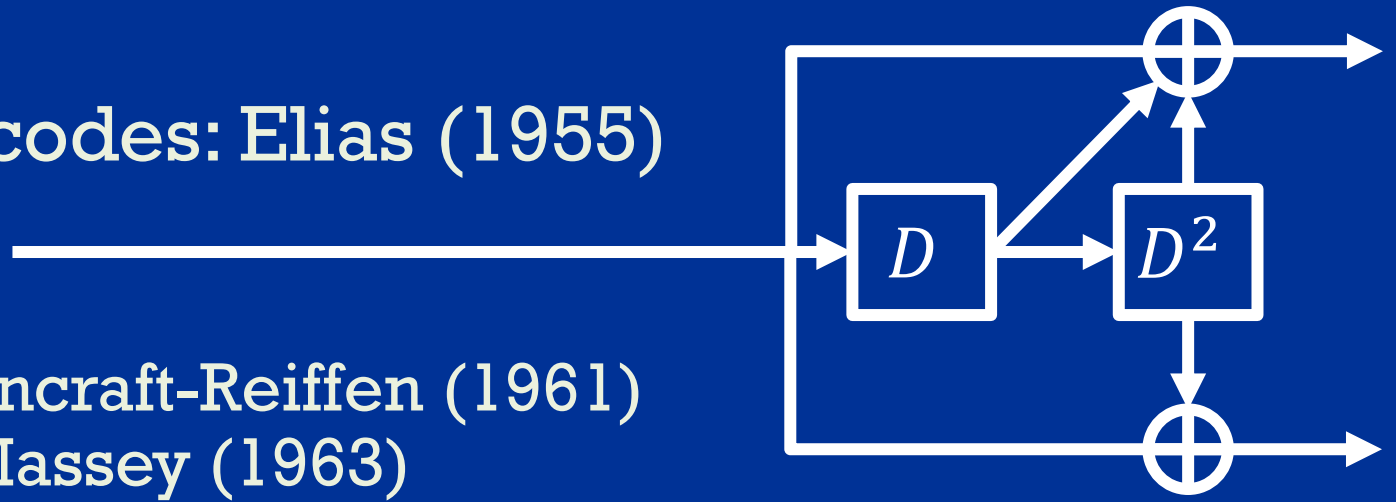
Bounds for convolutional codes

Ángela Barbero and Øyvind Ytrehus

University of Valladolid and Simula UiB

Based in part on joint work with Eirik Rosnes

A brief history of convolutional codes



- Binary convolutional codes: Elias (1955)
- Defined by encoder
- Decoding;
  - Sequential dec.:Wozencraft-Reiffen (1961)
  - Majority logic dec. : Massey (1963)
  - Viterbi dec. : Viterbi (1967)
  - BCJR dec.: Bahl et. al. (1974)
- Structure
  - Forney, Massey, Piret:
  - A minimal (complexity) encoder exists for each code
- Trellis coded modulation, Turbo codes

Convolutional codes vs Block codes

- Algebraic structure: Messy vs "Nice"
- Encoding: Simpler vs Simple
- Decoding: Soft decoding vs Code-dependent algebr. decoder

- But neither comes close to Shannon's bounds!

Convolutional code parameters

- Parameters:
  - q : field size
  - k : input bits of encoder
  - n : output bits of encoder, rate $\frac{k}{n}$
  - Distance properties $distance$
    - Free distance complexity d_{free} (Viterbi decoding)
    - Column distance profile CDP = $(d_1, \dots, d_{free})$ (Sequential decoding, latency)
  - $memcompl$: Memory M (latency) or complexity ν (Viterbi decoding)
- Optimize set of parameters $(q, k, n, distance, memcompl)$

Bounds on convolutional codes

- Given 3-/4-subset of parameters $\{q, k, n, distance, memcompl\}$
  - What value of the missing parameter(s) can surely be achieved?
    - Find a code by construction or by a computer search
  - What is the best possible value of the missing parameter(s)?
    - Prove that a better value cannot exist
  - For examples,
    - Given $\{q = 2, k, n, \nu\}$,
      - what is the largest d_{free} for which a binary (k, n, d_{free}, ν) is known to exist?
      - what is the largest d_{free} for which a binary (k, n, d_{free}, ν) can possibly exist?
    - Given $\{k, n, CDP, M\}$, what is the smallest field size q such that a (q, k, n, CDP) of memory M surely exists/can possibly exist?

