Optimum MDS convolutional codes over GF(2^m) and their relation to the trace function

Ángela Barbero and Øyvind Ytrehus

UVa, Simula@UiB, UiB

Problem setting

- Unicast transmission over the Internet
  - (Memoryless) packet erasure channel, capacity "$1-\varepsilon$"
- Solutions in the Internet:
  - TCP uses ARQ
    - Problem: Long round trip time (RTT) ≈ 100’s ms
      - **The recovery delay of any ARQ system large**
      - Rate loss due to inexact RTT estimation
  - **Delay of recovery**
    - If *no* delay constraints: ARQ sufficient in many cases
    - Applications *with* delay constraints: : Multimedia, IoT control applications, stock market applications, games
  - Better: Erasure correcting codes

Coding criteria

- Code rate close to channel capacity???
- (Low) probability of recovery failure
  - Either decoding failure:
    erasure pattern covers a codeword
  - Or recovery delay exceeding tolerance of application
- Recovery complexity: Systematic codes?

Coding candidates

- MDS, Reed-Solomon: Long delay
- «Rateless» , fountain codes: Long delay

Unsuited for delay sensitive app's

- Convolutional codes: «good» **column distance profile**
  - Binary?
  - q-ary
  - Flexible rate

«Block codes are for boys, convolutional codes are for men» – J. Massey

Convolutional codes for dummies

Block code:

$$c = uG = \begin{pmatrix} u_1 & \cdots & u_k \end{pmatrix} \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}$$

Minimum distance = $\min\{w(c): c \neq 0\}$

Convolutional code:

$$c = uG = \begin{pmatrix} u^{(0)} & u^{(1)} & \ldots \end{pmatrix} \begin{pmatrix} G_0 & G_1 & \cdots & G_L & \\ & G_0 & \ddots & \vdots & \cdots \\ & & & G_0 & \end{pmatrix}$$

$$c^{(0)} = u^{(0)} G_0,\ c^{(1)} = u^{(0)} G_1 + u^{(1)} G_0, \ldots$$

CDP= $\min\left\{w\left(c^{(0)}\right), w\left(c^{(0)} c^{(1)}\right), \cdots : c^{(0)} \neq 0\right\}$

Convolutional codes and erasure recovery for dummies

If CDP is $(2,3,4,\ldots,\mathscr{D})$ then

an erasure pattern

- of weight j and
- *starting* at block/time 1

will be recovered at time j iff $j < \mathscr{D}$

Convolutional code approach

- q-ary convolutional codes with optimum column distance profile
  - **MDS**-convolutional codes
    - cdp = $(n-k+1, 2(n-k)+1, \dots, \mathscr{D})$,
  - Existence of MDS code equivalent to existence of **superregular** matrices
  - Existing constructions require large field

Our convolutional code approach

- Systematic
- Over GF(2^m)
- High rate $\frac{n-1}{n}$
- MDS (CDP=(2,3,4, … , $\mathscr{D}$, $\mathscr{D}$, $\mathscr{D}$, …))

Parity-check matrix of a convolutional code

Let $m \geq 1, n \geq 2, k = n-1$ be integers, $\mathbb{F} = GF(2^m)$, and define the matrices and vectors

$$R_0 = (r_{0,1}, \ldots, r_{0,k}) \in \mathbb{F}^k \qquad H_0 = (R_0|1) \in \mathbb{F}^n,$$

$$R_i = (r_{i,1}, \ldots, r_{i,k}|0) \in \mathbb{F}^k, H_i = \begin{pmatrix} H_{i-1} \\ R_i \end{pmatrix} \in \mathbb{F}^{(i+1)\times n}$$

$$H^{(L)} = (H_L, \begin{pmatrix} 0_{1\times n} \\ H_{L-1} \end{pmatrix}, \ldots, \begin{pmatrix} 0_{(L-1)\times n} \\ H_0 \end{pmatrix}) \in \mathbb{F}^{(L+1)\times n(L+1)},$$

Example 1. *Let $\mathbb{F} = GF(2^3)$ with primitive element α defined by $\alpha^3 + \alpha + 1 = 0$.*

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \alpha^3 & 1 & 0 & 1 & \alpha & 0 & 1 & 1 & 1 \end{pmatrix}$$

H_2 $\quad H_1$ $\quad H_0$

Parity-check matrix of a convolutional code

Let $m \geq 1, n \geq 2, k = n-1$ be integers, $\mathbb{F} = GF(2^m)$, and define the matrices and vectors

$$R_0 = (r_{0,1}, \ldots, r_{0,k}) \in \mathbb{F}^k \qquad H_0 = (R_0|1) \in \mathbb{F}^n,$$

$$R_i = (r_{i,1}, \ldots, r_{i,k}|0) \in \mathbb{F}^k, H_i = \begin{pmatrix} H_{i-1} \\ R_i \end{pmatrix} \in \mathbb{F}^{(i+1)\times n}$$

$$H^{(L)} = (H_L, \begin{pmatrix} 0_{1\times n} \\ H_{L-1} \end{pmatrix}, \ldots, \begin{pmatrix} 0_{(L-1)\times n} \\ H_0 \end{pmatrix}) \in \mathbb{F}^{(L+1)\times n(L+1)},$$

Example 1. *Let $\mathbb{F} = GF(2^3)$ with primitive element α defined by $\alpha^3 + \alpha + 1 = 0$.*

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \alpha^3 & 1 & 0 & 1 & \alpha & 0 & & & \end{pmatrix}$$

$H^{(0)}$

Parity-check matrix of a convolutional code

Let $m \geq 1, n \geq 2, k = n-1$ be integers, $\mathbb{F} = GF(2^m)$, and define the matrices and vectors

$$R_0 = (r_{0,1}, \ldots, r_{0,k}) \in \mathbb{F}^k \qquad H_0 = (R_0|1) \in \mathbb{F}^n,$$

$$R_i = (r_{i,1}, \ldots, r_{i,k}|0) \in \mathbb{F}^k, H_i = \begin{pmatrix} H_{i-1} \\ R_i \end{pmatrix} \in \mathbb{F}^{(i+1)\times n}$$

$$H^{(L)} = (H_L, \begin{pmatrix} 0_{1\times n} \\ H_{L-1} \end{pmatrix}, \ldots, \begin{pmatrix} 0_{(L-1)\times n} \\ H_0 \end{pmatrix}) \in \mathbb{F}^{(L+1)\times n(L+1)},$$

Example 1. *Let* $\mathbb{F} = GF(2^3)$ *with primitive element* α *defined by* $\alpha^3 + \alpha + 1 = 0$.

