5TH PYTHAGOREAN CONFERENCE
KALAMATA, GREECE, JUNE 1-6, 2025
AN ADVANCED RESEARCH WORKSHOP IN FINITE GEOMETRY, COMBINATORIAL DESIGNS, ALGEBRAIC COMBINATORICS, CODING THEORY, CRYPTOGRAPHY & CRYPTOLOGY

Optimal Multidimensional Convolutional Codes

Zita Abreu

University of Aveiro
(zita.abreu@ua.pt)

June 5, 2025

Contents

mD Convolutional codes

- Coding theory $\Rightarrow$ **Convolutional Codes**
- Convolutional codes are especially useful for **sequential encoding** and **decoding with low delay** and hence very important for streaming applications.

mD Convolutional codes

- Coding theory $\Rightarrow$ **Convolutional Codes**
- Convolutional codes are especially useful for **sequential encoding** and **decoding with low delay** and hence very important for streaming applications.

Muiltidimensional (mD) convolutional codes generalize convolutional codes to polynomial rings in several variables.

Fornasini and Valcher introduced 2D convolutional codes in [1, 2]. In [3], the authors established an upper bound for the free distance of a 2D convolutional code and provided some optimal 2D convolutional code constructions. More 2D convolutional codes constructions are studied in [4, 5, 6].

There are notable differences between 1D and 2D convolutional codes, as well as between 2D and 3D convolutional codes [7].

mD Convolutional Codes

Let $\mathbb{F}$ be a finite field and $R = \mathbb{F}[z_1, \ldots, z_m]$ the polynomial ring in m variables with coefficients in $\mathbb{F}$.

Definition ([7])

An **mD** (finite support) **convolutional code** $\mathcal{C}$ of rate k/n is a free R-submodule of R^n of rank k.

A full row rank matrix $G(z_1, \ldots, z_m) \in R^{k \times n}$ whose rows constitute a basis for $\mathcal{C}$ is called an **encoder** of $\mathcal{C}$ and therefore

$$\begin{aligned}\mathcal{C} &= \mathrm{Im}_R\, G(z_1, \ldots, z_m) \\ &= \{v(z_1, \ldots, z_m) \in R^n : v(z_1, \ldots, z_m) = G(z_1, \ldots, z_m)u(z_1, \ldots, z_m), u(z_1, \ldots, z_m) \in R^k\}.\end{aligned}$$

Equivalent encoders

Definition ([7])

A square matrix $U(z_1, \ldots, z_m) \in R^{k \times k}$ is **unimodular** if and only if there is a matrix $V(z_1, \ldots, z_m) \in R^{k \times k}$ such that

$$U(z_1, \ldots, z_m) \cdot V(z_1, \ldots, z_m) = V(z_1, \ldots, z_m) \cdot U(z_1, \ldots, z_m) = I_k.$$

- A matrix $U(z_1, \ldots, z_m) \in R^{k \times k}$ is unimodular if and only if $det(U(z_1, \ldots, z_m))$ is a unit in R, i.e. a nonzero element of $\mathbb{F}$.

Two full row rank matrices $G_1(z_1, \ldots, z_m)$, $G_2(z_1, \ldots, z_m) \in R^{k \times n}$ are said to be **equivalent encoders** if

$$\mathrm{Im}_R\, G_1(z_1, \ldots, z_m) = \mathrm{Im}_R\, G_1(z_1, \ldots, z_m),$$

which happens if and only if

$$G_1(z_1, \ldots, z_m) = G_2(z_1, \ldots, z_m) U(z_1, \ldots, z_m)$$

for some unimodular matrix $U(z_1, \ldots, z_m) \in R^{k \times k}$.

Notation

Let $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$. By z^α we mean $z_1^{\alpha_1} \cdot \ldots \cdot z_m^{\alpha_m}$. A polynomial $f \in R$ can be written as

$$f(z_1, \ldots, z_m) = \sum_{\alpha \in \mathbb{N}^m} f_\alpha z^\alpha \text{ where } f_\alpha \in \mathbb{F}.$$

In a similar way a vector $w = \begin{bmatrix} w_1 & \cdots & w_n \end{bmatrix} \in R^n$ can be written as

$$w = \sum_{\alpha \in \mathbb{N}^m} w_\alpha z^\alpha \text{ where } w_\alpha \in \mathbb{F}^n.$$