Bounds on convolutional codes

- Heller bound
- Singleton bound
- Sphere packing bound
  - Binary codes (Rosnes&Ytrehus, 2004)
- Bounds on nonbinary codes
  - Superregular matrices: «Lower bounds»
    - Hutchison et. al.
    - Constructions for CDP = (2,3) and CDP= (2,3,4) (B&Y)
  - Superregular matrices: «Upper bounds» (B&Y)

The Heller bound

Theorem 1 (The Heller Bound): Let $\mathcal{C}$ be an $(n, n-r)$ convolutional code defined by the canonical parity-check matrix $\boldsymbol{H}(D)$ with row degrees ν_i, $1 \leq i \leq r$. Let ε_j, $1 \leq j \leq n$, be defined by the equation at the bottom of the page. Then if the code has free distance d_{free}, we get (5) at the top of the following page, where $d_{\max}(N, K)$ is the largest minimum Hamming distance of any linear block code of length N and dimension K.

$$\varepsilon_j = \max\left\{e : h^{(i)}_{j,\nu_i - l} = 0 \text{ for all } i \text{ and } l, 1 \leq i \leq r \text{ and } 0 \leq l < e, \text{ and } e \geq 0\right\}.$$

A. Heller, "Sequential decoding: Short constraint length convolutional codes," *Space Programs Summary*. Pasadena, CA, USA: JPL, 1968.

UVa

Bounds on convolutional codes

- Sphere packing bound: Binary codes (Rosnes&Y., 2004)

TABLE I
BOUNDS ON $N(1, \gamma_\nu, 5)$ FOR $5 \leq \nu \leq 12$

ν	Exhaustive search/Best known	SP-II	Heller	SP General
5	4	4	5	5
6	6	6	7	7
7	8	9	11	11
8	≥ 10	13	18	15
9	≥ 13	18	29	22
10	≥ 16	26	42	31
11	≥ 20	36	60	45
12	≥ 24	52	84	63

E. Rosnes and Ø. Ytrehus, "Sphere-packing bounds for convolutional codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2801–2809, Nov. 2004.

Nonbinary convolutional codes

- J. Justesen and L. Hughes, "On maximum-distance-separable convolutional codes, IEEE T-IT., 1974
- E. M. Gabidulin, "Convolutional codes over large alphabets," in *Proc. ACCT*, Varna 1988
- H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, *Strongly-MDS convolutional codes*, IEEE T-IT., 2006
- P. Almeida, D. Napp, and R. Pinto, "Superregular matrices and applications to convolutional codes," *Linear Algebra Appl.*, 2016
- D. Napp and R. Smarandache, "Constructing strongly MDS convolutional codes with maximum distance profile," *Adv. Math. Commun.*, 2016.
- B&Y, *Rate (n−1)/n Systematic Memory Maximum Distance Separable Convolutional Codes*, IEEE T-IT., 2018

Bounds on convolutional codes

- Singleton bound
- Minimum distance $\leq$ #Parity check symbols + 1
- Equality: Maximum distance separable (MDS) code
- Rate $(n-1)/n$ codes: CDP of a MDS code is $(2,3,\ldots, d_{free})$

