

# Construction of convolutional codes over the binary field with optimal column distances

Zita Abreu

University of Aveiro and University of Zurich

Joint work with Julia Lieb and Joachim Rosenthal

## Why? Binary convolutional codes

So far optimal binary convolutional codes have **only been presented for some special values of the code rate**.

- There are two tabulations of binary convolutional codes with maximal free distance for rates  $1/2$ ,  $1/3$ ,  $1/4$ ,  $2/3$  and  $3/4$ ; <sup>1 2</sup>
- Tables of binary convolutional codes of rates  $1/2$  and  $2/3$  with optimal column distances were presented. <sup>3</sup>

---

<sup>1</sup>K. Larsen, Short convolutional codes with maximal free distance for rates  $1/2$ ,  $1/3$ , and  $1/4$ , IEEE Transactions on Information Theory, vol. 19, no. 3, pp. 371-372, May 1973.

<sup>2</sup>E. Paaske, Short binary convolutional codes with maximal free distance for rates  $2/3$  and  $3/4$ , IEEE Transactions on Information Theory, vol. 20, no. 5, pp. 683-689, September 1974.

<sup>3</sup>R. Johannesson, E. Paaske, Further Results on Binary Convolutional Codes with an Optimum Distance Profile, IEEE Trans. Inform. Theory 24(2), pp. 264-268, 1978.

## Why? Binary convolutional codes

So far optimal binary convolutional codes have **only been presented for some special values of the code rate**.

- There are two tabulations of binary convolutional codes with maximal free distance for rates  $1/2$ ,  $1/3$ ,  $1/4$ ,  $2/3$  and  $3/4$ ; <sup>1 2</sup>
- Tables of binary convolutional codes of rates  $1/2$  and  $2/3$  with optimal column distances were presented. <sup>3</sup>

A **new** construction of binary convolutional codes with optimal column distances for more general code rates will be presented and for that we focus on **maximizing especially the small column distances that are most important for low delay decoding**.

---

<sup>1</sup>K. Larsen, Short convolutional codes with maximal free distance for rates  $1/2$ ,  $1/3$ , and  $1/4$ , IEEE Transactions on Information Theory, vol. 19, no. 3, pp. 371-372, May 1973.

<sup>2</sup>E. Paaske, Short binary convolutional codes with maximal free distance for rates  $2/3$  and  $3/4$ , IEEE Transactions on Information Theory, vol. 20, no. 5, pp. 683-689, September 1974.

<sup>3</sup>R. Johannesson, E. Paaske, Further Results on Binary Convolutional Codes with an Optimum Distance Profile, IEEE Trans. Inform. Theory 24(2), pp. 264-268, 1978.

## Preliminaries

### Definition

A **simplex code**  $S(k)$  of dimension  $k$  is a block code  $C = \{u \cdot S(k), u \in \mathbb{F}_2^k\}$  whose generator matrix  $S(k) \in \mathbb{F}_2^{k \times (2^k - 1)}$  has all nonzero vectors in  $\mathbb{F}_2^k$  as columns.

Note that  $S(k)$  is only unique up to column permutations inside the generator matrix leading to an equivalent code.

### Preposition

*All nonzero codewords of a  $k$ -dimensional simplex code of length  $n = 2^k - 1$  have weight  $2^{k-1} = \frac{n+1}{2}$ .*

### Example

*The generator matrix of the simplex  $[7, 3, 4]$  -code is thus:*

$$S(3) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

## Definition

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

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

## Definition

Let

$$G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}_q[z]^{k \times n}$$

with  $G_\mu \neq 0$  and  $k \leq n$ .

For each  $i$ ,  $1 \leq i \leq k$ , the  $i$ -th **row degree**  $\nu_i$  of  $G(z)$  is defined as the largest degree of any entry in row  $i$  of  $G(z)$ , in particular  $\mu = \max_{i=1, \dots, k} \nu_i$ .

The **external degree** of  $G(z)$  is the sum of the row degrees of  $G(z)$ . The **internal degree** of  $G(z)$  is the maximal degree of the  $k \times k$  minors of  $G(z)$ .

## Definition

A matrix  $G(z) \in \mathbb{F}_q[z]^{k \times n}$  is said to be **row reduced** if its internal and external degrees are equal. In this case,  $G(z)$  is called a **minimal generator matrix** of the convolutional code.

The **degree**  $\delta$  of a code  $\mathcal{C}$  is the external degree of a minimal generator matrix of  $\mathcal{C}$ . A convolutional code with rate  $k/n$  and degree  $\delta$  is called an  $(n, k, \delta)$  convolutional code.