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & & & & & & \\ \alpha^3 & 1 & 0 & & & & & & \end{pmatrix}$$

$H^{(1)}$

Parity-check matrix of a convolutional code

Let $m \geq 1, n \geq 2, k = n-1$ be integers, $\mathbb{F} = GF(2^m)$, and define the matrices and vectors

$$R_0 = (r_{0,1}, \ldots, r_{0,k}) \in \mathbb{F}^k \qquad H_0 = (R_0|1) \in \mathbb{F}^n,$$

$$R_i = (r_{i,1}, \ldots, r_{i,k}|0) \in \mathbb{F}^k, H_i = \begin{pmatrix} H_{i-1} \\ R_i \end{pmatrix} \in \mathbb{F}^{(i+1)\times n}$$

$$H^{(L)} = (H_L, \begin{pmatrix} 0_{1\times n} \\ H_{L-1} \end{pmatrix}, \ldots, \begin{pmatrix} 0_{(L-1)\times n} \\ H_0 \end{pmatrix}) \in \mathbb{F}^{(L+1)\times n(L+1)},$$

Example 1. *Let $\mathbb{F} = GF(2^3)$ with primitive element α defined by $\alpha^3 + \alpha + 1 = 0$.*

$$H^{(2)} = \left(\quad \right)$$

$H^{(2)}$

Generator matrix of a convolutional code

A systematic encoder for the code $\mathscr{C}^{(L)}$ is represented by

$$G^{(L)} = \begin{pmatrix} G_0 & G_1 & \cdots & G_L \\ & G_0 & \cdots & G_{L-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{pmatrix} \in \mathbb{F}^{k(L+1)\times n(L+1)}$$

where

$$\boxed{G_0 = (I_k | R_0^\top)} \in \mathbb{F}^{k\times n}, \boxed{G_i = (0_k | R_i^\top)} \in \mathbb{F}^{k\times n} \text{ for } i > 0,$$

Example 1. *Let* $\mathbb{F} = GF(2^3)$ *with primitive element* α *defined by* $\alpha^3 + \alpha + 1 = 0$.

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \alpha^3 & 1 & 0 & 1 & \alpha & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$G^{(2)} = \begin{pmatrix} & & 1 & 0 & 0 & 1 & 0 & 0 & \alpha^3 \\ & & 1 & 0 & 0 & \alpha & 0 & 0 & 1 \\ 0 & 0 & 0 & & & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & & & 1 & 0 & 0 & \alpha \\ 0 & 0 & 0 & 0 & 0 & 0 & & & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & & & 1 \end{pmatrix}$$

$G^{(2)}H^{(2)T}=(0)$

Proper minors and superregularity

Definition 1. *Consider a lower triangular matrix*

$$SR = \begin{pmatrix} r_0 & 0 & 0 & \cdots & 0 \\ r_1 & r_0 & 0 & \cdots & 0 \\ r_2 & r_1 & r_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_L & r_{L-1} & r_{L-2} & \cdots & r_0 \end{pmatrix}$$

where each element $r_i \in \mathbb{F}$.

Consider a square submatrix P *of size* p *of* SR*, formed by the entries of* SR *in the rows with indices* $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ *and columns of indices* $1 \le j_1 < \cdots < j_p \le (L+1)$*.* P*, and its corresponding minor, are proper if* $\boxed{j_l \le i_l}$ *for all* $l \in \{1, \ldots, p\}$*.*

Proper minors and superregularity

Definition 1. *Consider a lower triangular matrix*

$$SR = \begin{pmatrix} & & 0 & \cdots & \\ r_1 & r_0 & 0 & \cdots & 0 \\ & & r_0 & \cdots & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ & {}_1 & r_{L-2} & \cdots & \end{pmatrix}$$

where each element $r_i \in \mathbb{F}$.

Consider a square submatrix P *of size* p *of* SR, *formed by the entries of* SR *in the rows with indices* $1 \leq i_1 < i_2 < \cdots < i_p \leq (L+1)$ *and columns of indices* $1 \leq j_1 < \cdots < j_p \leq (L+1)$. P, *and its corresponding minor, are proper if* $\boxed{j_l \leq i_l}$ *for all* $l \in \{1, \ldots, p\}$.

Proper minors and superregularity

Definition 1. *Consider a lower triangular matrix*

$$SR = \begin{pmatrix} r_0 & 0 & 0 & \cdots & 0 \\ & r_0 & & \cdots & 0 \\ & r_1 & & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_L & r_{L-1} & r_{L-2} & \cdots & r_0 \end{pmatrix}$$

where each element $r_i \in \mathbb{F}$.

Consider a square submatrix P *of size* p *of* SR*, formed by the entries of* SR *in the rows with indices* $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ *and columns of indices* $1 \le j_1 < \cdots < j_p \le (L+1)$*.* P*, and its corresponding minor, are proper if* $\boxed{j_l \le i_l}$ *for all* $l \in \{1, \ldots, p\}$*.*

Proper minors and superregularity

Definition 1. *Consider a lower triangular matrix*

$$SR = \begin{pmatrix} r_0 & & & \cdots & \\ r_1 & r_0 & 0 & \cdots & 0 \\ r_2 & & & \cdots & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_L & & & \cdots & \end{pmatrix}$$

where each element $r_i \in \mathbb{F}$.

Consider a square submatrix P *of size* p *of* SR*, formed by the entries of* SR *in the rows with indices* $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ *and columns of indices* $1 \le j_1 < \cdots < j_p \le (L+1)$*.* P*, and its corresponding minor, are proper if* $\boxed{j_l \le i_l}$ *for all* $l \in \{1, \ldots, p\}$*.*

Proper minors and superregularity

Definition 1. *Consider a lower triangular matrix*

$$SR = \begin{pmatrix} r_0 & 0 & 0 & \cdots & 0 \\ r_1 & r_0 & 0 & \cdots & 0 \\ r_2 & r_1 & r_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_L & r_{L-1} & r_{L-2} & \cdots & r_0 \end{pmatrix}$$

where each element $r_i \in \mathbb{F}$.

Consider a square submatrix P of size p of SR, formed by the entries of SR in the rows with indices $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ and columns of indices $1 \le j_1 < \cdots < j_p \le (L+1)$. P, and its corresponding minor, are proper if $\boxed{j_l \le i_l}$ for all $l \in \{1, \ldots, p\}$.

SR is superregular if all its proper $p \times p$ minors are non singular for any $p \le L+1$.

When matrix SR is upper triangular the definition of proper submatrices is analogous.

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha^2 & \alpha & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & \alpha & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \alpha & \alpha & 1 \end{pmatrix}$$

$\alpha^3 + \alpha + 1 = 0.$

Our contributions

- *s*-superregularity
- Constructions of MDS codes with CDP=(2,3, $\mathscr{D}=4$)
- Efficient algorithm to search for MDS codes with CDP=(2,3,4,…, $\mathscr{D}$), $\mathscr{D}\geq 5$

Proper minors and s-superregularity

Definition 2. *Consider an* s-lower triangular *matrix (where s is a positive integer)*

$$SSR = \begin{pmatrix} r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ r_{2,1} & \cdots & r_{2,s} & r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & r_{L-3,1} & \cdots & r_{L-3,s} & \cdots & 0 & \cdots & 0 \\ r_{L,1} & \cdots & r_{L,s} & r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & \cdots & r_{0,1} & \cdots & r_{0,s} \end{pmatrix} \tag{4}$$

Consider a square submatrix P of size p of SSR, formed by the entries of SSR in the rows with indices $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ and columns of indices $1 \le j_1 < \cdots < j_p \le s(L+1)$. P, and its corresponding minor, are proper if $\boxed{j_l \le s \cdot i_l}$ for all $l \in \{1, \ldots, p\}$.

