = \widehat{G}(z_1, z_2)\widehat{\boldsymbol{u}}(z_1, z_2)$, then*

$$\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right) \geq n\ell_2 - (k - t) + 1.$$

Proof: Since $\delta \geq k$ we have that $\left\lfloor \frac{\delta}{k} \right\rfloor \geq 1$.

Consider $\widehat{\boldsymbol{u}}(z_1, z_2)$, $\widehat{\boldsymbol{v}}(z_1, z_2)$, and $\widehat{\boldsymbol{v}}_m(z_1, z_2)$ as in expressions (13), (14), and (15). For $m = 1, 2, \ldots, M$, define the sets

$$S_m = \left\{(i, j) \in \mathbb{N}_0^2 \mid (i, j) \in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_c(z_1, z_2)\right) \text{ for exactly } m \text{ values of } c \in \{1, 2, \ldots, M\}\right\}.$$

See Figure 1 for $M = 2, 3$.

It follows then that

$$\bigcup_{m=1}^{M} \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_m(z_1, z_2)\right) = \bigcup_{m=1}^{M} S_m \tag{20}$$

and that

$$\sum_{m=1}^{M} \#\,\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_m(z_1, z_2)\right) = \sum_{m=1}^{M} m\,\#\,S_m. \tag{21}$$

Since there are ℓ_1 pairs (a, b) such that $r_m + s_m \leq a + b \leq r_m + s_m + \left\lfloor \frac{\delta}{k} \right\rfloor + 1$ (see expression (16)) and the pairs (r_m, s_m) are pairwise distinct, every $(i, j) \in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1, z_2)\right)$ is contained in $\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_m(z_1, z_2)\right)$ for at most ℓ_1 different values of m. This shows that $S_m = \emptyset$ for $m > \ell_1$.

If $(i, j) \in S_m$, we have that $(i, j) \in \bigcap_{w=1}^{m} \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_{a_w}(z_1, z_2)\right)$ for some $a_1, a_2, \ldots, a_m \in \{1, 2, \ldots, M\}$, and therefore from expression (2), the coefficient $\boldsymbol{v}(i, j)$ is given by

$$\boldsymbol{v}(i, j) = \sum_{w=1}^{m} G(i - r_{a_w}, j - s_{a_w})\boldsymbol{u}(r_{a_w}, s_{a_w}).$$

By expression (11), this is a linear combination of at most mk columns of $\mathcal{G}$ and as $n \geq k\ell_1 \geq km$, it follows that

$$\mathrm{wt}\left(\boldsymbol{v}(i, j)\right) \geq n - (mk - 1), \quad \text{for } (i, j) \in S_m, \tag{22}$$

and therefore $\boldsymbol{v}(i,j)$ is always different from zero. This yields that

$$\mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right)=\bigcup_{m=1}^{M}\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)$$

and consequently, from expression (20),

$$\#\ \mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right)=\sum_{m=1}^{M}\#\,S_m. \tag{23}$$

Let us see now that $\sum_{m=1}^{M}\#S_m\geq \ell_2+M$.

Bearing in mind expression (17) it follows that

$$\#\ \mathrm{Supp}\left(\sum_{m=1}^{L}\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)\geq \#\ \mathrm{Supp}\left(\sum_{m=2}^{L}\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)+1,\quad \text{for all } L \text{ with } 2\leq L\leq M,$$

and therefore

$$\begin{aligned}\#\ \mathrm{Supp}\left(\sum_{m=1}^{M}\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)&\geq \#\ \mathrm{Supp}\left(\sum_{m=2}^{M}\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)+1\\ &\geq\cdots\geq \#\ \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_{M-1}(z_1,z_2)+\widehat{\boldsymbol{v}}_M(z_1,z_2)\right)+M-2.\end{aligned} \tag{24}$$

We study now the value of $\#\ \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_{M-1}(z_1,z_2)+\widehat{\boldsymbol{v}}_M(z_1,z_2)\right)$.

Note that $r_M=r_{M-1}$ and $s_M\neq s_{M-1}$, or $r_M\neq r_{M-1}$. This implies that either

$$(r_{M-1}+a,s_{M-1})\in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_{M-1}(z_1,z_2)\right)\setminus\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_M(z_1,z_2)\right),\quad \text{for } a=0,1,\ldots,\left\lfloor\frac{\delta}{k}\right\rfloor$$

or

$$(r_{M-1},s_{M-1}+b)\in \mathrm{Supp}\left(\widehat{\boldsymbol{v}}_{M-1}(z_1,z_2)\right)\setminus\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_M(z_1,z_2)\right),\quad \text{for } b=0,1,\ldots,\left\lfloor\frac{\delta}{k}\right\rfloor.$$