## Definition

$G(z) \in \mathbb{F}_q[z]^{k \times n}$  is said to have **generic row degrees** if

- $\nu_1 = \dots = \nu_t = \lceil \frac{\delta}{k} \rceil$  and
- $\nu_t = \dots = \nu_k = \lfloor \frac{\delta}{k} \rfloor$

for  $t = \delta + k - k \lceil \frac{\delta}{k} \rceil$ .

## Definition

A generator matrix  $G(z) \in \mathbb{F}_q[z]^{k \times n}$  with  $G_0 = G(0)$  full (row) rank is called **delay-free**.

## Definition

The (Hamming) weight of a polynomial vector

$$v(z) = \sum_{t=0}^{\deg(v(z))} v_t z^t \in \mathbb{F}_q[z]^n$$

is defined as

$$wt(v(z)) = \sum_{t=0}^{\deg(v(z))} wt(v_t),$$

where  $wt(v_t)$  is the weight of  $v_t \in \mathbb{F}_q^n$ .

## Definition

The **free distance** of a convolutional code  $\mathcal{C}$  is given by

$$d_{free}(\mathcal{C}) := \min_{v(z) \in \mathcal{C}} \{wt(v(z)) \mid v(z) \neq 0\}.$$

## Definition

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

$$d_j^{\mathcal{C}} := \min \{ wt(v_0, \dots, v_j) \mid v(z) \in \mathcal{C} \text{ and } v_0 \neq 0 \}.$$

## Definition

Let  $G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}_q[z]^{k \times n}$  be a generator matrix of a convolutional code  $\mathcal{C}$ . For  $j \in \mathbb{N}_0$ , define the **truncated sliding generator matrices** as

$$G_j^{\mathcal{C}} := \begin{bmatrix} G_0 & \dots & G_j \\ & \ddots & \vdots \\ & & G_0 \end{bmatrix} \in \mathbb{F}_q^{(j+1)k \times (j+1)n}$$

where we set  $G_i = 0$  for  $i > \mu$ .



## Definition

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

$$d_j^{\mathcal{C}}(\mathcal{C}) := \min \{ wt(v_0, \dots, v_j) \mid v(z) \in \mathcal{C} \text{ and } v_0 \neq 0 \}.$$

## Definition

Let  $G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}_q[z]^{k \times n}$  be a generator matrix of a convolutional code  $\mathcal{C}$ . For  $j \in \mathbb{N}_0$ , define the **truncated sliding generator matrices** as

$$G_j^{\mathcal{C}} := \begin{bmatrix} G_0 & \dots & G_j \\ & \ddots & \vdots \\ & & G_0 \end{bmatrix} \in \mathbb{F}_q^{(j+1)k \times (j+1)n}$$

where we set  $G_i = 0$  for  $i > \mu$ .

Since the convolutional codes which we will construct will all be delay-free, we can use that in this case

$$d_j^{\mathcal{C}}(\mathcal{C}) = \min \{ wt(u_0, \dots, u_j) G_j^{\mathcal{C}} \mid u(z)G(z) \in \mathcal{C} \text{ and } u_0 \neq 0 \}$$

## Definition

A full row rank matrix  $H(z) \in \mathbb{F}_q[z]^{(n-k) \times n}$  satisfying

$$\mathcal{C} = \ker H(z) = \{v(z) \in \mathbb{F}_q[z]^n : H(z)v(z)^T = 0\}$$

is called a **parity-check matrix** of  $\mathcal{C}$ . If such a matrix exists,  $\mathcal{C}$  is called **non-catastrophic**, otherwise it is called **catastrophic**.

A code is non-catastrophic if and only if  $G(z)$  is left prime which is equivalent to  $G(z)$  having full row rank for all elements from the closure  $z \in \overline{\mathbb{F}_q}$ .

**Each non-catastrophic convolutional code is delay-free.** Moreover, if  $\mathcal{C}$  is non-catastrophic,  $d_{free}(\mathcal{C}) = \lim_{j \rightarrow \infty} d_j^{\mathcal{C}}(\mathcal{C})$ .

**Theorem ([1],[8])**

Let  $\mathcal{C}$  be an  $(n, k, \delta)$  convolutional code. Then,

- (i)  $d_{\text{free}}(\mathcal{C}) \leq (n - k) \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) + \delta + 1$
- (ii)  $d_j^{\mathcal{C}}(\mathcal{C}) \leq (n - k)(j + 1) + 1$  for all  $j \in \mathbb{N}_0$

The bound in (i) is called **generalized Singleton bound**.