Rate k/(k+1) Syst. m-MDS CCs

- A «superregular» matrix

$$\begin{pmatrix}
r_{0,1} & \cdots & r_{0,k} & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
r_{1,1} & \cdots & r_{1,k} & r_{0,1} & \cdots & r_{0,k} & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
r_{2,1} & \cdots & r_{2,k} & r_{1,1} & \cdots & r_{1,k} & r_{0,1} & \cdots & r_{0,k} & \cdots & 0 & \cdots & 0 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \ddots & \vdots \\
r_{D-1,1} & \cdots & r_{D-1,k} & r_{D-2,1} & \cdots & r_{D-2,k} & r_{D-3,1} & \cdots & r_{D-3,k} & \cdots & 0 & \cdots & 0 \\
r_{D,1} & \cdots & r_{D,k} & r_{D-1,1} & \cdots & r_{D-1,k} & r_{D-2,1} & \cdots & r_{D-2,k} & \cdots & r_{0,1} & \cdots & r_{0,k}
\end{pmatrix}$$

with all «nontrivial» $(i+1) \times (i+1)$ minors nonzero, $i \leq D$:

- The corresponding code has CDP $2,3,\ldots,D+2$.

Bounds on convolutional codes

– Superregular matrices: Gilbert-Varshamov-type bound

– Theorem: a $(q, 1,2, CDP = 2,3, \dots, D + 2)$ of memory D exists if

$$q > \frac{1}{2}\left(\frac{1}{D+1}\binom{2D}{D} + \binom{D}{\lfloor D/2 \rfloor}\right)$$

– Tight only for very low values of D

R. Hutchinson, R. Smarandache, and J. Trumpf, "On superregular matrices and MDP convolutional codes," *Linear Algebra Appl.*, vol. 428,nos. 11–12, pp. 2585–2596, 2008.

UVa

Rate k/(k+1) Syst. m-MDS CCs

- $GF(2^m), k = n - 1,$ cdp = 2,3,4.
- Code rate $\frac{2^{m-1}-1}{2^{m-1}}$

$$Tr^m(): \quad \mathbb{F} \rightarrow GF(2)$$
$$x \rightarrow Tr^m(x) = \sum_{i=0}^{m-1} x^{2^i}.$$

Consider the set

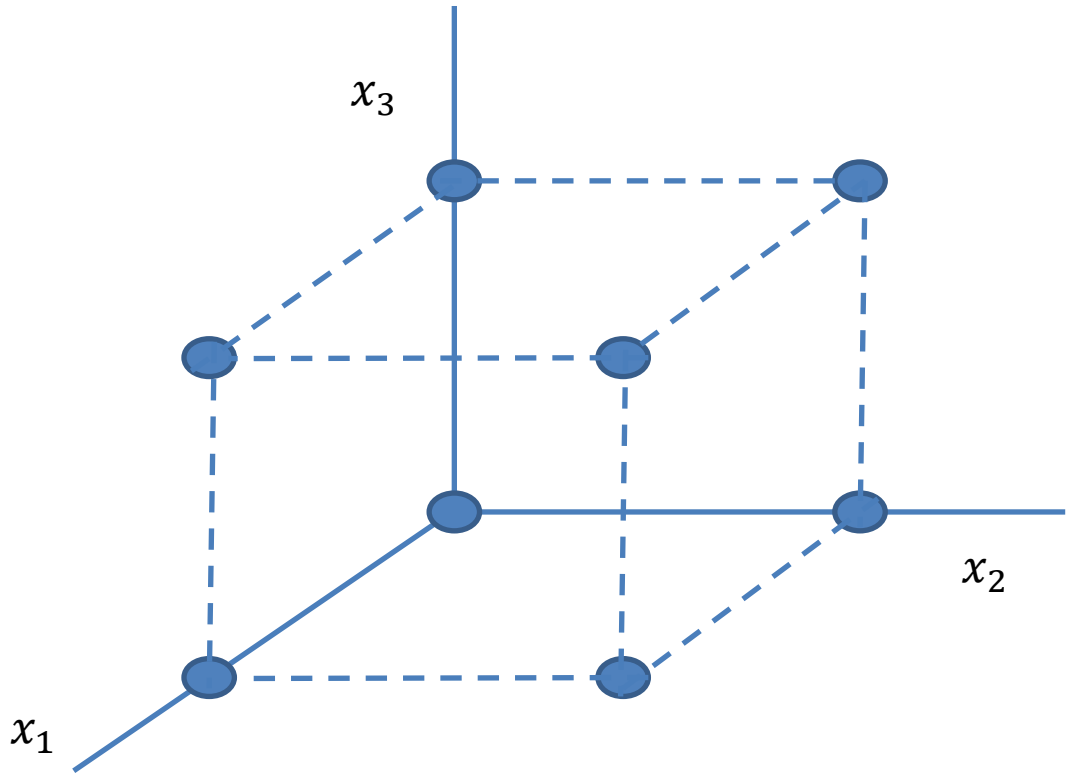
$$H_\beta = \{x \in \mathbb{F} | Tr^m(\beta x) = 0\}.$$