Proper minors and s-superregularity

Definition 2. *Consider an* s-lower triangular *matrix (where* s *is a positive integer)*

$$SSR = \begin{pmatrix} {} & \cdots & {} & 0 & \cdots & 0 & {} & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ {} & \cdots & {} & r_{1,1} & \cdots & r_{1,s} & {} & \cdots & r_{0,s} & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ldots & \vdots & \ddots & \vdots \\ {} & \cdots & {} & r_{L-2,1} & \cdots & r_{L-2,s} & {} & \cdots & r_{L-3,s} & \cdots & 0 & \cdots & 0 \\ r_{L,1} & \cdots & r_{L,s} & r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & \cdots & r_{0,1} & \cdots & r_{0,s} \end{pmatrix} \qquad (4)$$

Consider a square submatrix P *of size* p *of SSR, formed by the entries of SSR in the rows with indices* $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ *and columns of indices* $1 \le j_1 < \cdots < j_p \le s(L+1)$. P*, and its corresponding minor, are* *proper* *if* $\boxed{j_l \le s \cdot i_l}$ *for all* $l \in \{1, \ldots, p\}$.

Proper minors and s-superregularity

Definition 2. *Consider an* s-lower triangular *matrix (where* s *is a positive integer)*

$$SSR = \begin{pmatrix} & \cdots & r_{0,s} & 0 & \cdots & 0 & & \cdots & & \cdots & 0 & \cdots & 0 \\ r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ & \cdots & r_{2,s} & r_{1,1} & \cdots & r_{1,s} & & \cdots & & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & & \cdots & & \cdots & 0 & \cdots & 0 \\ r_{L,1} & \cdots & r_{L,s} & r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & \cdots & r_{0,1} & \cdots & r_{0,s} \end{pmatrix} \tag{4}$$

Consider a square submatrix P *of size* p *of SSR, formed by the entries of SSR in the rows with indices* $1 \leq i_1 < i_2 < \cdots < i_p \leq (L+1)$ *and columns of indices* $1 \leq j_1 < \cdots < j_p \leq s(L+1)$. P*, and its corresponding minor, are* *proper* *if* $\boxed{j_l \leq s \cdot i_l}$ *for all* $l \in \{1, \ldots, p\}$.

Proper minors and s-superregularity

Definition 2. *Consider an s-*lower triangular *matrix (where s is a positive integer)*

$$SSR = \begin{pmatrix} & \cdots & r_{0,s} & 0 & \cdots & 0 & & \cdots & 0 & \cdots & & \cdots & 0 \\ r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ & \cdots & r_{2,s} & r_{1,1} & \cdots & r_{1,s} & & \cdots & r_{0,s} & \cdots & & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & & \cdots & r_{L-3,s} & \cdots & & \cdots & 0 \\ r_{L,1} & \cdots & r_{L,s} & r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & \cdots & r_{0,1} & \cdots & r_{0,s} \end{pmatrix} \quad (4)$$

Consider a square submatrix P of size p of SSR, formed by the entries of SSR in the rows with indices $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ *and columns of indices* $1 \le j_1 < \cdots < j_p \le s(L+1)$. *P, and its corresponding minor, are proper if* $\boxed{j_l \le s \cdot i_l}$ *for all* $l \in \{1, \ldots, p\}$.

Proper minors and s-superregularity

Definition 2. *Consider an s-*lower triangular *matrix (where s is a positive integer)*

$$SSR = \begin{pmatrix} r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ r_{2,1} & \cdots & r_{2,s} & r_{1,1} & \cdots & r_{1,s} & r_{0,1} & \cdots & r_{0,s} & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\ r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & r_{L-3,1} & \cdots & r_{L-3,s} & \cdots & 0 & \cdots & 0 \\ r_{L,1} & \cdots & r_{L,s} & r_{L-1,1} & \cdots & r_{L-1,s} & r_{L-2,1} & \cdots & r_{L-2,s} & \cdots & r_{0,1} & \cdots & r_{0,s} \end{pmatrix} \tag{4}$$

Consider a square submatrix P of size p of SSR, formed by the entries of SSR in the rows with indices $1 \le i_1 < i_2 < \cdots < i_p \le (L+1)$ *and columns of indices* $1 \le j_1 < \cdots < j_p \le s(L+1)$. *P, and its corresponding minor, are* proper *if* $\boxed{j_l \le s \cdot i_l}$ *for all* $l \in \{1, \ldots, p\}$.

*The matrix SSR is called s-*superregular *iff all of its proper* $p \times p$ *minors, for any* $p \le L+1$, *are nonsingular.*

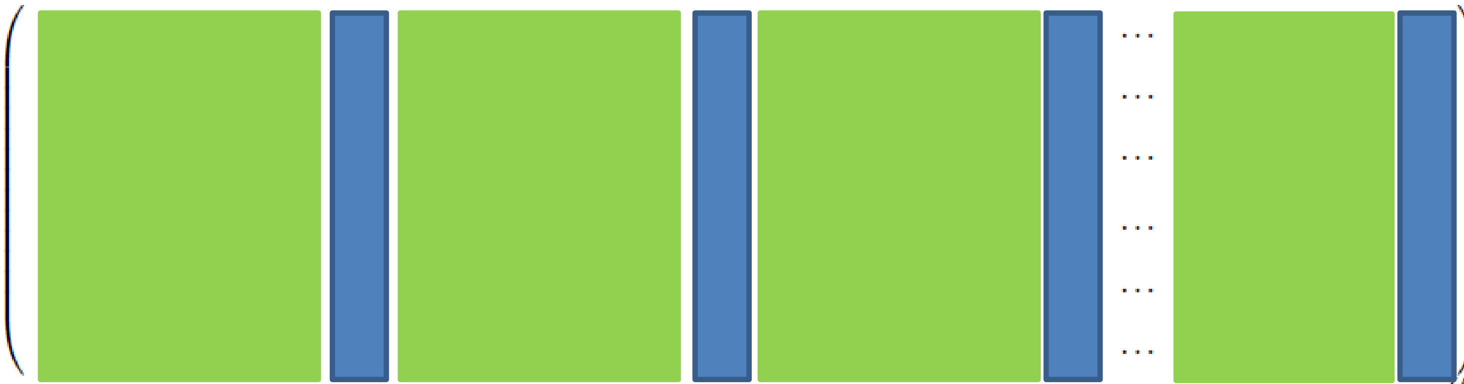
$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 1 & 1 & 0 & 0 \\ \alpha^3 & 1 & 1 & \alpha & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 1 & 0 & 0 \\ 1 & \alpha & 1 & \alpha & 1 & 1 \end{pmatrix}$$

$\alpha^3 + \alpha + 1 = 0.$

Superregularity and CDP

Lemma 1. *Let $H^{(D)}$ be the parity check matrix of the $D-th$ truncation of a systematic convolutional code, given by*

$H^{(D)} =$



(5)

and let $H'^{(D)}$ be the matrix obtained from $H^{(D)}$ by removing the columns in positions $(k+1), 2(k+1), 3(k+1), \ldots, (D+1)(k+1)$, that is

$H'^{(D)} =$

(6)

Then the CDP of the convolutional code given by $H^{(D)}$ is $(2,3,\ldots,D+2)$ if and only if $H'^{(D)}$ is a k-superregular matrix.