Then, using that $\#\,\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_M(z_1,z_2)\right)\geq\ell_2$ we obtain that

$$\#\ \mathrm{Supp}\left(\left(\widehat{\boldsymbol{v}}_M(z_1,z_2)+\widehat{\boldsymbol{v}}_{M-1}(z_1,z_2)\right)\right)\geq \#\ \mathrm{Supp}\left(\left(\widehat{\boldsymbol{v}}_M(z_1,z_2)\right)\right)+\left\lfloor\frac{\delta}{k}\right\rfloor+1\geq\ell_2+2,$$

which together with expressions (23) and (24) implies that

$$\sum_{m=1}^{M}\#S_m=\#\,\mathrm{Supp}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right)=\#\,\mathrm{Supp}\left(\sum_{m=1}^{M}\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)\geq\ell_2+M. \tag{25}$$

Finally, observe that since $\#\,\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)\leq\ell_1$, for $m=1,2,\ldots,M$, then by expressions (21) and (25), it follows that

$$\begin{aligned}\sum_{m=1}^{M}(mk-1)\,\#S_m&=\sum_{m=1}^{M}mk\,\#S_m-\sum_{m=1}^{M}\#S_m\\ &\leq k\sum_{m=1}^{M}\#\,\mathrm{Supp}\left(\widehat{\boldsymbol{v}}_m(z_1,z_2)\right)-\ell_2-M\leq M\ell_1k-2.\end{aligned} \tag{26}$$

Then, since $\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right)=\sum_{m=1}^{M}\sum_{(i,j)\in S_m}\mathrm{wt}\left(\boldsymbol{v}(i,j)\right)$, it follows by expression (22) that

$$\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right)=\sum_{m=1}^{M}\sum_{(i,j)\in S_m}\mathrm{wt}\left(\boldsymbol{v}(i,j)\right)\geq\sum_{m=1}^{M}\sum_{(i,j)\in S_m}(n-(mk-1))$$

$$= \sum_{m=1}^{M} (n-(mk-1))\#S_m = n\sum_{m=1}^{M}\#S_m - \sum_{m=1}^{M}(mk-1)\#S_m$$

and therefore, by expressions (25) and (26) and the fact that $n \geq \ell_1 k$, we obtain

$$\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right) \geq n\ell_2 + nM - M\ell_1 k + 2 \geq n\ell_2 + 2 \geq n\ell_2 - (k-t) + 1,$$

which concludes the proof. ■

Next we will prove that $\widehat{G}(z_1,z_2)$ constructed in expression (9) is an encoder of an MDS 2D convolutional code if $n \geq k\ell_1$.

Theorem 2: *Let $\widehat{G}(z_1,z_2)$ be the matrix defined by expression (9). If $n \geq k\ell_1$, then $\mathcal{C} = \mathrm{Im}_{\mathbb{F}[z_1,z_2]}\,\widehat{G}(z_1,z_2)$ is an MDS 2D convolutional code of rate k/n and degree δ.*

Proof: The fact that $\mathcal{C}$ is a 2D convolutional code of rate k/n and degree δ follows from Lemma 3.

Since $t = \delta - k\left\lfloor \frac{\delta}{k} \right\rfloor$, it follows that

$$n\ell_2 - (k-t) + 1 = n\frac{\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right)}{2} - k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

According to Definition 5, to prove that $\mathcal{C}$ is MDS, we need to show that if $\widehat{\boldsymbol{v}}(z_1,z_2) \in \mathcal{C}$ is a nonzero codeword, then

$$\mathrm{wt}\left(\widehat{\boldsymbol{v}}(z_1,z_2)\right) \geq n\ell_2 - (k-t) + 1. \tag{27}$$

Since $\widehat{\boldsymbol{v}}(z_1,z_2) \neq \mathbf{0}$, it follows that $\widehat{\boldsymbol{v}}(z_1,z_2) = \widehat{G}(z_1,z_2)\widehat{\boldsymbol{u}}(z_1,z_2)$ for some $\widehat{\boldsymbol{u}}(z_1,z_2) \in \mathbb{F}[z_1,z_2]^k$ with $\widehat{\boldsymbol{u}}(z_1,z_2) \neq \mathbf{0}$ which we can write as the sum of M different nonzero monomials as in expression (13).

If $M = 1$, the proof of the theorem follows from Lemma 4. Assume then that $M > 1$.