When $\mathbb{F}$ is regarded as an m-dimensional vector space over $GF(2)$, the set H_β is a hyperplane (an $(m-1)$-dimensional linear subspace) of $\mathbb{F}$. 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 $a_1, \ldots, a_k := r_{1,1}, \ldots, r_{1,k}$ 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 $s = 1, \ldots, k$.

B&Y, *Rate (n−1)/n Systematic Memory Maximum Distance Separable Convolutional Codes*, IEEE T-IT., 2018

Code construction

$m = 3$



$GF(2^3) = F_2(\alpha)$

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

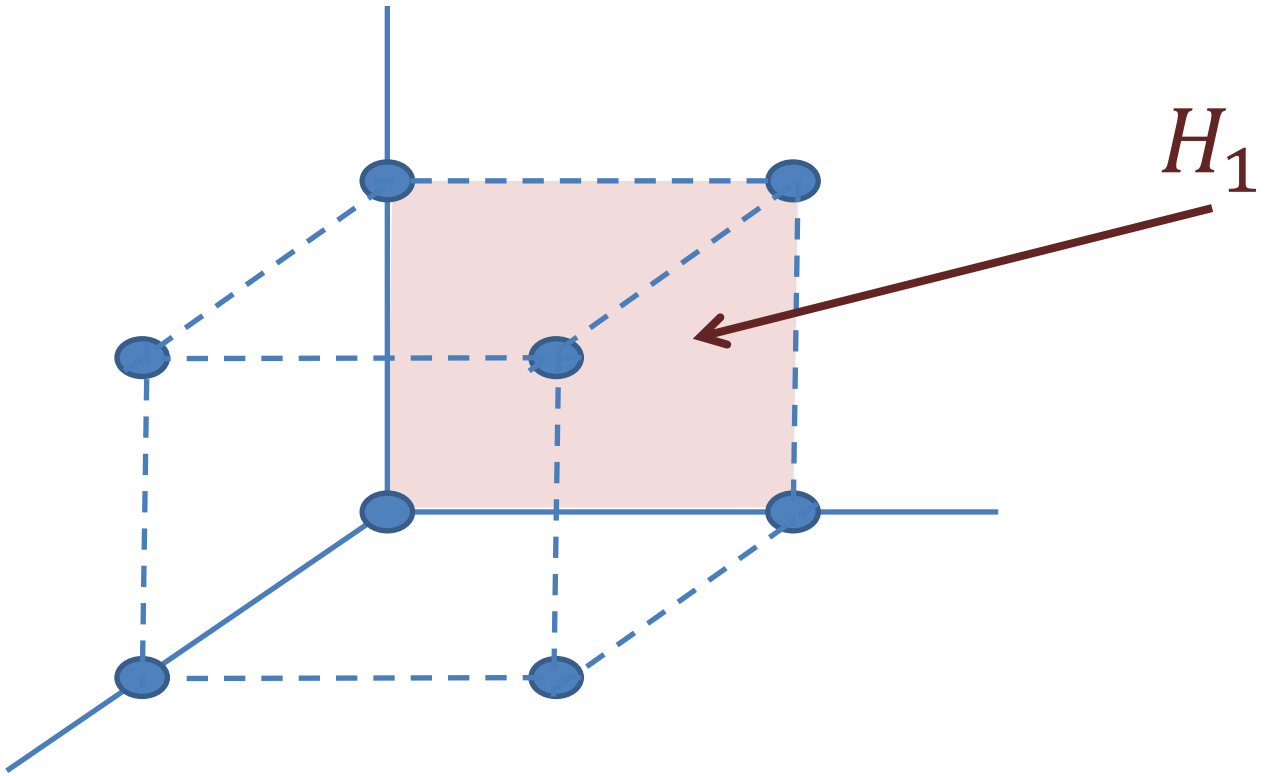
$x = x_1 + x_2\alpha + x_3\alpha^2$

$x_1, x_2, x_3 \epsilon F_2$

Code construction

Tr^3: $GF(2^3) \rightarrow F_2$

$x \rightarrow Tr^3(x) = x^{2^0} + x^{2^1} + x^{2^2}$

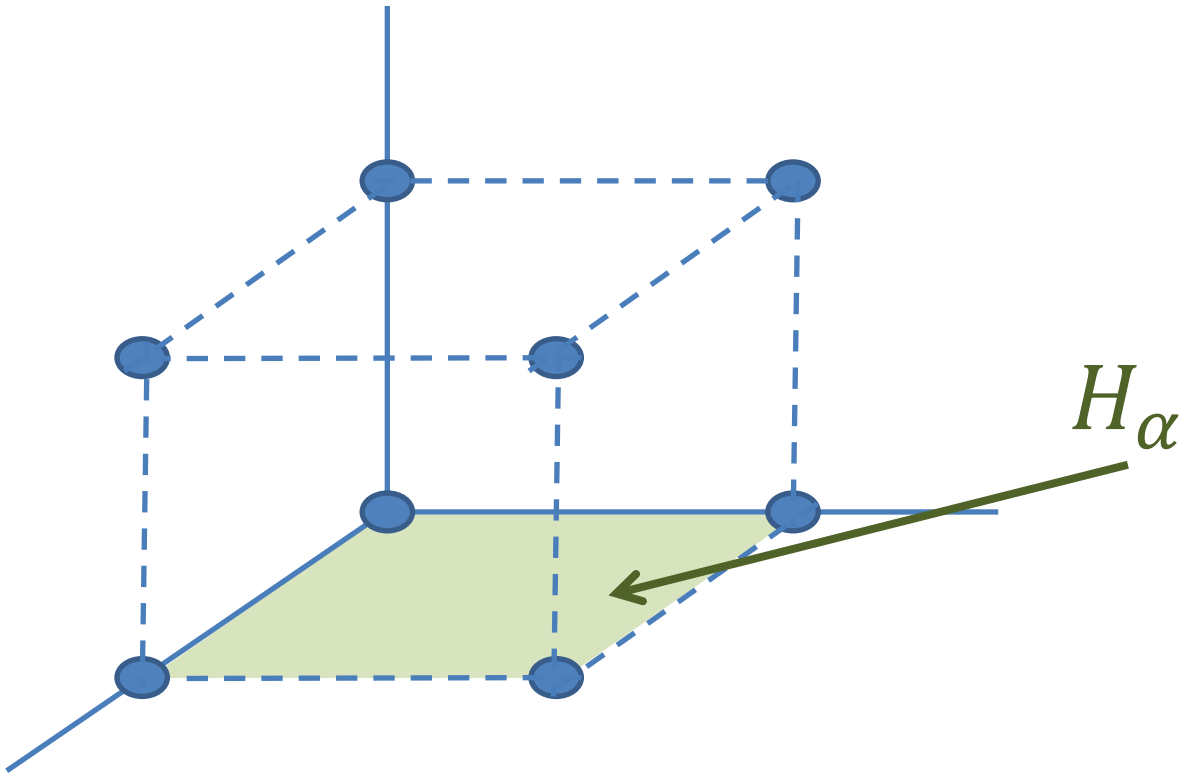