Weight

Definition

The **weight** of $a \in \mathbb{F}^n$ is denoted by $wt(a)$ and is given by the number of nonzero entries of a. The weight of $f \in R$ is denoted by $wt(f)$ and is the number of nonzero terms of f. If $w = \begin{bmatrix} w_1 & \cdots & w_n \end{bmatrix} \in R^n$ then the weight of w is given by

$$wt(w) = \sum_{j=1}^{n} wt(w_j).$$

Equivalently, if $w = \sum_{\alpha \in \mathbb{N}^m} w_\alpha z^\alpha$ where $w_\alpha \in \mathbb{F}^n$ then

$$wt(w) = \sum_{\alpha \in \mathbb{N}^m} wt(w_\alpha).$$

Example

Let $\mathbb{F} = \mathbb{F}_2$ and $R = \mathbb{F}[z_1, z_2]$. If $w = \begin{bmatrix} 1 + z_2 & z_1 z_2 + z_2 & z_1^2 \end{bmatrix}$, then $w = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} z_2 + \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} z_1^2 + \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} z_1 z_2$. Thus $wt(w) = 5$.

Distance

Definition ([7])

Given two elements $w, \tilde{w} \in R^n$, the (Hamming) distance between w and $\tilde{w}$ is given by $dist(w, \tilde{w}) = wt(w - \tilde{w})$. The **free distance** of $\mathcal{C}$ is

$$dist(\mathcal{C}) = min\{dist(w, \tilde{w}) : w, \tilde{w} \in \mathcal{C}, w \neq \tilde{w}\}.$$

For any convolutional code $\mathcal{C}$, since $dist(w_1, w_2) = wt(w_1 - w_2)$ and $\mathcal{C}$ is linear, then

$$dist(\mathcal{C}) = min\{wt(w) : w \in \mathcal{C}, w \neq 0\}.$$

Degree

The degree of polynomial

$$f = \sum_{\alpha \in \mathbb{N}^m} f_\alpha z^\alpha \in R$$

is, as usual, defined by the formula

$$max\{\alpha_1 + \cdots + \alpha_m : f_\alpha \neq 0\}.$$

Let ν_i be the **column degree** of the i-th column of a polynomial matrix $G(z_1, \ldots, z_m)$, i.e, the maximum degree of the entries of the i-th column of $G(z_1, \ldots, z_m)$. The external degree of $G(z_1, \ldots, z_m)$ is the sum of its column degrees, i.e., $\sum_{i=1}^{k} \nu_i$.

Definition

The **degree** of $\mathcal{C}$ is defined as the minimum of the external degrees among all the encoders of $\mathcal{C}$.

mD Generalized Singleton Bound

- Upper bound on the distance of mD convolutional codes of rate k/n and degree δ.

Lemma ([8])

Let $\#S$ denote the cardinality of S. Then

$$\#\{\alpha \in \mathbb{N}_0^m : 1 \leq \alpha_1 + \cdots + \alpha_m \leq \nu\} = \frac{(\nu + m)!}{\nu! m!} - 1$$

mD Generalized Singleton Bound

- Upper bound on the distance of mD convolutional codes of rate k/n and degree δ.

Lemma ([8])

Let $\#S$ denote the cardinality of S. Then

$$\#\{\alpha \in \mathbb{N}_0^m : 1 \leq \alpha_1 + \cdots + \alpha_m \leq \nu\} = \frac{(\nu + m)!}{\nu! m!} - 1$$

Theorem

Let $\mathcal{C}$ be a mD convolutional code of rate k/n and degree δ. Then

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

Proof of the Theorem

Let $G(z_1, \ldots, z_m) \in R^{n\times k}$ be an encoder of $\mathcal{C}$ with column degrees $\nu_1, \nu_2, \ldots, \nu_k$ and external degree δ. Then $\nu_1 + \nu_2 + \cdots + \nu_k = \delta$, and let us assume that

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

i.e. ν_k is the minimum value of the column degrees of $G(z_1, \ldots, z_m)$ and $G(z_1, \ldots, z_m)$ has at least $k - t + 1$ columns degrees equal to ν_k, for $1 \leq t \leq k$.