If $\delta < k$, then $\ell_1 = 3$ and therefore $n \geq 3k$; it follows then that $\ell_2 = 1$ and inequality (27) holds by Lemma 5. Finally, if $\delta \geq k$, inequality (27) holds by Lemma 6. ■

So far we have assumed that $k \nmid \delta$. Assume now that $k \mid \delta$, i.e., $t = 0$. As in the previous case, we consider matrices

$$A_r = \left[\begin{array}{cccc} \boldsymbol{g}_0^r & \boldsymbol{g}_1^r & \cdots & \boldsymbol{g}_{\ell_2-1}^r \end{array}\right] \in \mathbb{F}^{n\times\ell_2} \quad \text{for} \quad r = 1,2,\ldots,k$$

such that

$$\begin{aligned} \mathfrak{G} &= \left[\begin{array}{cccc} A_1 & A_2 & \cdots & A_k \end{array}\right] \in \mathbb{F}^{n\times k\ell_2}, \\ \mathcal{G} &= \left[\begin{array}{cccc} \mathrm{rsh}\,(A_1) & \mathrm{rsh}\,(A_2) & \cdots & \mathrm{rsh}\,(A_k) \end{array}\right] \in \mathbb{F}^{n\ell_2\times k} \end{aligned} \tag{28}$$

are superregular matrices. Then

$$\widehat{G}_r(z_1,z_2) = \sum_{0\leq i+j\leq \frac{\delta}{k}} \boldsymbol{g}_{\mu(i,j)}^r z_1^i z_2^j \in \mathbb{F}[z_1,z_2]^n \quad \text{for} \quad r = 1,2,\ldots,k$$

is a polynomial vector of degree $\frac{\delta}{k}$ with coefficients vectors $\boldsymbol{g}_w^r \in \mathbb{F}^n$, for $w = 0,1,\ldots,\ell_2-1$, and the encoder

$$\widehat{G}(z_1,z_2) = \left[\begin{array}{cccc} \widehat{G}_1(z_1,z_2) & \widehat{G}_2(z_1,z_2) & \cdots & \widehat{G}_k(z_1,z_2) \end{array}\right] \in \mathbb{F}[z_1,z_2]^{n\times k}, \tag{29}$$

has column degrees $\nu_r = \frac{\delta}{k}$, for $r = 1, 2, \ldots, k$ and, consequently, $\delta_e(\widehat{G}(z_1, z_2)) = \delta$.

Remark 3: It is not difficult to show that Lemmas 3, 4, 5 and 6, and Theorem 2 (with $n \geq k\ell_2$ instead of $n \geq k\ell_1$) also hold for matrix $\widehat{G}(z_1, z_2)$ defined as in (29) instead of the same matrix defined as in (9).

V. Construction and Examples

In this section, we use the method introduced by Roth in [26] to obtain a circulant Cauchy matrix (see also [27]). These matrices will allow us to obtain the superregular matrices $\mathfrak{G}$, $\mathcal{G}_1$ and $\mathcal{G}_2$, if $t \neq 0$, (or $\mathfrak{G}$ and $\mathcal{G}$ if $t = 0$) needed to construct the MDS 2D convolutional codes presented in the previous section.

Theorem 3: *Let k and δ be positive integers and consider t, ℓ_1 and ℓ_2 as defined in Section IV. Assume that $n \geq k\ell$, with*

$$\ell = \begin{cases} \ell_1, & \text{if } t \neq 0, \\ \ell_2, & \text{if } t = 0. \end{cases}$$

Assume also that $\mathbb{F}$ is a finite field with q elements where q is an odd number such that $q \geq 2n\ell + 1$. Let α be an element of order $\frac{(q-1)}{2}$ (that is α is a square of a primitive element of $\mathbb{F}$) and let b be a nonsquare element in $\mathbb{F}$. Consider the $(\frac{q-1}{2}) \times (\frac{q-1}{2})$ Cauchy circulant matrix $C = \left[c_{ij} \right]$ where

$$c_{ij} = \frac{1}{1 - b\alpha^{j-i}}, \quad \text{for} \quad 0 \leq i, j \leq \frac{q-3}{2}.$$

1) *For $t \neq 0$, we define the matrices $\mathcal{G}_1$ and $\mathcal{G}_2$ in the following way*