The fact that  $d_j^{\mathcal{C}}(\mathcal{C}) \leq d_{\text{free}}(\mathcal{C})$  for all  $j \in \mathbb{N}_0$  implies

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

for all  $j \in \mathbb{N}_0$ . Hence  $j = L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$  is the largest possible value of  $j$  for which  $d_j^{\mathcal{C}}(\mathcal{C})$  can attain the upper bound in (ii).

### Theorem ([1],[8])

Let  $\mathcal{C}$  be an  $(n, k, \delta)$  convolutional code. Then,

- (i)  $d_{\text{free}}(\mathcal{C}) \leq (n - k) \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) + \delta + 1$
- (ii)  $d_j^{\mathcal{C}}(\mathcal{C}) \leq (n - k)(j + 1) + 1$  for all  $j \in \mathbb{N}_0$

The bound in (i) is called **generalized Singleton bound**.

The fact that  $d_j^{\mathcal{C}}(\mathcal{C}) \leq d_{\text{free}}(\mathcal{C})$  for all  $j \in \mathbb{N}_0$  implies

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

for all  $j \in \mathbb{N}_0$ . Hence  $j = L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$  is the largest possible value of  $j$  for which  $d_j^{\mathcal{C}}(\mathcal{C})$  can attain the upper bound in (ii).

### Lemma ([1])

Let  $\mathcal{C}$  be an  $(n, k, \delta)$  convolutional code. If  $d_j^{\mathcal{C}}(\mathcal{C}) = (n - k)(j + 1) + 1$  for some  $j \in \{1, \dots, L\}$ , then  $d_i^{\mathcal{C}}(\mathcal{C}) = (n - k)(i + 1) + 1$  for all  $i \leq j$ .

**Definition ([1])**

An  $(n, k, \delta)$  convolutional code  $\mathcal{C}$  is said to be **maximum distance profile (MDP)** if

$$d_j^{\mathcal{C}}(\mathcal{C}) = (n - k)(j + 1) + 1 \text{ for } j = L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n - k} \right\rfloor.$$

## Definition ([1])

An  $(n, k, \delta)$  convolutional code  $\mathcal{C}$  is said to be **maximum distance profile (MDP)** if

$$d_j^{\mathcal{C}}(\mathcal{C}) = (n - k)(j + 1) + 1 \text{ for } j = L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n - k} \right\rfloor.$$

It is known that for the existence of MDP codes the size of the underlying finite field has to be sufficiently large (see e.g. [2, 5]), i.e. **we cannot construct MDP codes over the binary field.**

# Upper and lower bounds for column distances

## Lemma

Let  $C$  be an  $(n, k, \delta)$  convolutional code with generator matrix  $G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}_q[z]^{k \times n}$  with  $G_{\mu} \neq 0$ . Denote by  $wt_r(G_i)$  the weight of row  $r$  of  $G_i$ . Then,

$$\sum_{i=0}^j \min_{u_0 \neq 0} wt \left( (u_0 \cdots u_j) \begin{pmatrix} G_j \\ \vdots \\ G_0 \end{pmatrix} \right) \leq d_j^c(C) \leq \min_{r \in \{1, \dots, k\}} \sum_{i=0}^{\min(j, \delta)} wt_r(G_i) \quad (1)$$

$$\text{and} \quad \min_{r \in \{1, \dots, k\}} \sum_{i=0}^{\min(j, \delta)} wt_r(G_i) \leq n((\min(j, \delta) + 1)). \quad (2)$$

## Upper and lower bounds for column distances

### Lemma

Let  $\mathcal{C}$  be an  $(n, k, \delta)$  convolutional code with generator matrix  $G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}_q[z]^{k \times n}$  with  $G_\mu \neq 0$ . Denote by  $wt_r(G_i)$  the weight of row  $r$  of  $G_i$ . Then,

$$\sum_{i=0}^j \min_{u_0 \neq 0} wt \left( (u_0 \cdots u_i) \begin{pmatrix} G_i \\ \vdots \\ G_0 \end{pmatrix} \right) \leq d_j^{\mathcal{C}}(\mathcal{C}) \leq \min_{r \in \{1, \dots, k\}} \sum_{i=0}^{\min(j, \delta)} wt_r(G_i) \quad (1)$$

$$\text{and} \quad \min_{r \in \{1, \dots, k\}} \sum_{i=0}^{\min(j, \delta)} wt_r(G_i) \leq n((\min(j, \delta) + 1)). \quad (2)$$