Known for k=1: Gluesing-Luerssen *et al* 2006, Gabidulin 1989

Binary superregular matrices?

- *1*-superregularity
- 1x1:

$$(1) \quad \rightarrow (2,1)\ block\ code$$

- 2x2:

$$\begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix} \rightarrow (2,1)\ conv.code, cdp = (2,3)$$

- 3x3 not possible

$$\begin{pmatrix} 1 & & \\ 1 & 1 & \\ ? & 1 & 1 \end{pmatrix} \rightarrow NO\ (2,1)\ conv.code, cdp = (2,3,4)$$

The problem addressed here

Definition 3. *Let $\Delta(2^m, n)$ be the largest free distance $\mathscr{D}$ such that there exists a rate $(n-1)/n$ systematic MDS convolutional code over $GF(2^m)$ with column distance profile as in (3).*

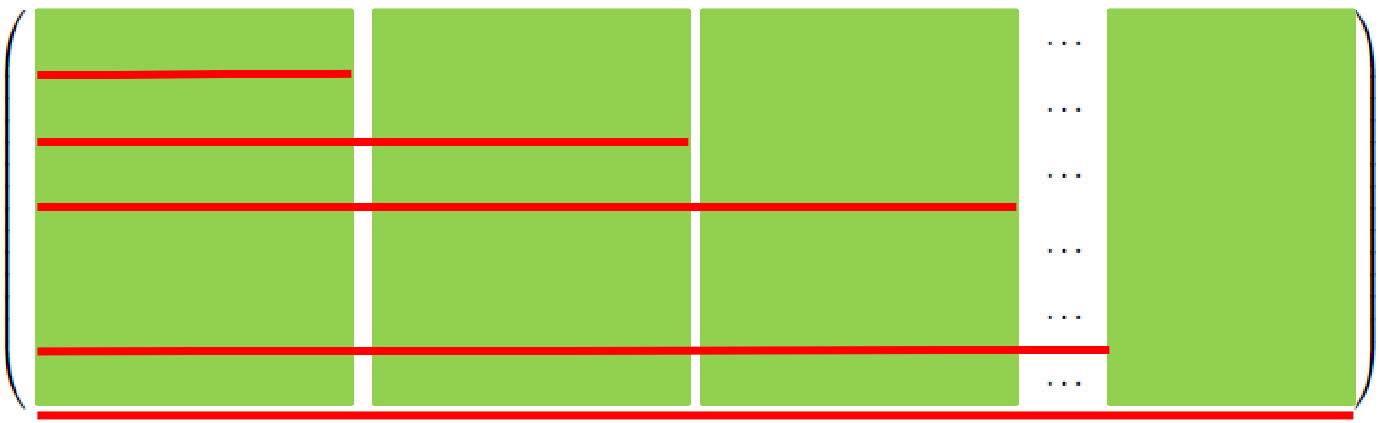
$$d_0 = 2, d_1 = 3, \ldots, d_j = j+2, \ldots, d_D = D+2 = \mathscr{D}. \tag{3}$$

The main problem that we address in this paper is to determine exact values, or constructive lower bounds, for $\Delta(2^m, n)$. Please note that there is no restriction of the degree D in Definition 3.

The problem addressed here : approach

Add coefficients $r_{i,j}$. How many layers $r_{i,1}, \dots, r_{i,k}$ can be completed, maintaining the s-superregularity?

$H'^{(D)} =$



If the layer $r_{D,1}, \dots, r_{D,k}$ can be completed, maintaining the superregularity, the corresponding code has column distance $2, 3, \dots, D+2$

Previous world records for $2^m \geq 4$

Rate	Field size	$\mathscr{D}$

Table I

Some rate $(n-1)/n$ MDS codes (not necessarily systematic) described in the literature.

New constructions : distance 3

Lemma 2. *We can w.l.o.g assume* $r_{0,1} = \cdots = r_{0,n} = 1$.

Proposition 2. $\Delta(q^m, q^m) = 3$ *for* q *prime and* $m \geq 0$.

Proof: Select $r_{0,i} = 1$ and $r_{1,i}$, $i = 1, \ldots, q^m - 1$ as the $q^m - 1$ distinct nonzero elements of $GF(q^m)$. Without loss of generality, the parity check matrix of (1) takes the form

$$H^{(1)} = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 2 & \cdots & q^m - 1 & 0 & 1 & \cdots & 1 & 1 \end{pmatrix}$$

$$H'^{(1)} = \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ 1 & 2 & \cdots & q^m - 1 & 1 & \cdots & 1 \end{pmatrix}$$

Comparison with Wyner-Ash code:

$$H_{\mathrm{WA}} = \begin{pmatrix} 1 + x + x^2 & 1 + x & 1 + x^2 & 1 \end{pmatrix}.$$

It is easy to see that the CDP of the Wyner-Ash code is $[2, 2, 3]$, i. e. *this is* not *an MDS code. The construction of Proposition 2 can be considered as a* q^m*-ary generalization of the Wyner-Ash code, of memory 2, but this code is an MDS code, with CDP* $[2, 3]$.

New constructions: distance 4

Lemma 4. *For a code with a CDP of* $[2,3,4]$, *its parity check matrix* $H^{(2)}$ *must satisfy*
(i) $r_{i,s} \neq 0$ *for* $i = 1,2,\ s = 1,\ldots,k$,
(ii) $r_{i,s} \neq r_{i,t}$ *for* $i = 1,2,\ 1 \leq s < t \leq k$,
(iii) $r_{1,t} \neq r_{2,s}/r_{1,s}$ *for* $1 \leq s,t \leq k$,
(iv) $r_{2,s}/r_{1,s} \neq r_{2,t}/r_{1,t}$ *for* $1 \leq s < t \leq k$,
(v) $r_{2,s} - r_{2,t} \neq r_{1,u}(r_{1,s} - r_{1,t})$ *for* $1 \leq s < t \leq k,\ 1 \leq u \leq k$,
(vi) $r_{2,s} \neq (r_{1,s}(r_{2,u} - r_{2,t}) - r_{1,t}r_{2,u} + r_{1,u}r_{2,t})/(r_{1,u} - r_{1,t})$ *for* $1 \leq s < t < u \leq k$.