$$\begin{aligned} \mathcal{G}_1 &= \left[\begin{array}{cccccccc} \operatorname{rsh}(A_1) & \operatorname{rsh}(A_2) & \cdots & \operatorname{rsh}(A_t) & \operatorname{rsh}(A_{t+1}) & \cdots & \operatorname{rsh}(A_k) \end{array} \right] \\ &= \left[\begin{array}{cccccc} \boldsymbol{g}_0^1 & \boldsymbol{g}_0^2 & \cdots & \boldsymbol{g}_0^t & \boldsymbol{g}_0^{t+1} & \cdots & \boldsymbol{g}_0^k \\ \boldsymbol{g}_1^1 & \boldsymbol{g}_1^2 & \cdots & \boldsymbol{g}_1^t & \boldsymbol{g}_1^{t+1} & \cdots & \boldsymbol{g}_1^k \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \boldsymbol{g}_{\ell_2-1}^1 & \boldsymbol{g}_{\ell_2-1}^2 & \cdots & \boldsymbol{g}_{\ell_2-1}^t & \boldsymbol{g}_{\ell_2-1}^{t+1} & \cdots & \boldsymbol{g}_{\ell_2-1}^k \end{array} \right], \\ \mathcal{G}_2 &= \left[\begin{array}{cccc} \operatorname{rsh}(B_1) & \operatorname{rsh}(B_2) & \cdots & \operatorname{rsh}(B_t) \end{array} \right] \\ &= \left[\begin{array}{cccc} \boldsymbol{g}_{\ell_2}^1 & \boldsymbol{g}_{\ell_2}^2 & \cdots & \boldsymbol{g}_{\ell_2}^t \\ \boldsymbol{g}_{\ell_2+1}^1 & \boldsymbol{g}_{\ell_2+1}^2 & \cdots & \boldsymbol{g}_{\ell_2+1}^t \\ \vdots & \vdots & & \vdots \\ \boldsymbol{g}_{\ell_1-1}^1 & \boldsymbol{g}_{\ell_1-1}^2 & \cdots & \boldsymbol{g}_{\ell_1-1}^t \end{array} \right] \end{aligned}$$

where

$$\boldsymbol{g}_j^r = \begin{bmatrix} c_{jn,r-1} \\ c_{jn+1,r-1} \\ \vdots \\ c_{(j+1)n-1,r-1} \end{bmatrix} \tag{30}$$

for $(j,r) \in (\{0,1,\ldots,\ell_2-1\}\times\{1,2,\ldots,k\}) \cup (\{\ell_2,\ell_2+1,\ldots,\ell_1-1\}\times\{1,2,\ldots,t\})$. *Moreover, let* $\mathfrak{G}$ *be the matrix defined in expression (5) obtained from* $\mathcal{G}_1$ *and* $\mathcal{G}_2$. *Then* $\mathfrak{G}$, $\mathcal{G}_1$ *and* $\mathcal{G}_2$ *are superregular matrices.*

2) *For* $t = 0$, *we define the matrix* $\mathcal{G}$ *in the following way*

$$\mathcal{G} = \left[\begin{array}{cccc} \mathrm{rsh}\,(A_1) & \mathrm{rsh}\,(A_2) & \cdots & \mathrm{rsh}\,(A_k) \end{array} \right] = \left[\begin{array}{cccc} \boldsymbol{g}_0^1 & \boldsymbol{g}_0^2 & \cdots & \boldsymbol{g}_0^k \\ \boldsymbol{g}_1^1 & \boldsymbol{g}_1^2 & \cdots & \boldsymbol{g}_1^k \\ \vdots & \vdots & & \vdots \\ \boldsymbol{g}_{\ell_2-1}^1 & \boldsymbol{g}_{\ell_2-1}^2 & \cdots & \boldsymbol{g}_{\ell_2-1}^k \end{array} \right]$$

where $\boldsymbol{g}_j^r$ *is defined as in (30) for* $(j,r) \in (\{0,1,\ldots,\ell_2-1\}\times\{1,2,\ldots,k\})$. *Moreover, let* $\mathfrak{G}$ *be the matrix defined in expression (28) obtained from* $\mathcal{G}$. *Then* $\mathfrak{G}$ *and* $\mathcal{G}$ *are superregular matrices.*

Proof: 1) The assumptions on α and b ensure that C is a Cauchy circulant matrix (see [26, page 1317]), and therefore, that C is a superregular matrix (see also [22, page 323]). The matrices $\mathcal{G}_1$ and $\mathcal{G}_2$ are superregular because they are submatrices of C.

Now, taking into account that $\alpha^{\frac{q-1}{2}} = 1$, it follows that

$$c_{u,v} = \frac{1}{1-b\alpha^{v-u}} = \frac{1}{1-b\alpha^{\frac{q-1}{2}-u+v}} = c_{0,\frac{q-1}{2}-u+v}, \quad \text{for } 0 \le u,v \le \frac{q-3}{2}$$

and, consequently,

$$\boldsymbol{g}_j^r = \left[\begin{array}{c} c_{0,\frac{q-1}{2}-jn+r-1} \\ c_{1,\frac{q-1}{2}-jn+r-1} \\ \vdots \\ c_{n-1,\frac{q-1}{2}-jn+r-1} \end{array} \right],$$

$$\text{for } (j,r) \in (\{0,1,\ldots,\ell_2-1\}\times\{1,2,\ldots,k\}) \cup (\{\ell_2,\ell_2+1,\ldots,\ell_1-1\}\times\{1,2,\ldots,t\}).$$

So, after the appropriate rearrangement of the columns of $\mathfrak{G}$, we obtain a submatrix of the Cauchy matrix C formed by the first n rows and the $\ell_2 k + (\ell_1-\ell_2)t$ columns defined by the above expression. Consequently, $\mathfrak{G}$ is also a superregular matrix.