Let us write

$$G(z_1, \ldots, z_m) = \begin{bmatrix} G^{(1)}(z_1, \ldots, z_m) & G^{(2)}(z_1, \ldots, z_m) \end{bmatrix}$$

where $G^{(1)}(z_1, \ldots, z_m) \in R^{n\times(t-1)}$ and $G^{(2)}(z_1, \ldots, z_m) \in R^{n\times(k-t+1)}$.

Since the column degrees of $G^{(2)}(z_1, \ldots, z_m)$ are all equal to ν_k we can write

$$G^{(2)}(z_1, \ldots, z_m) = \sum_{0\leq\alpha_1+\cdots+\alpha_m\leq\nu_k} G^{(2)}_{\alpha_1\cdots\alpha_m} z^{(\alpha_1,\cdots,\alpha_m)}.$$

Proof of the Theorem

Let $u = \begin{bmatrix} 0 \\ \tilde{u} \end{bmatrix}$, with $\tilde{u} \in \mathbb{F}^{k-t+1}$, be a nonzero vector such that $G^{(2)}_{0\dots0}\tilde{u}$ has $k-t$ entries equal to zero.
Then, by the Lemma we have that:

$$\begin{aligned} wt(G(z_1,\dots,z_m)u) &= wt(G^{(2)}(z_1,\dots,z_m)\tilde{u}) \\ &= wt\big(G^{(2)}_{0\dots0}\tilde{u}\big) + \sum_{1\le\alpha_1+\dots+\alpha_m\le\nu_k} wt\big(G^{(2)}_{\alpha_1\dots\alpha_m}\tilde{u}\big) \\ &\le n-(k-t)+n\Big(\frac{(\nu_k+m)!}{\nu_k!m!}-1\Big) \\ &= n\Big(\frac{(\nu_k+m)!}{\nu_k!m!}\Big)-(k-t) \end{aligned}$$

and therefore

$$dist(\mathcal{C}) \le n\frac{(\nu_k+m)!}{\nu_k!m!}-(k-t)+1.$$

The maximum value of this upper bound is achieved by maximizing ν_k and then t, i.e. when $\nu_k = \left\lfloor \frac{\delta}{k} \right\rfloor$ and $t = \delta - k\left\lfloor \frac{\delta}{k} \right\rfloor + 1$ and therefore

$$dist(\mathcal{C}) \le n\frac{(\lfloor \frac{\delta}{k} \rfloor+m)!}{\lfloor \frac{\delta}{k} \rfloor!m!}-k\Big(\Big\lfloor \frac{\delta}{k} \Big\rfloor+1\Big)+\delta+1.$$

MDS mD convolutional code

- The upper bound given is the extension to mD convolutional codes of the generalized Singleton bound for 2D convolutional codes [3] and we call it **mD generalized Singleton bound**.
- An mD convolutional code of rate k/n and degree δ with distance equal to the mD generalized Singleton bound is called a **Maximum Distance Separable (MDS) mD convolutional code**.

Construction of MDS 3D convolutional codes of rate $1/n$ and degree $\delta \leq 2$

The next definition defines superregular matrix which will be useful on the construction of these codes.

Definition

Given a square matrix $A = [a_{ij}] \in \mathbb{F}_q^{r\times r}$, define

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

where $X = \{x_{ij} \ : \ i,j \in \{1,\ldots,r\}\}$ is a set of indeterminates over $\mathbb{F}_q$, and let $\overline{A} = [\overline{a}_{ij}] \in \mathbb{F}_q[X]$. Then A has a non trivially zero determinant if the determinant of $\overline{A}$ is not the zero polynomial. A matrix is **superregular** if each of its non trivially zero minors is nonzero.

Construction of MDS 3D convolutional codes of rate $1/n$ and degree $\delta \leq 2$

The next theorem gives sufficient conditions in order for a matrix to be superregular.

Theorem ([9])

Let α be a primitive element of a finite field $\mathbb{F} = \mathbb{F}_{p^N}$ and $B = [\nu_{i\ell}]$ be a matrix over $\mathbb{F}$ with the following properties:

1. *if $\nu_{i\ell} \neq 0$ then $\nu_{i\ell} = \alpha^{\beta_{i\ell}}$ for a positive integer $\beta_{i\ell}$;*
2. *if $\nu_{i\ell} = 0$ then $\nu_{i'\ell} = 0$, for any $i' > i$ or $\nu_{i\ell'} = 0$, for any $\ell' < \ell$;*
3. *if $\ell < \ell'$, $\nu_{i\ell} \neq 0$ and $\nu_{i\ell'} \neq 0$ then $2\beta_{i\ell} \leq \beta_{i\ell'}$;*
4. *if $i < i'$, $\nu_{i\ell} \neq 0$ and $\nu_{i'\ell} \neq 0$ then $2\beta_{i\ell} \leq \beta_{i'\ell}$.*

Suppose N is greater than any exponent of α appearing as a nontrivial term of any minor of B. Then B is superregular.