Proof:

$$\begin{vmatrix} 1 & 0 \\ r_{i,s} & 1 \end{vmatrix}, \begin{vmatrix} 1 & 0 \\ r_{2,s} & r_{1,t} \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ r_{i,s} & r_{i,t} \end{vmatrix}, \begin{vmatrix} r_{1,s} & 1 \\ r_{2,s} & r_{1,t} \end{vmatrix}, \begin{vmatrix} r_{1,s} & r_{1,t} \\ r_{2,s} & r_{2,t} \end{vmatrix}$$

$$\begin{vmatrix} 1 & 0 & 0 \\ r_{i,s} & 1 & 0 \\ r_{2,s} & r_{2,t} & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 & 0 \\ r_{i,s} & r_{1,t} & 0 \\ r_{2,s} & r_{2,t} & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 & 0 \\ r_{i,s} & r_{1,t} & 1 \\ r_{2,s} & r_{2,t} & r_{1,u} \end{vmatrix}, \begin{vmatrix} 1 & 1 & 1 \\ r_{i,s} & r_{1,t} & r_{1,u} \\ r_{2,s} & r_{2,t} & r_{2,u} \end{vmatrix}$$

New constructions

Example 1:

has CDP equal to [2,3,4].

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \alpha^3 & 1 & 0 & 1 & \alpha & 0 & 1 & 1 & 1 \end{pmatrix} \quad H(x) = (1 + x + \alpha^3 x^2, 1 + \alpha x + x^2, 1).$$

New constructions

Proposition 3. $\Delta(2^m, 2^{m-1}) = 4.$

Proof:

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ a_1 & a_2 & \dots & a_k & 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ b_1 & b_2 & \dots & b_k & a_1 & a_2 & \dots & a_k & 1 & 1 & \dots & 1 \end{pmatrix}$$

Let $\mathbb{F} = GF(2^m)$.

$$\begin{array}{rccc} Tr^m(): & \mathbb{F} & \to & GF(2) \\ & x & \to & Tr^m(x) = \sum_{i=0}^{m-1} x^{2^i}. \end{array}$$

$H_\beta = \{x \in \mathbb{F} | Tr^m(\beta x) = 0\}.$

Let $k = 2^{m-1} - 1$, select β as an arbitrary nonzero field element, select c as an arbitrary constant in $\mathbb{F} \setminus H_\beta$. Then select $a_1, \dots, a_k := r_{1,1}, \dots, r_{1,k}$ as all distinct nonzero elements in H_β, and set $b_s := r_{2,s} = a_s(a_s + c) = r_{1,s}(r_{1,s} + c)$ for $s = 1, \dots, k$. We need to verify that this construction satisfies the conditions in Lemma 4

Proof, distance=4, rate=$\frac{2^{m-1}-1}{2^{m-1}}$ construction

(i) This holds because $b_s = a_s(a_s + c)$ is a product of two nonzeros.
(ii) All a_s's are distinct. Assume that $b_s = b_t, s \neq t$. Then $0 = a_s(a_s+c) = a_t(a_t+c) = (a_s+a_t)c + a_s^2 + a_t^2 = (a_s+a_t)c + (a_s+a_t)^2 = (a_s+a_t)(c+a_s+a_t)$. The first factor is nonzero since $a_s \neq a_t$. The second factor is also nonzero since $a_s + a_t \in H_\beta$ (because H_β is closed under addition) while $c \notin H_\beta$, a contradiction.
(iii) Assume that $a_s a_t = b_s$. Then $a_s a_t = a_s(a_s+c) \Rightarrow a_t = a_s + c$, a contradiction, since $a_t \in H_\beta$ and $a_s + c \notin H_\beta$.
(iv) Assume that $b_s/a_s = b_t/a_t, s \neq t$. Then $a_s + c = a_t + c \Rightarrow a_s = a_t$, a contradiction.
(v)

$$\begin{aligned} b_s + b_t + a_u(a_s+a_t) &= a_s(a_s+c) + a_t(a_t+c) + a_u(a_s+a_t) \\ &= a_s^2 + a_t^2 + (a_s+a_t)(c+a_u) \\ &= (a_s+a_t)^2 + (a_s+a_t)(c+a_u) \\ &= (a_s+a_t)(a_s+a_t+c+a_u) \end{aligned}$$

which again is a product of nonzero factors, because $c \notin H_\beta$ and $a_s + a_t + a_u \in H_\beta$, and hence nonzero.
(vi)

$$\begin{aligned} b_s + \frac{a_s(b_t+b_u) + a_u b_t + a_t b_u}{a_t + a_u} &= a_s(a_s+c) + \frac{a_s(a_t(a_t+c) + a_u(a_u+c)) + a_u a_t(a_t+c) + a_t a_u(a_u+c)}{a_t+a_u} \\ &= a_s(a_s+c) + \frac{a_s(a_t+a_u)^2 + a_s c(a_t+a_u) + a_t a_u(a_t+a_u)}{a_t+a_u} \\ &= a_s(a_s+c) + a_s(a_t+a_u) + a_s c + a_t a_u \\ &= a_s^2 + a_s a_t + a_s a_u + a_t a_u \\ &= (a_s+a_t)(a_s+a_u) \neq 0. \end{aligned}$$

Computer search algorithm

The goal of the search algorithm is to select the coefficients $r_{i,j}$ successively, ordered first on i and then reversely on j, in such a way that the conditions on the minors are met.

1) Some useful facts:

Lemma 5. *We can w.l.o.g assume* $r_{1,i} < r_{1,i+1}$, $i = 1,\dots,k-1$ *for any choice of ordering* $<$.

Lemma 6. *Consider an MDS convolutional code* $\mathscr{C}$ *with polynomial parity check matrix*

$$H(x) = (1+\sum_{i=1}^{D} r_{i,1}x^i,\dots,1+\sum_{i=1}^{D} r_{i,k}x^i,1) \in \mathbb{F}[x].$$

Then the code $\mathscr{C}_c$ *with parity check matrix*

$$H_c(x) = (1+\sum_{i=1}^{D} c^i r_{i,1}x^i,\dots,1+\sum_{i=1}^{D} c^i r_{i,k}x^i,1) \in \mathbb{F}[x]$$

is also MDS for any $c \in \mathbb{F}\setminus\{0\}$.

Proof. Let $v(x) = (v_1(x),\dots,v_n(x)) = (\sum_{i=0}^{D} v_{1,i}x^i,\dots,\sum_{i=0}^{D} v_{n,i}x^i)$. Then $v(x)H(x)^\top = 0$ iff $v_c(x)H_c(x)^\top = 0$ for

$$v_c(x) = (\sum_{i=0}^{D} c^{-i}v_{1,i}x^i,\dots,\sum_{i=0}^{D} c^{-i}v_{n,i}x^i).$$

□

Corollary 1. *If a systematic MDS convolutional code exists, we can w.l.o.g. assume that it has a parity check matrix with* $r_{1,k} = 1$.

Computer search algorithm

The goal of the search algorithm is to select the coefficients $r_{i,j}$ successively, ordered first on i and then reversely on j, in such a way that the conditions on the minors are met.