2) Analogous to 1). ■

By Theorem 2, from the matrices $\mathfrak{G}$, $\mathcal{G}_1$ and $\mathcal{G}_2$, if $t \neq 0$, or the matrices $\mathfrak{G}$ and $\mathcal{G}$, if $t = 0$, defined in Theorem 3, we construct an encoder $\widehat{G}(z_1,z_2)$ of an MDS 2D convolutional code of rate k/n and degree δ. The following two examples help us to understand the above construction.

Example 2: Let $k = 2$ and $\delta = 2$. Then $t = 0$ and $\ell = \ell_2 = 3$. Since $k\ell = 6$, we consider $n = 6$. Furthermore, since $2n\ell + 1 = 37$, we consider $q = 37$ which is an odd prime.

Then the Cauchy circulant matrix $C = \left[c_{ij} \right]$ defined by

$$c_{ij} = \frac{1}{1-b\alpha^{j-i}}, \quad \text{for} \quad 0 \le i,j \le 17$$

with $\alpha = 4$ and $b = 5$ is

$$C = \begin{bmatrix}
9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 \\
33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 \\
25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 \\
13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 \\
5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 \\
29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 \\
3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 \\
16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 \\
30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 \\
31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 \\
21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 & 36 \\
36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 & 2 \\
2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 & 17 \\
17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 & 7 \\
7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 & 8 \\
8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 & 22 \\
22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9 & 35 \\
35 & 22 & 8 & 7 & 17 & 2 & 36 & 21 & 31 & 30 & 16 & 3 & 29 & 5 & 13 & 25 & 33 & 9
\end{bmatrix}.$$

Thus according to part 2 of Theorem 3, the matrix $\mathcal{G}$ is constituted by the first two columns of C, i.e.,

$$\mathcal{G} = \begin{bmatrix} \mathrm{rsh}\,(A_1) & \mathrm{rsh}\,(A_2) \end{bmatrix} = \begin{bmatrix} \boldsymbol{g}_0^1 & \boldsymbol{g}_0^2 \\ \boldsymbol{g}_1^1 & \boldsymbol{g}_1^2 \\ \boldsymbol{g}_2^1 & \boldsymbol{g}_2^2 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 33 & 25 & 13 & 5 & 29 & 3 & 16 & 30 & 31 & 21 & 36 & 2 & 17 & 7 & 8 & 22 & 35 \\ 35 & 9 & 33 & 25 & 13 & 5 & 29 & 3 & 16 & 30 & 31 & 21 & 36 & 2 & 17 & 7 & 8 & 22 \end{bmatrix}^T.$$

This matrix is superregular because it is a submatrix of C.

The matrix $\mathfrak{G}$ obtained from matrix $\mathcal{G}$ is

$$\mathfrak{G} = \begin{bmatrix} A_1 & A_2 \end{bmatrix} = \left[\begin{array}{ccc|ccc} \boldsymbol{g}_0^1 & \boldsymbol{g}_1^1 & \boldsymbol{g}_2^1 & \boldsymbol{g}_0^2 & \boldsymbol{g}_1^2 & \boldsymbol{g}_2^2 \end{array}\right] = \left[\begin{array}{ccc|ccc} 9 & 3 & 2 & 35 & 29 & 36 \\ 33 & 16 & 17 & 9 & 3 & 2 \\ 25 & 30 & 7 & 33 & 16 & 17 \\ 13 & 31 & 8 & 25 & 30 & 7 \\ 5 & 21 & 22 & 13 & 31 & 8 \\ 29 & 36 & 35 & 5 & 21 & 22 \end{array}\right].$$

Note that according to Theorem 3, the matrix $\mathfrak{G}$ is the submatrix of C formed by the 6 first rows of the columns $0, 12, 6, 1, 13, 7$.