The next result is trivial and will be very useful.

Lemma

Let B be a superregular matrix and $\tilde{B}$ a matrix obtained from B by permutation of columns. Then $\tilde{B}$ is also a superregular matrix.

Construction of MDS 3D convolutional codes of rate $1/n$ and degree $\delta \leq 2$

Theorem ([4])

Let α be a primitive element of a finite field with p^N elements $\mathbb{F} = \mathbb{F}_{p^N}$ for some $N \in \mathbb{N}$. Let $n, k, \delta, \tilde{\nu}$ such that $k \nmid \delta$, $\tilde{\nu} = \left\lfloor \frac{\delta}{k} \right\rfloor$ and $n > k + \delta$. Consider

$$G(z_1, z_2) = \sum_{0 \leq a+b \leq \tilde{\nu}+1} G_{ab} z_1^a z_2^b \in \mathbb{F}[z_1, z_2]^{n \times k}$$

with

$$G_{ab} = \left[g_{i,j}^{(a,b)} \right] \in \mathbb{F}^{n \times k}$$

defined by

$$g_{i,j}^{(a,b)} = \begin{cases} \alpha^{2^{(a(\tilde{\nu}+2)+b)n+i+j-2}} & \text{if } 0 \leq a+b \leq \tilde{\nu} \\ \alpha^{2^{(a(\tilde{\nu}+2)+b)n+i+j-2}} & \text{if } a+b = \tilde{\nu}+1 \text{ and } j \leq \delta - k\tilde{\nu} \\ 0 & \text{if } a+b = \tilde{\nu}+1 \text{ and } j > \delta - k\tilde{\nu} \\ 0 & \text{if } a+b > \tilde{\nu}+1. \end{cases}$$

Then, for $N \in \mathbb{N}$ sufficiently large, $\mathcal{C} = \mathrm{Im}_{\mathbb{F}[z_1,z_2]} G(z_1, z_2)$ is an MDS 2D convolutional code of rate k/n and degree δ.

Construction of MDS 3D convolutional codes of rate $1/n$ and degree $\delta \leq 2$

Theorem ([6])

Let n and δ be non-negative integers and set $\ell = \frac{(\delta+1)(\delta+2)}{2}$. Let $\mathbb{F}$ be large enough such that there exists a superregular matrix

$$\begin{bmatrix} g_0 & g_1 & \cdots & g_{\ell-1} \end{bmatrix} \in \mathbb{F}^{n\times \ell}$$

and define

$$G(z_1, z_2) = \sum_{0\leq i+j\leq \delta} G_{ij} z_1^i z_2^j \in \mathbb{F}[z_1, z_2]^n$$

where $G_{ij} = g_{\mu(i,j)}$ and $\mu : \mathbb{N}^2 \to \mathbb{N}^2$ is the map defined by

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

Then, if $n \geq \ell$, the 2D convolutional code with encoder $G(z_1, z_2)$ is an MDS 2D convolutional code of rate $1/n$ and degree δ.

Construction of MDS 3D convolutional codes of rate $1/n$ and degree $\delta \leq 2$

Let us consider $\delta = 2$ and let us construct an MDS 3D convolutional code of rate $1/n$ and degree 2. An encoder $G(z_1, z_2, z_3)$ of $\mathcal{C}$ can be written as

$$G(z_1, z_2, z_3) = \sum_{0 \leq i+j+l \leq 2} G_{ijl} z_1^i z_2^j z_3^l, \text{ with } G_{ijl} \in \mathbb{F}^{n \times 1}.$$