**Proof:** The (2) is obvious. For (1) recall that by definition

$$d_j^{\mathcal{C}}(\mathcal{C}) = \min_{u_0 \neq 0} \sum_{i=0}^j wt \left( (u_0 \cdots u_i) \begin{pmatrix} G_i \\ \vdots \\ G_0 \end{pmatrix} \right).$$

From this the lower bound on  $d_j^{\mathcal{C}}(\mathcal{C})$  is clear. The upper bound follows as  $d_j^{\mathcal{C}}(\mathcal{C})$  is upper bounded by the weight of any of the first  $k$  rows of  $G_j^{\mathcal{C}}$ .



## Definition

We say that a binary  $(n, k, \delta)$  convolutional code  $\mathcal{C}$  has **optimal column distances** if there exists no binary  $(n, k, \delta)$  convolutional code  $\hat{\mathcal{C}}$  such that

$$d_j^{\mathcal{C}}(\hat{\mathcal{C}}) > d_j^{\mathcal{C}}(\mathcal{C})$$

for some  $j \in \mathbb{N}_0$  and

$$d_i^{\mathcal{C}}(\hat{\mathcal{C}}) = d_i^{\mathcal{C}}(\mathcal{C})$$

for all  $0 \leq i < j$ .

## Construction of rate $1/n$

- Maximize  $d_0^c$ , i.e. we have to choose  $G_0 = (1 \dots 1)$ .
- Start with the generator matrix of a simplex code but only take the columns whose first entry is equal to 1 and set the resulting matrix equal to  $\begin{pmatrix} G_0 \\ \vdots \\ G_\delta \end{pmatrix}$ .

### Example

For  $n = 3$ , the corresponding simplex code has generator matrix  $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$  and we obtain from this the  $(2, 1, 1)$  convolutional code  $\mathcal{C}$  with  $G_0 = (1 \ 1)$  and  $G_1 = (1 \ 0)$ .

One has  $d_0^c(\mathcal{C}) = 2$ ,  $d_1^c(\mathcal{C}) = d_2^c(\mathcal{C}) = \dots = d_{free}(\mathcal{C}) = 3$ .

Moreover, the lower and upper bound of (1) are sharp for all  $j$  and (2) shows us that this is an optimal binary code for these parameters.

## Definition

Take a generator matrix  $S(\delta + 1)$  of a simplex code and remove the columns with first entry equal to zero and define the resulting matrix as  $S(\delta + 1)_1 \in \mathbb{F}_2^{(\delta+1) \times 2^\delta}$ .

For  $m \in \mathbb{N}$ , we call the (block) code with generator matrix

$$S(\delta + 1)_1^m := [S(\delta + 1)_1 \cdots S(\delta + 1)_1] \in \mathbb{F}_2^{(\delta+1) \times m \cdot 2^\delta},$$

an  $m$ -fold **partial simplex code**  $S(\delta + 1)_1^m$  of dimension  $\delta + 1$ .

## Proposition

All codewords of  $\mathcal{S}(\delta + 1)_1^m$  except  $(1 \dots 1) \in \mathbb{F}_2^{m \cdot 2^\delta}$  have weight  $m \cdot 2^{\delta-1}$ . In particular, the minimum distance of such a code is equal to  $m \cdot 2^{\delta-1}$ .

## Proof.

It is enough to show the statement for  $m = 1$ .

Take a generator matrix  $S(\delta + 1)$  of a simplex code such that the first  $2^\delta$  columns have a 1 in the first row, i.e. write

$$S(\delta + 1) = \begin{pmatrix} S(\delta + 1)_1 & 0_{1 \times (2^\delta - 1)} \\ & S(\delta) \end{pmatrix}.$$

Since all codewords of  $S(\delta + 1)$  have weight  $2^\delta$  and all codewords in  $S(\delta)$  have weight  $2^{\delta-1}$ , all codewords of  $S(\delta + 1)_1$  except the first row of  $S(\delta + 1)_1$  have weight

$$2^\delta - 2^{\delta-1} = 2^{\delta-1}.$$



## Theorem

Let  $n = m \cdot 2^\delta$  and  $\mathcal{C}$  be the  $(n, 1, \delta)$  convolutional code with generator matrix

$$G(z) = \sum_{i=0}^{\delta} G_i \in \mathbb{F}_2[z]^{1 \times m \cdot 2^\delta} \text{ where } \begin{pmatrix} G_0 \\ \vdots \\ G_\delta \end{pmatrix} = S(\delta + 1)_1^m.$$