Finally, from expression (29) we have that

$$\widehat{G}(z_1,z_2) = \left[\begin{array}{cc} \boldsymbol{g}_0^1+\boldsymbol{g}_1^1 z_1+\boldsymbol{g}_2^1 z_2 & \boldsymbol{g}_0^2+\boldsymbol{g}_1^2 z_1+\boldsymbol{g}_2^2 z_2 \end{array}\right]$$
$$= \left[\begin{array}{cc} 9+3z_1+2z_2 & 35+29z_1+36z_2 \\ 33+16z_1+17z_2 & 9+3z_1+2z_2 \\ 25+30z_1+7z_2 & 33+16z_1+17z_2 \\ 13+31z_1+8z_2 & 25+30z_1+7z_2 \\ 5+21z_1+22z_2 & 13+31z_1+8z_2 \\ 29+36z_1+35z_2 & 5+21z_1+22z_2 \end{array}\right]$$

is an encoder of an MDS 2D convolutional code of rate $2/6$ and degree 2. Note that we also can obtain matrix $\widehat{G}(z_1,z_2)$ from matrix $\mathcal{G}$ and expression (12) as

$$\widehat{G}(z_1,z_2) = \left[\begin{array}{ccc} I & Iz_1 & Iz_2 \end{array}\right]\mathcal{G}$$

with I the 6×6 identity matrix. □

Example 3: Let $k=2$ and $\delta=3$. Then $t=1$, $\ell_2=3$, and $\ell_1=6$, and therefore $\ell=6$. Since $k\ell=12$, we consider $n=12$. Furthermore, since $2n\ell+1=145$, we consider $q=149$ which is an odd prime. For $\alpha=4$ and $b=3$ we have the Cauchy circulant matrix $C=\left[c_{ij}\right]$ where

$$c_{ij} = \frac{1}{1-3\cdot 4^{j-i}}, \quad 0\leq i,j\leq 71.$$

Consider the matrices

$$\mathcal{G}_1 = \left[c_{ij}\right] \quad \text{for} \quad i=0,1,\ldots,35 \text{ and } j=0,1$$

and

$$\mathcal{G}_2 = \left[c_{ij}\right] \quad \text{for} \quad i=36,37,\ldots,71 \text{ and } j=0.$$

Thus the matrix $\mathfrak{G}$ obtained from $\mathcal{G}_1$ and $\mathcal{G}_2$ is given by

$$\mathfrak{G} = \left[\begin{array}{ccc} A_1 & B_1 & A_2 \end{array}\right]$$
$$= \left[\begin{array}{ccc|ccc|cc} \boldsymbol{g}_0^1 & \boldsymbol{g}_1^1 & \boldsymbol{g}_2^1 & \boldsymbol{g}_3^1 & \boldsymbol{g}_4^1 & \boldsymbol{g}_5^1 & \boldsymbol{g}_0^2 & \boldsymbol{g}_1^2 & \boldsymbol{g}_2^2 \end{array}\right]$$

$$= \left[\begin{array}{ccc|ccc|ccc} 74 & 146 & 16 & 23 & 8 & 110 & 27 & 80 & 108 \\ 4 & 76 & 53 & 112 & 43 & 63 & 74 & 146 & 16 \\ 70 & 123 & 87 & 107 & 38 & 97 & 4 & 76 & 53 \\ 67 & 131 & 40 & 142 & 127 & 134 & 70 & 123 & 87 \\ 140 & 111 & 122 & 61 & 77 & 42 & 67 & 131 & 40 \\ 116 & 62 & 128 & 24 & 45 & 33 & 140 & 111 & 122 \\ 50 & 132 & 35 & 85 & 32 & 49 & 116 & 62 & 128 \\ 100 & 55 & 21 & 148 & 9 & 102 & 50 & 132 & 35 \\ 34 & 48 & 141 & 2 & 129 & 95 & 100 & 55 & 21 \\ 10 & 101 & 118 & 65 & 115 & 18 & 34 & 48 & 141 \\ 83 & 117 & 105 & 126 & 22 & 88 & 10 & 101 & 108 \\ 80 & 108 & 73 & 89 & 28 & 39 & 83 & 117 & 105 \end{array}\right]$$

Finally, from expressions (10) and (11), the polynomial matrix $\widehat{G}(z_1, z_2)$ obtained from $\mathfrak{G}$, is

$$\widehat{G}(z_1, z_2) = \left[\begin{array}{cc} \boldsymbol{g}_0^1 + \boldsymbol{g}_1^1 z_1 + \boldsymbol{g}_2^1 z_2 + \boldsymbol{g}_3^1 z_1^2 + \boldsymbol{g}_4^1 z_1 z_2 + \boldsymbol{g}_5^1 z_2^2 & \boldsymbol{g}_0^2 + \boldsymbol{g}_1^2 z_1 + \boldsymbol{g}_2^2 z_2 \end{array}\right]$$