1) Some useful facts:

Lemma 7. *Let M be a k-superregular matrix over $GF(q^m)$, with q a prime. Raising each element of M to power q yields another k-superregular matrix.*

Corollary 2. *In particular, let M be a k-superregular matrix over $GF(2^m)$. Squaring each element of M yields another k-superregular matrix.*

Corollary 3. *Assume that the values for $r_{0,i}$, $i = 1,\ldots,k$ and for $r_{1,k}$ are all fixed to 1, as allowed by Lemma 3 and Corollary 1. Then, for $r_{1,k-1}$, it suffices to consider one representative of each cyclotomic coset.*

Computer search algorithm

The goal of the search algorithm is to select the coefficients $r_{i,j}$ successively, ordered first on i and then reversely on j, in such a way that the conditions on the minors are met.

Algorithm 1: A computer search algorithm

Result: finds good 2^m-ary MDS codes of rate $(n-1)/n$

Input : Field size 2^m, target distance $\mathscr{D}^*$, code length n

Data: ρ points to current position

initialization;

value$(r_{0,i}) := 1, i = 1, \ldots, k,$ *value*$(r_{1,k}) = 1;$

Precompute the set of proper submatrices $\mathscr{M} = \bigcup_{\rho=r_{1,k-1}}^{r_{\mathscr{D}^*-2,1}} \mathscr{M}_\rho;$

$\rho := r_{1,k-1};$

Precompute the set of legal values $\mathscr{L}(\rho);$

while $\rho \leq r_{\mathscr{D}^*-2,1}$ *and* more coefficient values to check for ρ **do**

    if *more coefficient values to check for* ρ **then**

        assign next value to coefficient at ρ;

        update determinants needed for $\mathscr{M}_{\rho+1}$, and $\mathscr{L}(\rho+1)$;

        if *deepest level so far* **then**

            record selected values of coefficients;

        end

        $\rho = \rho + 1;$

    else

        $\rho = \rho - 1;$

    end

end

Codes found by computer search

n	Δ	Coefficients	R	Remark
2	6	0, 1, 4, 3	0.035	

Justesen & Hughes (1974)

Table II

TABLE OF BOUNDS ON $\Delta(2^3, n)$ FOR THE FIELD DEFINED BY $1+\alpha+\alpha^3=0$.

n	Δ	Coefficients	R	Remark
2	7	0, 1, 4, 3, 0	0.024	
3	5	1, 0, 7	0.014	

Gluesing-Luersen et. al, «Strongly MDS…», 2006

Table III

TABLE OF BOUNDS ON $\Delta(2^4, n)$ FOR THE FIELD DEFINED BY $1+\alpha+\alpha^4=0$. PLEASE ALSO SEE EXAMPLE 3.

Example 3.

$$H(x) = (+ \alpha x + x^2 + \alpha^7 x^3, + x + x^2 + x^3,)$$

Implicit

$$G(x) = \begin{pmatrix} 1 & 0 & 1+\alpha x + x^2 + \alpha^7 x^3 \\ 0 & 1 & 1 + x + \alpha^4 x^2 + \alpha x^3 \end{pmatrix}$$

Polynomial notation for convolutional codes

In the conventional polynomial notation of convolutional codes [10], the parity check matrix can be described as

$$H(x) = \left(\sum_{i=0}^{D} r_{i,1}x^i, \ldots, \sum_{i=0}^{D} r_{i,k}x^i, 1\right) \in \mathbb{F}[x].$$

Example 1:

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \alpha^3 & 1 & 0 & 1 & \alpha & 0 & 1 & 1 & 1 \end{pmatrix} \quad H(x) = (1 + x + \alpha^3 x^2, 1 + \alpha x + x^2, 1).$$

$$G^{(2)} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \alpha^3 \\ 0 & 1 & 1 & 0 & 0 & \alpha & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \alpha \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad G(x) = \begin{pmatrix} 1 & 0 & 1 + x + \alpha^3 x^2 \\ 0 & 1 & 1 + \alpha x + x^2 \end{pmatrix}$$

Codes found by computer search

n	Δ	Coefficients	R	Remark
2	6	0, 1, 4, 3	0.035	[3]

Table II

TABLE OF BOUNDS ON $\Delta(2^3, n)$ FOR THE FIELD DEFINED BY $1+\alpha+\alpha^3=0$.

n	Δ	Coefficients	R	Remark
2	7	0, 1, 4, 3, 0	0.024	
3	5	0 [illegible] 4 [illegible] 1 [illegible]	0.014	[5]

Table III

TABLE OF BOUNDS ON $\Delta(2^4, n)$ FOR THE FIELD DEFINED BY $1+\alpha+\alpha^4=0$. PLEASE ALSO SEE EXAMPLE 3.

Example 3.

$$H(x) = (1+\alpha x+x^2+\alpha^7 x^3, 1+x+\alpha^4x^2+\alpha x^3, 1)$$

$$G(x) = \begin{pmatrix} 1 & 0 & 1+\alpha x+x^2+\alpha^7x^3 \\ 0 & 1 & 1+x+\alpha^4x^2+\alpha x^3 \end{pmatrix}$$

Codes found by computer search

n	Δ	Coefficients	R
2	9	0, 1, 19, 5, 24, 15, 0	$3.4 \cdot 10^{-8}$
3	6	0 1, 11 28, 21 6, 24 11	$4.4 \cdot 10^{-5}$
5	5	0 1 18 2, 5 8 17 25, 3 2 13 18	$5.2 \cdot 10^{-11}$

Table IV

TABLE OF BOUNDS ON $\Delta(2^5, n)$ FOR THE FIELD DEFINED BY $1 + \alpha^2 + \alpha^5 = 0$.

n	Δ	Coefficients	R
2	10	0, 1, 6, 61, 60, 46, 28, 23	$1.2 \cdot 10^{-10}$
3	7	0 1, 6 0, 2 37, 21 44, 55 28	$4.1 \cdot 10^{-11}$
4	≥ 6	0 1 6, 2 6 26, 13 61 38, 30 33 60	$1.4 \cdot 10^{-11}$
7	≥ 5	0 1 6 2 12 3, 14 36 26 25 51 13, 19 60 16 62 5 58	$3.2 \cdot 10^{-20}$

Table V

TABLE OF BOUNDS ON $\Delta(2^6, n)$ FOR THE FIELD DEFINED BY $1 + \alpha + \alpha^6 = 0$.

Rareness

rareness of the parameter pair $(n, \mathscr{D})$

probability that a randomly generated convolutional code over $GF(2^m)$ of rate $(n-1)/n$ will be an MDS code with CDP of $[2, \ldots, \mathscr{D}]$.