Then,  $\mathcal{C}$  is non-catastrophic and

$$d_j^{\mathcal{C}}(\mathcal{C}) = \begin{cases} n + j \frac{n}{2} & \text{for } j \leq \delta \\ n + \delta \frac{n}{2} & \text{for } j \geq \delta \end{cases} \text{ and } d_{\text{free}}(\mathcal{C}) = n + \delta \frac{n}{2}.$$

## Theorem

Let  $n = m \cdot 2^\delta$  and  $\mathcal{C}$  be the  $(n, 1, \delta)$  convolutional code with generator matrix

$$G(z) = \sum_{i=0}^{\delta} G_i \in \mathbb{F}_2[z]^{1 \times m \cdot 2^\delta} \text{ where } \begin{pmatrix} G_0 \\ \vdots \\ G_\delta \end{pmatrix} = S(\delta + 1)_1^m.$$

Then,  $\mathcal{C}$  is non-catastrophic and

$$d_j^{\mathcal{C}}(\mathcal{C}) = \begin{cases} n + j\frac{n}{2} & \text{for } j \leq \delta \\ n + \delta\frac{n}{2} & \text{for } j \geq \delta \end{cases} \text{ and } d_{\text{free}}(\mathcal{C}) = n + \delta\frac{n}{2}.$$

## Theorem

Let  $\mathcal{C}$  be a binary  $(m \cdot 2^\delta, 1, \delta)$  convolutional code constructed as in the previous theorem. Then,  $\mathcal{C}$  has optimal column distances in the sense of Definition 16.

If  $n$  is not of the form  $m \cdot 2^\delta$  for some  $m \in \mathbb{N}$ :

For this, we use that if we keep the length  $n$  and increase the degree from  $\delta$  to  $\delta + 1$ , the coefficient matrices of the generator matrix of the optimal code of degree  $\delta + 1$  have to coincide until  $G_\delta$  with some optimal code of degree  $\delta$ .

Similarly, if we keep the degree  $\delta$  and increase the length from  $n$  to  $n + 1$ , the generator matrix for an optimal code of length  $n + 1$  has to coincide in its first  $n$  entries with an optimal code of length  $n$ .

Hence, we can use  $S(\delta + 1)_1^m$  with  $m = \left\lfloor \frac{n}{2^\delta} \right\rfloor$  for the construction and add  $n - \left\lfloor \frac{n}{2^\delta} \right\rfloor \cdot 2^\delta$  further columns of  $S(\delta + 1)_1$ .

## For $\delta = 1$ :

- If  $n$  is even, we obtain optimal column distances from  $S(2)_1^{\frac{n}{2}}$ .
  - If  $n$  is odd, to construct  $\begin{pmatrix} G_0 \\ \vdots \\ G_\delta \end{pmatrix}$  we can use  $S(2)_1^{\lfloor \frac{n}{2} \rfloor}$  and add another column from the matrix  $S(2)_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ .
- We obtain that  $d_0^c(C) = n$  and  $d_{free}(C) = d_j^c(C) = n + \lfloor \frac{n}{2} \rfloor$  for  $j \in \mathbb{N}$ , which is optimal.



## For $\delta = 2$ :

We can use  $S(3)_1^{\frac{n}{4}}$  in case  $n \equiv 0 \pmod{4}$ . If  $n \not\equiv 0 \pmod{4}$ , to obtain  $(n, 1, \delta)$  convolutional codes  $\mathcal{C}$  with optimal distances, we just need to find optimal  $(s, 1, \delta)$  convolutional codes  $\mathcal{C}_{\text{mod } 4}$  with  $s \in \{1, 2, 3\}$  such that  $n \equiv s \pmod{4}$  to use it to extend  $S(3)_1^{\lfloor \frac{n}{4} \rfloor}$ .

- For  $s = 1$ , i.e.  $n - 1 \equiv 0 \pmod{4}$ , no matter which column of  $S(3)_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$

we choose to construct  $\begin{pmatrix} G_0 \\ G_1 \\ G_2 \end{pmatrix}$ , we obtain that  $d_j^c(\mathcal{C}_{\text{mod } 4}) = 1$  for all  $j \in \mathbb{N}_0$ , i.e.

$$d_j^c(\mathcal{C}) = n + \left(\frac{n-1}{2}\right)j$$

for  $j \leq \delta = 2$  and

$$d_{\text{free}}(\mathcal{C}) = d_j^c(\mathcal{C}) = n + \left(\frac{n-1}{2}\right)\delta = 2n - 1$$

for  $j \geq \delta = 2$ .