$$= \left[\begin{array}{cc} 74 + 146z_1 + 16z_2 + 23z_1^2 + 8z_1z_2 + 110z_2^2 & 27 + 80z_1 + 108z_2 \\ 4 + 76z_1 + 53z_2 + 112z_1^2 + 43z_1z_2 + 63z_2^2 & 74 + 146z_1 + 16z_2 \\ 70 + 123z_1 + 87z_2 + 107z_1^2 + 38z_1z_2 + 97z_2^2 & 4 + 76z_1 + 53z_2 \\ 67 + 131z_1 + 40z_2 + 142z_1^2 + 127z_1z_2 + 134z_2^2 & 70 + 123z_1 + 87z_2 \\ 140 + 111z_1 + 122z_2 + 61z_1^2 + 77z_1z_2 + 42z_2^2 & 67 + 131z_1 + 40z_2 \\ 116 + 62z_1 + 128z_2 + 24z_1^2 + 45z_1z_2 + 33z_2^2 & 140 + 111z_1 + 122z_2 \\ 50 + 132z_1 + 35z_2 + 85z_1^2 + 32z_1z_2 + 49z_2^2 & 116 + 62z_1 + 128z_2 \\ 100 + 55z_1 + 21z_2 + 148z_1^2 + 9z_1z_2 + 102z_2^2 & 50 + 132z_1 + 35z_2 \\ 34 + 48z_1 + 141z_2 + 2z_1^2 + 129z_1z_2 + 95z_2^2 & 100 + 55z_1 + 21z_2 \\ 10 + 101z_1 + 118z_2 + 65z_1^2 + 115z_1z_2 + 18z_2^2 & 34 + 48z_1 + 141z_2 \\ 83 + 117z_1 + 105z_2 + 126z_1^2 + 22z_1z_2 + 88z_2^2 & 10 + 101z_1 + 108z_2 \\ 80 + 108z_1 + 73z_2 + 89z_1^2 + 28z_1z_2 + 39z_2^2 & 83 + 117z_1 + 105z_2 \end{array}\right],$$

which is an encoder of an MDS 2D convolutional code of rate $2/12$ and degree 3. □

VI. Conclusions

In this paper we have introduced a natural upper bound on the distance of 2D (finite support) convolutional codes of rate k/n and degree δ and we have consequently generalized the concept of MDS 1D convolutional codes to MDS 2D convolutional codes. Moreover, we have proved that these codes exist, presenting a concrete construction of MDS 2D convolutional codes which makes use of a special class of superregular matrices. Finally, we have shown how these matrices can be constructed by means of a Cauchy circulant matrix.

REFERENCES

[1] Liam Alfandary. Two-dimensional tail-biting convolutional codes. Master's thesis, The Zandman-Slaner Graduate School of Engineering, Tel Aviv University, Tel Aviv, Israel, 2008.

[2] Liam Alfandary and Dan Raphaeli. Ball codes – two-dimensional tail-biting convolutional codes. In *Proceedings of the 2010 IEEE Global Communications Conference (GLOBECOM 2010)*, pages 1–6, Miami, FL, 2010. IEEE.

[3] Zuzana Beerliová-Trubíniová and Martin Hirt. Perfectly-secure MPC with linear communication complexity. In Ran Canetti, editor, *Theory of Cryptography*, volume 4948 of *Lecture Notes in Computer Science*, pages 213–230. Springer-Verlag, Berlin, 2008.

[4] Chalie Charoenlarpnopparut. Applications of Gröbner bases to the structural description and realization of multidimensional convolutional code. *Science Asia*, 35:95–105, 2009.

[5] Joan-Josep Climent, Diego Napp, Carmen Perea, and Raquel Pinto. A construction of MDS 2D convolutional codes of rate $1/n$ based on superregular matrices. *Linear Algebra and its Applications*, 437:766–780, 2012.

[6] Ettore Fornasini and Maria Elena Valcher. Algebraic aspects of two-dimensional convolutional codes. *IEEE Transactions on Information Theory*, 40(4):1068–1082, 1994.

[7] Heide Gluesing-Luerssen, Joachim Rosenthal, and Roxana Smarandache. Strongly MDS convolutional codes. *IEEE Transactions on Information Theory*, 52(2):584–598, 2006.

[8] Heide Gluesing-Luerssen, Joachim Rosenthal, and Paul A. Weiner. Duality between multidimensional convolutional codes and systems. In F. Colonius, U. Helmke, F. Wirth, and D. Prätzel-Wolters, editors, *Advances in Mathematical Systems Theory, A Volume in Honor of Diedrich Hinrichsen*, pages 135–150. Birkhäuser, Boston, 2001.

[9] James Hirschfeld. *Projective Geometries over Finite Field*. Oxford Mathematical Monographs. Oxford University Press, Oxford, UK, second edition, 1998.

[10] Ryan Hutchinson, Roxana Smarandache, and Jochen Trumpf. On superregular matrices and MDP convolutional codes. *Linear Algebra and its Applications*, 428:2585–2596, 2008.