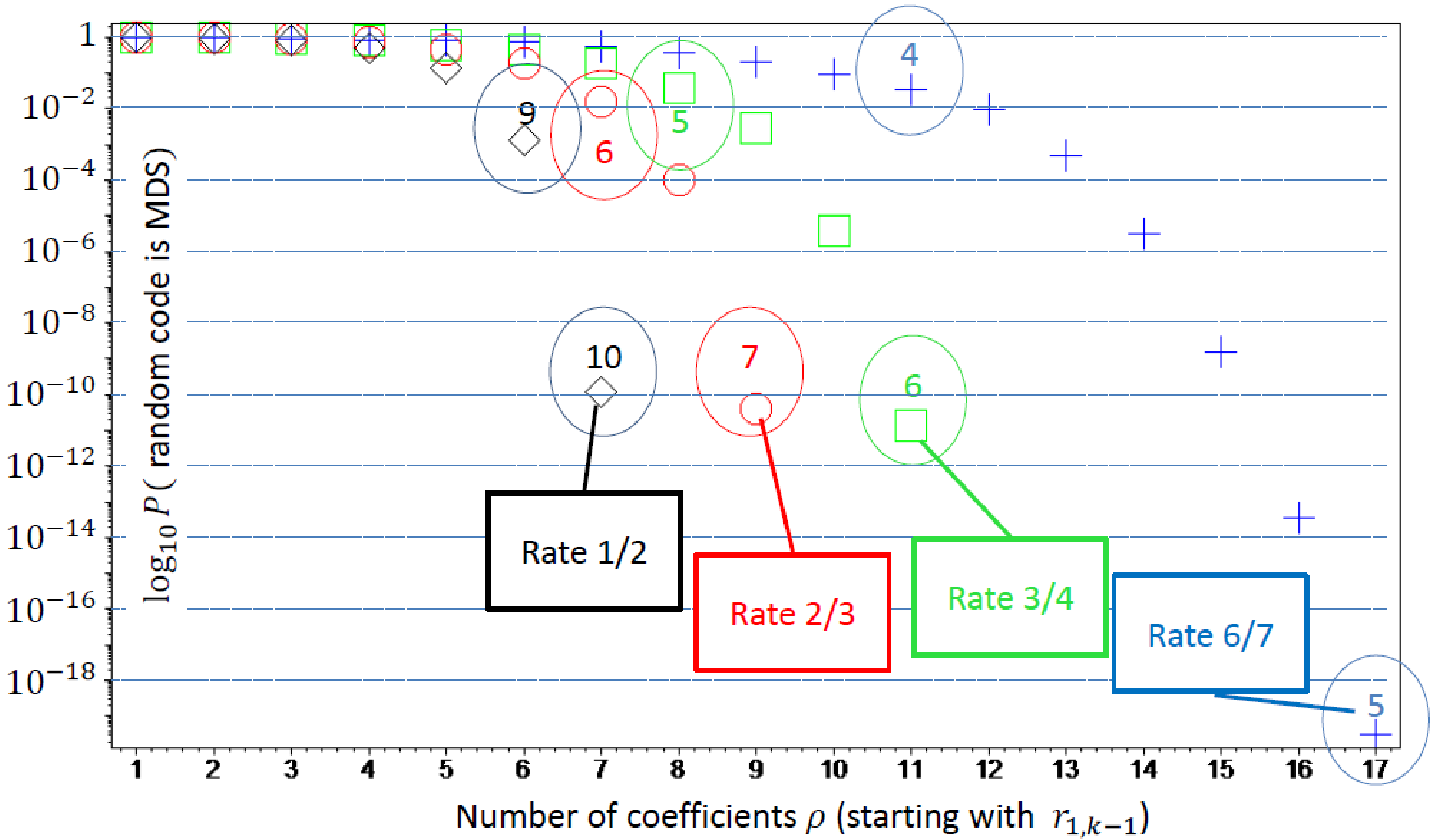


Figure 1. Rareness $P_R(\rho, n, 6)$ of codes for $GF(64)$ for $n \in \{2,3,4,7\}$: Exact rareness $P_R(\rho, n, 6)$ for $\rho \leq 7$, estimates $\tilde{P}_R(\rho, n, 6)$ for $n > 7$. In the figure, the search depth ρ is measured in terms of number of coefficients. In order to construct a rate 6/7 encoder of distance $\mathscr{D} = 5$, it is necessary to find a sequence of 17 coefficients $r_{1,5}, \ldots, r_{1,1}, r_{2,6}, \ldots, r_{3,1}$. To get an encoder with distance $\mathscr{D} = 4$, it suffices with 11 coefficients. Similar for the other cases.

Codes found by computer search

n	Δ	Coefficients	R
5	≥ 6	0 1 31 2, 62 103 64 125, 51 57 19 110, 11 39 43 114	$8 \cdot 10^{-18}$
8	≥ 5	0 1 31 2 62 32 103, 3 31 15 0 7 1 63, 8 94 119 51 41 10 17	$6.4 \cdot 10^{-16}$

Table VI

TABLE OF BOUNDS ON $\Delta(2^7, n)$ FOR THE FIELD DEFINED BY $1+\alpha^3+\alpha^7=0$.

n	Δ	Coefficients	R
2	≥ 11	0, 1, 25, 3, 0, 198, 152, 56, 68	$2.2 \cdot 10^{-7}$
3	≥ 8	0 1, 25 0, 1 238, 100 106, 195 245, 37 33	$2.0 \cdot 10^{-12}$
4	≥ 7	0 1 25, 2 25 198, 1 14 228, 113 74 214, 21 250 172	$\approx 2 \cdot 10^{-17}$
11	≥ 5	0 96 95 176 156 169 160 81 11 245, 107 5 223 167 7 177 98 238 93 53, 37 208 233 89 75 74 184 31 119 100	$\approx 3 \cdot 10^{-28}$

Table VII

TABLE OF BOUNDS ON $\Delta(2^8, n)$ FOR THE FIELD DEFINED BY $1+\alpha^2+\alpha^3+\alpha^4+\alpha^8=0$.

Codes found by computer search

n	Δ	Coefficients	R
2	≥ 12	0, 54, 91, 181, 267, 291, 379, 28, 95, 143	$1.4 \cdot 10^{-11}$
6	≥ 6	0 280 362 276 426, 206 155 326 324 360, 356 447 507 312 144, 224 375 236 55 448	$3.9 \cdot 10^{-11}$
13	≥ 5	0 19 325 321 356 397 317 455 98 130 149 413, 48 101 120 272 209 188 405 352 46 343 289 152, 318 80 256 98 255 274 147 340 392 453 30 451	$8.4 \cdot 10^{-27}$

Table VIII

TABLE OF BOUNDS ON $\Delta(2^9, n)$ FOR THE FIELD DEFINED BY $1 + \alpha^4 + \alpha^9 = 0$.

n	Δ	Coefficients	R
3	≥ 9	0 603, 246 106, 115 693, 483 544, 603 152, 815 788, 984 721	$\approx 10^{-15}$
5	≥ 7	0 498 997 964, 560 214 101 723, 453 111 370 54, 455 17 625 509, 904 431 926 856	$5 \cdot 10^{-18}$
8	≥ 6	0 322 804 12 140 1004 384, 778 916 786 247 586 698 294, 379 7 784 239 817 284 398, 178 588 110 41 425 976 393	$3 \cdot 10^{-24}$
17	≥ 5	0 1 77 2 154 78 956 3 10 155 325 79 618 957 231 4, 308 0 4 77 11 1 200 10 80 3 24 155 87 325 619 618, 958 768 255 404 577 976 368 374 709 33 530 109 677 594 652 226	$4 \cdot 10^{-39}$

Table IX

TABLE OF BOUNDS ON $\Delta(2^{10}, n)$ FOR THE FIELD DEFINED BY $1 + \alpha^3 + \alpha^{10} = 0$.