- For  $s = 2$ , we know from the case  $\delta = 1$ , which gives us  $\begin{pmatrix} G_0 \\ G_1 \end{pmatrix}$ , that to have optimal

$d_0^C$  and  $d_1^C$ , we need to choose two columns of  $S(3)_1$  of the form  $\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ x & y \end{pmatrix}$  with

$x, y \in \mathbb{F}_2$ .

One obtains in any case  $d_0^C = 2$ ,  $d_1^C = 3$ ,  $d_2^C = 3$ . For  $(x, y) \in \{(0, 0), (0, 1)\}$ ,  $d_i^C = 3$  for  $i \geq 3$ , for  $(x, y) = (1, 0)$ ,  $d_i^C = 4$  for  $i \geq 3$ , for  $(x, y) = (1, 1)$ ,  $d_3^C = d_4^C = 4$  and  $d_i^C = 5$  for  $i \geq 5$ .

This means  $(x, y) = (1, 1)$  yields the unique optimal choice leading to  $d_0^C(C) = n$ ,  $d_1^C(C) = n + \frac{n}{2}$ ,  $d_2^C(C) = 2n - 1$ ,  $d_3^C(C) = d_4^C(C) = 2n$ ,  $d_{free}(C) = d_i^C(C) = 2n + 1$  for  $i \geq 5$ .

- For  $s = 3$ , using the previous results, we have the two options  $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$  and

$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$  for choosing three columns of  $S(3)_1$ . For  $i \leq 3$ , both lead to the same

column distances  $d_i^C = i + 3$ . But, for  $i \geq 4$ , the first option has  $d_i^C = 7$ , while the second option has  $d_i^C = 6$ . So, the first choice is optimal, leading to  $d_0^C(C) = n$ ,  $d_1^C(C) = n + \frac{n-1}{2}$ ,  $d_2^C(C) = 2n - 1$ ,  $d_3^C(C) = 2n$ ,  $d_{free}(C) = d_i^C(C) = 2n + 1$  for  $i \geq 4$ .

For  $\delta = 3$ :

We need to find optimal  $(s, 1, 3)$  convolutional codes  $C_s$  for  $s = 1, \dots, 7$ .

From the case  $\delta = 2$  we deduce that  $\begin{pmatrix} G_0 \\ G_1 \\ G_2 \end{pmatrix}$  has to be equal to the first  $s$  columns of the matrix  $S(3)_1^2$ .

$wt^s$  - the minimal weight of the code generated by the first  $s$  columns of  $\begin{pmatrix} S(3)_1^2 \\ \tilde{G}_3 \end{pmatrix}$ .

We obtained with the help of the computer that in order to optimize  $wt^s$ ,  $\tilde{G}_3$  has to be equal to one of the following vectors:

$(0\ 0\ 0\ 1\ 1\ 1\ 1\ 0)$ ,  $(0\ 0\ 1\ 0\ 1\ 1\ 0\ 1)$ ,  $(0\ 1\ 0\ 0\ 1\ 0\ 1\ 1)$ ,  $(0\ 1\ 1\ 1\ 1\ 0\ 0\ 0)$ ,  
 $(1\ 0\ 0\ 0\ 0\ 1\ 1\ 1)$ ,  $(1\ 0\ 1\ 1\ 0\ 1\ 0\ 0)$ ,  $(1\ 1\ 0\ 1\ 0\ 0\ 1\ 0)$ ,  $(1\ 1\ 1\ 0\ 0\ 0\ 0\ 1)$ .

For all these 8 optimal  $\tilde{G}_3$ , we obtain the following values for  $wt^s$ :

$$\left\| \begin{array}{c|c|c|c|c|c|c|c} s & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline wt^s & 0 & 0 & 0 & 1 & 1 & 2 & 3 \end{array} \right\|$$

and we have that  $d_3^c(C_s) \geq d_2^c(C_s) + wt_s$ .

For  $\delta = 4$ :

We can take any of these  $\tilde{G}_3$  to form the matrix  $S(4)_1 = \begin{pmatrix} S(3)_1^2 & S(3)_1^2 \\ \tilde{G}_3 & \tilde{G}_3 \end{pmatrix}$ .

$wt^t$  - minimal weight of the code generated by the first  $t \in \{1, \dots, 15\}$  columns of  $\begin{pmatrix} S(4)_1 \\ \tilde{G}_4 \end{pmatrix}$ .