[11] Pramote Jangisarakul and Chalie Charoenlarpnopparut. Algebraic decoder of multidimensional convolutional code: constructive algorithms for determining syndrome decoder and decoder matrix based on Gröbner basis. *Multidimensional Systems and Signal Processing*, 22(1–3):67–81, 2011.

[12] Rolf Johannesson and Kamil Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, NY, 1999.

[13] Pascal Junod and Serge Vaudenay. Perfect diffusion primitives for block ciphers. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography – SAC 2004*, volume 3357 of *Lecture Notes in Computer Science*, pages 84–99. Springer-Verlag, Berlin, 2005.

[14] Jørn Justesen and Søren Forchhammer. *Two-Dimensional Information Theory and Coding*. Cambridge University Press, Cambridge, UK, 2010.

[15] Gerzson Kéri. Types of superregular matrices and the number of n-arcs and complete n-arcs in $PG(r, q)$. *Journal of Combinatorial Designs*, 14(5):363–390, 2006.

[16] Gerzson Kéri. Correction to: Types of superregular matrices and the number of n-arcs and complete n-arcs in $PG(r, q)$. *Journal of Combinatorial Designs*, 16(3):262, 2008.

[17] Bruce Kitchens. Multidimensional convolutional codes. *SIAM Journal on Discrete Mathematics*, 15(3):367–381, 2002.

[18] Jérôme Lacan and Jérôme Fimes. A construction of matrices with no singular square submatrices. In Gary L. Mullen, Alain Poli, and Henning Stichtenoth, editors, *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Computer Science*, pages 145–147. Springer-Verlag, Berlin, 2003.

[19] Ruben G. Lobo, Donald L. Bitzer, and Mladen A. Vouk. Locally invertible multivariate polynomial matrices. In Øyvind Ytrehus, editor, *Coding and Cryptography*, volume 2969 of *Lecture Notes in Computer Science*, pages 427–441. Springer-Verlag, Berlin, 2006.

[20] Ruben Gerald Lobo. *On Locally Invertible Encoders and Multidimensional Convolutional Codes*. PhD thesis, Department of Computer Engineering, North Carolina State University, Raleigh, North Carolina, August 2006.

[21] Vakhtang Lomadze. The predictable degree property, column reducedness, and minimality in multidimensional convolutional coding. arXiv:cs.IT/1404.5043v1, April 2014.

[22] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 6 edition, 1988.

[23] Robert J. McEliece and Richart P. Stanley. The general theory of convolutional codes. Progress Report 42-120, California Institute of Technology, Pasadena, CA, February 1993.

[24] Diego Napp, Carmen Perea, and Raquel Pinto. Input-state-output representations and constructions of finite support 2D convolutional codes. *Advances in Mathematics of Communications*, 4(4):533–545, 2010.

[25] Joachim Rosenthal and Roxana Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Engineering, Communication and Computing*, 10:15–32, 1999.

[26] Ron M. Roth and Abraham Lempel. On MDS codes via Cauchy matrices. *IEEE Transactions on Information Theory*, 35(6):1314–1319, 1989.

[27] Ron M. Roth and Abraham Lempel. Application of circulant matrices to the construction and decoding of linear codes. *IEEE Transactions on Information Theory*, 36(5):1157–1163, 1990.

[28] Ron M. Roth and Gadiel Seroussi. On generator matrices of MDS codes. *IEEE Transactions on Information Theory*, 31(6):826–830, 1985.

[29] Jaswinder Singh and Maninder Lal Singh. A new family of two-dimensional codes for optical CDMA systems. *Optik - International Journal for Light and Electron Optics*, 120:959–962, 2009.

[30] Roxana Smarandache, Heide Gluesing-Luerssen, and Joachim Rosenthal. Construction results for mds-convolutional codes. In *Proceedings of the 2000 IEEE International Symposium on Information Theory (ISIT 2000)*, page 294, Sorrento, Italy, June 2000. IEEE.

[31] Roxana Smarandache, Heide Gluesing-Luerssen, and Joachim Rosenthal. Constructions of MDS-convolutional codes. *IEEE Transactions on Information Theory*, 47(5):2045–2049, 2001.

[32] Virtudes Tomás, Joachim Rosenthal, and Roxana Smarandache. Decoding of convolutional codes over the erasure channel. *IEEE Transactions on Information Theory*, 58(1):90–108, 2012.

[33] Paul A. Weiner. *Multidimensional Convolutional Codes*. PhD thesis, Department of Mathematics, University of Notre Dame, Indiana, USA, April 1998.

[34] Eva Zerz. On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings. *Asian Journal of Control*, 12(2):119–126, 2010.

[35] Xiu-Li Zhou and Yu Hu. Multilength two-dimensional codes for optical CDMA systems. *Optoelectronics Letters*, 1(3):232–234, 2005.