We can write

$$\begin{aligned} G(z_1, z_2, z_3) &= \sum_{l=0}^{2} G^{(l)}(z_1, z_2) z_3^l \\ &= G^{(0)}(z_1, z_2) + G^{(1)}(z_1, z_2) z_3 + G^{(2)}(z_1, z_2) z_3^2, \end{aligned}$$

where

$$G^{(0)}(z_1, z_2) = \sum_{0 \leq i+j \leq 2} G_{ij0} z_1^i z_2^j,$$

$$G^{(1)}(z_1, z_2) = \sum_{0 \leq i+j \leq 1} G_{ij1} z_1^i z_2^j \text{ and}$$

$$G^{(2)}(z_1, z_2) = G_{002}.$$

Construction of MDS 3D convolutional codes

Theorem

Let α be a primitive element of a finite field $\mathbb{F}_{p^N}$ with $N \in \mathbb{N}$ sufficiently large. Let $n \geq 6$ and $\hat{G}(z_1, z_2) = \sum_{0 \leq a+b \leq 2} G_{ab} z_1^a z_2^b \in \mathbb{F}[z_1, z_2]^{n \times 2}$ with $G_{ab} = \left[g_{i,j}^{(a,b)} \right] \in \mathbb{F}^{n \times 2}$ defined by

$$g_{i,j}^{(a,b)} = \begin{cases} \alpha^{2^{(3a+b)n+i+j-2}} & \text{if } 0 \leq a+b \leq 1 \\ \alpha^{2^{(3a+b)n+i+j-2}} & \text{if } a+b=2 \text{ and } j \leq 1 \\ 0 & \text{if } a+b=2 \text{ and } j > 1 \\ 0 & \text{if } a+b > 2. \end{cases}$$

and write

$$\hat{G}(z_1, z_2) = \left[G^{(0)}(z_1, z_2) \; G^{(1)}(z_1, z_2) \right].$$

Define

$$G(z_1, z_2, z_3) = G^{(0)}(z_1, z_2) + G^{(1)}(z_1, z_2) z_3 + G^{(2)}(z_1, z_2) z_3^2,$$

where $G^{(2)}(z_1, z_2) = G_{002} \in \mathbb{F}^n$ is a vector with all the entries different from zero. Then

$$\mathcal{C} = \mathrm{Im}_{\mathbb{F}[z_1, z_2, z_3]} G(z_1, z_2, z_3)$$

is a 3D MDS convolutional code of rate $1/n$ and degree 2.

Conclusion

- We considered mD convolutional codes and we established an upper bound on the distance of these codes.
- We presented concrete constructions of 3D convolutional codes of rate $1/n$ and degree δ that attain such bound for $n \geq 6$ and $\delta \leq 2$.
- As future work it could be interesting to investigate similar constructions for $2 \leq n \leq 5$.
- Further research must be done to investigate the existence of mD convolutional codes of any rate k/n and degree δ.

References

[1] M.E. Valcher and E. Fornasini. On 2D finite support convolutional codes: an algebraic approach. Multidim. Sys. and Sign. Proc., 5:231-243, 1994.

[2] E. Fornasini and M.E. Valcher. Algebraic aspects of two-dimensional convolutional codes. IEEE Trans. Inf. Theory, 40, 1068–1082, 1994.

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

[4] P. Almeida,D. Napp, and R. Pinto. MDS 2D convolutional codes with optimal 1D horizontal projections. Des. Codes Cryptogr. 86, 285–302, 2018.

[5] P. Almeida, D. Napp, R. Pinto. From 1D Convolutional Codes to 2D Convolutional Codes of Rate 1/n, in: "Coding Theory and Applications", CIM Series in Mathematical Sciences, vol 3, Springer, 2015.

[6] J.J. Climent, D. Napp, C. Perea, R. Pinto. A construction of MDS 2D convolutional codesof rate 1/n based on superregular matrices. Linear Algebra and its Applications, vol. 437(3), 766–780, 2012.

[7] P. Weiner. Muldimensional Convolutional Codes, PhD dissertation, University of Notre Dame, USA, 1998.

[8] K. H. Rosen. Discrete Mathematics and Its Applications, McGraw-Hill Higher Education, 2006.

[9] P. Almeida, D. Napp, and R. Pinto. Superregular matrices and applications to convolutional codes. Linear Algebra and its Applications, vol. 499, 1–25, 2016.

Acknowledgments

This work is supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), reference UID/04106 and by FCT grant UI/BD/151186/2021 (https://doi.org/10.54499/UI/BD/151186/2021).