We found that for each optimal choice  $\tilde{G}_3 = (\tilde{G}_3^1 \ \tilde{G}_3^2)$  with  $\tilde{G}_3^1, \tilde{G}_3^2 \in \mathbb{F}_2^4$ , there are the same eight optimal choices for  $\tilde{G}_4$ , namely exactly all vectors of the form  $(\tilde{G}_3^1 \ \tilde{G}_3^1 \ \tilde{G}_3^2 \ \tilde{G}_3^2)$ .

In this way, we obtain 64 optimal codes leading to the following optimal values for  $wt^t$ :

$t$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$wt^t$	0	0	0	0	1	1	1	2	2	3	4	4	5	6	7

# If $2^\delta \nmid n$ :

## Theorem

Set  $m = \lfloor \frac{n}{2^\delta} \rfloor$ ,  $n_1 := m \cdot 2^\delta$  and write  $n - n_1 = 2^{a_1-1} + \dots + 2^{a_b-1}$  with  $b, a_i \in \mathbb{N}$  for  $i = 1, \dots, b$  and  $\delta \geq a_1 > \dots > a_b$ .

Set  $\begin{pmatrix} G_0 \\ \vdots \\ G_\delta \end{pmatrix} = [S(\delta+1)_1^m \ S]$  where  $S$  consists of  $n - n_1$  columns of  $S(\delta+1)_1$  and has

the form  $S = D_0 = \begin{pmatrix} S(a_1)_1 & D_1 \\ * & * \end{pmatrix}$ ,  $D_1 = \begin{pmatrix} S(a_2)_1 & D_2 \\ * & * \end{pmatrix}$ , ...,  $D_i = \begin{pmatrix} S(a_{i+1})_1 & D_{i+1} \\ * & * \end{pmatrix}$ ,  
 ...,  $D_{b-1} = S(a_b)_1$ .

Then, the  $(n, 1, \delta)$  binary convolutional code  $C$  with generator matrix  $G(z)$  has column distances which are **near optimal** in the following sense:

For  $j \leq a_b - 1$ ,  $d_j^c(C) = n + j \frac{n}{2}$ , i.e. optimal, and for  $a_{x+1} < j+1 \leq a_x$  with  $x \in \{1, \dots, b-1\}$ ,

$$d_j^c(C) \geq \frac{n_1}{2} + 2^{a_1-2} + \dots + 2^{a_x-2} + d_{j-1}^c(C)$$

## Example

Take  $\delta = 4$  and  $n = 14$ . First, note that  $2^4 = 16 \nmid 14$ . In this example,  $m = \left\lfloor \frac{n}{2^\delta} \right\rfloor = 0$  and consecutively  $n_1 = 0$ . So

$$n_1 - n = n = 14 = 2^3 + 2^2 + 2^1.$$

Then  $a_1 = 3 + 1 = 4$ ,  $a_2 = 2 + 1 = 3$  and  $a_3 = 0 + 1 = 1$ .

$$\begin{pmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \\ G_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \end{pmatrix}$$

$S(4)_1$  with 4 rows and  $2^3$  columns

$S(3)_1$  with 3 rows and  $2^2$  columns

$S(2)_1$  with 2 rows and  $2^1$  columns

**The first two rows are optimal and the code is near optimal!**

## Construction with $k > 1$

### Definition

Take a generator matrix  $S(\delta + k)$  of a simplex code and remove the columns whose first  $k$  entries are equal to zero and define the resulting matrix as

$$S(k + \delta)_k \in \mathbb{F}_2^{(\delta+k) \times (2^{\delta+k} - 2^\delta)}.$$

For  $m \in \mathbb{N}$ , we call the (block) code with generator matrix

$$S(\delta + k)_k^m := [S(\delta + k)_k \cdots S(\delta + k)_k] \in \mathbb{F}_2^{(\delta+k) \times m \cdot (2^{\delta+k} - 2^\delta)}$$

an  $m$ -fold  $k$ -partial simplex code  $S(\delta + k)_k^m$  of dimension  $\delta + k$ .