Codes found by computer search

n	Δ	Coefficients	R
2	≥ 13	0, 1992, 813, 1890, 440, 630, 1947, 1574, 1356, 234, 1266	$1.0 \cdot 10^{-9}$
4	≥ 8	0 1809 1118, 2027 1610 539, 1042 7 1730, 2020 591 1459, 902 899 1584, 172 1192 513	$5.6 \cdot 10^{-15}$
9	≥ 6	0 1999 762 1845 1102 1115 1014 328, 1349 345 498 1561 27 987 1300 1793, 1728 562 488 304 43 71 1911 1140, 1524 660 465 327 322 748 1574 1414	$2.0 \cdot 10^{-22}$

Table X

TABLE OF BOUNDS ON $\Delta(2^{11}, n)$ FOR THE FIELD DEFINED BY $1 + \alpha^2 + \alpha^{11} = 0$.

n	Δ	Coefficients	R
2	≥ 14	0, 3294, 1040, 448, 3624, 2406, 826, 1122, 587, 1034, 342, 4037	$< 10^{-15}$
6	≥ 7	0 3202 2711 92 2688, 3908 1649 1252 3897 1604, 3687 3602 1603 2339 1350, 1700 2969 104 3406 2679, 1345 919 3302 2116 810	$1.2 \cdot 10^{-14}$
11	≥ 6	0 669 4050 4007 745 3863 324 1617 3951 1343, 703 1123 782 3343 1919 3177 1839 1006 2183 426, 2139 2050 1676 1187 3222 467 1764 2387 2868 641, 2564 2249 3187 3114 3228 743 443 1220 3540 2620	$3 \cdot 10^{-31}$

Table XI

TABLE OF BOUNDS ON $\Delta(2^{12}, n)$ FOR THE FIELD DEFINED BY $1 + \alpha^3 + \alpha^4 + \alpha^7 + \alpha^{12} = 0$.

Codes found by computer search

n	Δ	Coefficients	R
3	$\geq$10	0 337, 7672 6843, 3625 3361, 7970 7490, 5531 2322, 5227 5758, 133 2290, 1453 189	$3.6 \cdot 10^{-11}$
5	$\geq$8	0 441 2192 3413, 3222 7502 7405 4155, 88 5939 343 6171, 1082 8149 2823 7269, 8022 6454 4999 3373, 3518 442 710 6968	$\approx 5 \cdot 10^{-21}$
7	$\geq$7	0 5160 5711 7681 748 5319, 2131 6233 723 4539 7315 5654, 5126 7465 3577 6826 5553 1131, 4954 6763 6593 1568 7157 8112, 1961 4310 877 2927 7197 2672	$2 \cdot 10^{-19}$
13	$\geq$6	0 5645 7651 3109 2678 802 6934 1946 5589 2833 5821 38, 5394 2500 5877 3141 4724 3374 5191 7218 4844 423 822 6875, 5712 6619 3935 6414 8025 1422 4391 5698 5481 6850 2635 4786, 556 2558 1063 5172 566 7978 3664 5848 3859 6905 6434 71	$\approx 8 \cdot 10^{-37}$

Table XII

TABLE OF BOUNDS ON $\Delta(2^{13}, n)$ FOR THE FIELD DEFINED BY $1+\alpha+\alpha^3+\alpha^4+\alpha^{13}=0$.

Codes found by computer search

n	Δ	Coefficients	R
4	≥ 9	0 61 9533, 1260 4487 6469, 3689 8777 4510, 11257 13252 1239, 15121 10306 11679, 9618 13110 4549, 12420 5210 13006	$3 \cdot 10^{-14}$
8	≥ 7	0 14132 6404 8841 7620 6707 1150, 14939 8238 9174 9560 1677 4156 11112, 11424 2037 7827 4640 11071 14007 6628, 13374 10684 2080 14648 1097 14383 1198, 10966 15875 9746 9595 13007 4019 1354	$1.4 \cdot 10^{-22}$
15	≥ 6	0 15439 10581 4136 503 11096 5590 8608 16006 8229 562 15423 14311 16137, 5899 1875 8985 16334 15293 13429 5172 5303 9128 109 10068 1358 7752 6288, 13251 13386 11513 2438 443 15582 4641 2845 3509 12593 6608 14686 11470 15578, 8683 12489 444 8891 4727 12844 12383 5530 4478 9079 9226 5886 6790 8363	$2 \cdot 10^{-38}$

Table XIII

TABLE OF BOUNDS ON $\Delta(2^{14}, n)$ FOR THE FIELD DEFINED BY $1+\alpha+\alpha^{11}+\alpha^{12}+\alpha^{14}=0$.

Upper bounds

Theorem 1. *For rate $(n-1)/n$ codes over $GF(q^m)$ with $CDP = [2,3,\ldots,\mathscr{D}]$, $n-1 \leq (q^m-1)/(\mathscr{D}-2)$.*

Proof:

$\mathscr{D}=3$ Proposition 2.

$\mathscr{D}=4$

$$\begin{vmatrix} 1 & 1 \\ r_{1,s} & r_{1,t} \end{vmatrix} = r_{1,s}+r_{1,t}, \begin{vmatrix} r_{1,s} & r_{1,t} \\ r_{2,s} & r_{2,t} \end{vmatrix} = r_{1,s}r_{2,t}+r_{1,t}r_{2,s}, \text{ and } \begin{vmatrix} r_{1,s} & 1 \\ r_{2,s} & r_{1,t} \end{vmatrix} = r_{2,s}+r_{1,s}r_{1,t}.$$

$\mathscr{D}>4$

$$\begin{vmatrix} r_{2,s} & r_{2,t} \\ r_{3,s} & r_{3,t} \end{vmatrix} = r_{2,s}r_{3,t}+r_{2,t}r_{3,s}, \begin{vmatrix} r_{2,s} & 1 \\ r_{3,s} & r_{1,t} \end{vmatrix} = r_{2,s}r_{1,t}+r_{3,s}, \text{ and } \begin{vmatrix} r_{2,s} & r_{1,t} \\ r_{3,s} & r_{2,t} \end{vmatrix} = r_{2,s}r_{2,t}+r_{1,t}r_{3,s}.$$

Generalizing the argument, it follows that all $r_{i,t}/r_{i-1,t}$ for $1 \leq i \leq \mathscr{D}-2, 1 \leq t \leq k$ are distinct nonzero values.

Conclusions

Motivated by the practical problem of fast recovery of a coded packet-erasure channel, we have studied systematic MDS convolutional codes over $GF(2^m)$.

We have presented new optimum constructions for free distances $\mathscr{D} \leq 4$,

tables of new codes found by computer search,

and a combinatorial upper bound which is tight in the case of small free distances.

In order to assess how "good" a code is, we have also introduced the concept of *rareness*.


Questions?
Comments?