### Proposition

*All codewords of  $S(\delta + k)_k^m$  that are linear combinations of just the first  $k$  rows of  $S(\delta + k)_k^m$  have weight  $m \cdot 2^{\delta+k-1}$  and all other codewords have weight  $m \cdot (2^{\delta+k-1} - 2^{\delta-1})$ . In particular, the minimum distance of such a code is equal to  $m \cdot (2^{\delta+k-1} - 2^{\delta-1}) = m \cdot 2^{\delta-1} (2^k - 1)$ .*

## Theorem

Let  $C$  be an  $(m \cdot 2^\delta (2^k - 1), k, \delta)$  convolutional code with generator matrix

$G(z) = \sum_{i=0}^{\lfloor \frac{\delta}{k} \rfloor} G_i z^i \in \mathbb{F}_2[z]^{k \times m \cdot 2^\delta (2^k - 1)}$  where  $\begin{pmatrix} G_0 \\ \vdots \\ G_{\lfloor \frac{\delta}{k} \rfloor - 1} \\ G_{\lfloor \frac{\delta}{k} \rfloor} \end{pmatrix} = S(\delta + k)_k^m$ . Then,  $C$  is

non-catastrophic and

$$d_j^C(C) = \begin{cases} n \cdot \frac{2^k - 1}{2^{k-1}} + j \frac{n}{2} & \text{for } j \leq \lfloor \frac{\delta}{k} \rfloor \\ n \cdot \frac{2^k - 1}{2^{k-1}} + \lfloor \frac{\delta}{k} \rfloor \cdot \frac{n}{2} & \text{for } j \geq \lfloor \frac{\delta}{k} \rfloor \end{cases}$$

## Theorem

Let  $C$  be a binary  $(m \cdot 2^\delta (2^k - 1), k, \delta)$  convolutional code constructed as in the previous theorem. Then,  $C$  has optimal column distances in the sense of Definition 16.



## Example

Take  $k = 2$ ,  $n = 12$  and  $\delta = 2$ . Then  $\mu = 1$ ,  $m = 1$  and  $\delta + k = 4$ .

The optimal  $G_0$ , leading to  $d_0^c = 8$  is

$$G_0 = S(2)^4 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

To maximize  $d_1^c$  we take

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

such that  $\begin{pmatrix} G_0 \\ G_1 \end{pmatrix} = S(4)_2$  and  $d_1^c = 14$ .

## Conclusion

- *Convolutional codes with optimal or near optimal column distances are attractive as they are capable of correcting a maximal number of errors per time interval.*
- *We start with simplex codes and using both the technique of puncturing and folding we are able to construct new binary convolutional codes whose column distances are optimal for certain parameters and near optimal for the other parameters.*
- **Zita Abreu, Julia Lieb, Joachim Rosenthal. Binary convolutional codes with optimal column distances, submitted, <http://arxiv.org/abs/2305.04693>.**

## Future Work

*Development of a decoding algorithm for these binary convolutional codes*

## Acknowledgments

This work is supported by the SNSF grant n. 188430 and by CIDMA through Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), UIDB/04106/2020 and UIDP/04106/2020.

The work of Zita Abreu was also supported by FCT grant UI/BD/151186/2021 and the work of Julia Lieb was also by Forschungskredit of the University of Zurich, grant no. FK-21-127.











CIÊNCIA, TECNOLOGIA  
E ENSINO SUPERIOR



UNIÃO EUROPEIA  
Fundo Social Europeu

## References

-  H. Gluesing-Luerssen, J. Rosenthal, R. Smarandache, Strongly MDS convolutional codes, *IEEE Trans. Inform. Theory* 52(2), pp. 584–598, 2006.
-  R. Hutchinson, R. Smarandach, J. Trunpf, On superregular matrices and MDP convolutional codes, *Linear Algebra and its Applications*, vol. 428, pp. 2585-2596, 2008.
-  R. Johannesson, E. Paaske, Further Results on Binary Convolutional Codes with an Optimum Distance Profile, *IEEE Trans. Inform. Theory* 24(2), pp. 264–268, 1978.
-  K. Larsen, Short convolutional codes with maximal free distance for rates  $1/2$ ,  $1/3$ , and  $1/4$ , *IEEE Transactions on Information Theory*, vol. 19, no. 3, pp. 371-372, May 1973.
-  J. Lieb, Necessary field size and probability for MDP and complete MDP convolutional codes, *Des. Codes Cryptogr.* 87, pp. 3019–3043, 2019.
-  S. Lin, D. Costello, *Error Control Coding: Fundamentals and Applications*, Prentice Hall Professional Technical Reference, 1994.
-  E. Paaske, Short binary convolutional codes with maximal free distance for rates  $2/3$  and  $3/4$ , *IEEE Transactions on Information Theory*, vol. 20, no. 5, pp. 683-689, September 1974.
-  J. Rosenthal, R. Smarandache, Maximum distance separable convolutional codes, *Appl. Algebra Engrg. Comm. Comput.* 10(1), 15–32, 1999.