$H_\beta = \{x \epsilon GF(2^3) \mid Tr^3(\beta x) = 0\}$

Code construction

Tr^3: $GF(2^3) \rightarrow F_2$

$x \rightarrow Tr^3(x) = x^{2^0} + x^{2^1} + x^{2^2}$

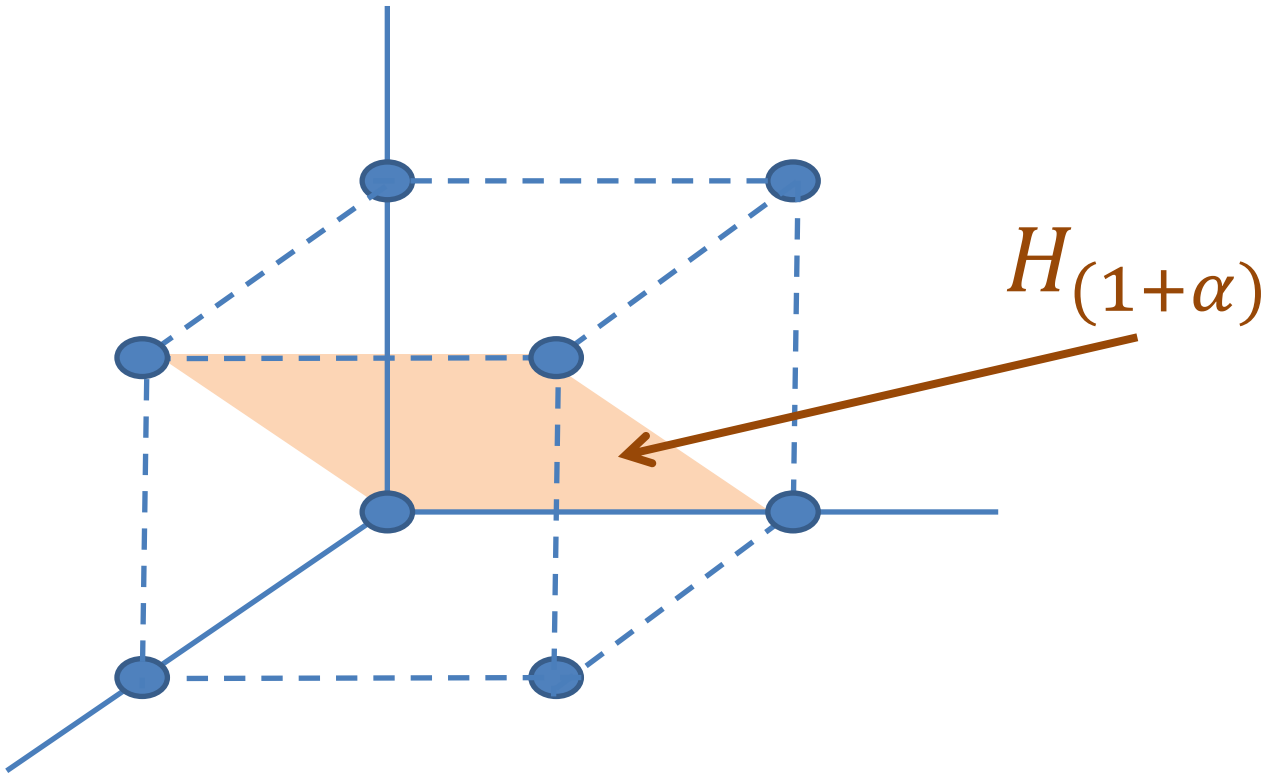


$H_\beta = \{x \epsilon GF(2^3) \mid Tr^3(\beta x) = 0\}$

Code construction

Tr^3: $GF(2^3) \rightarrow F_2$

$x \rightarrow Tr^3(x) = x^{2^0} + x^{2^1} + x^{2^2}$

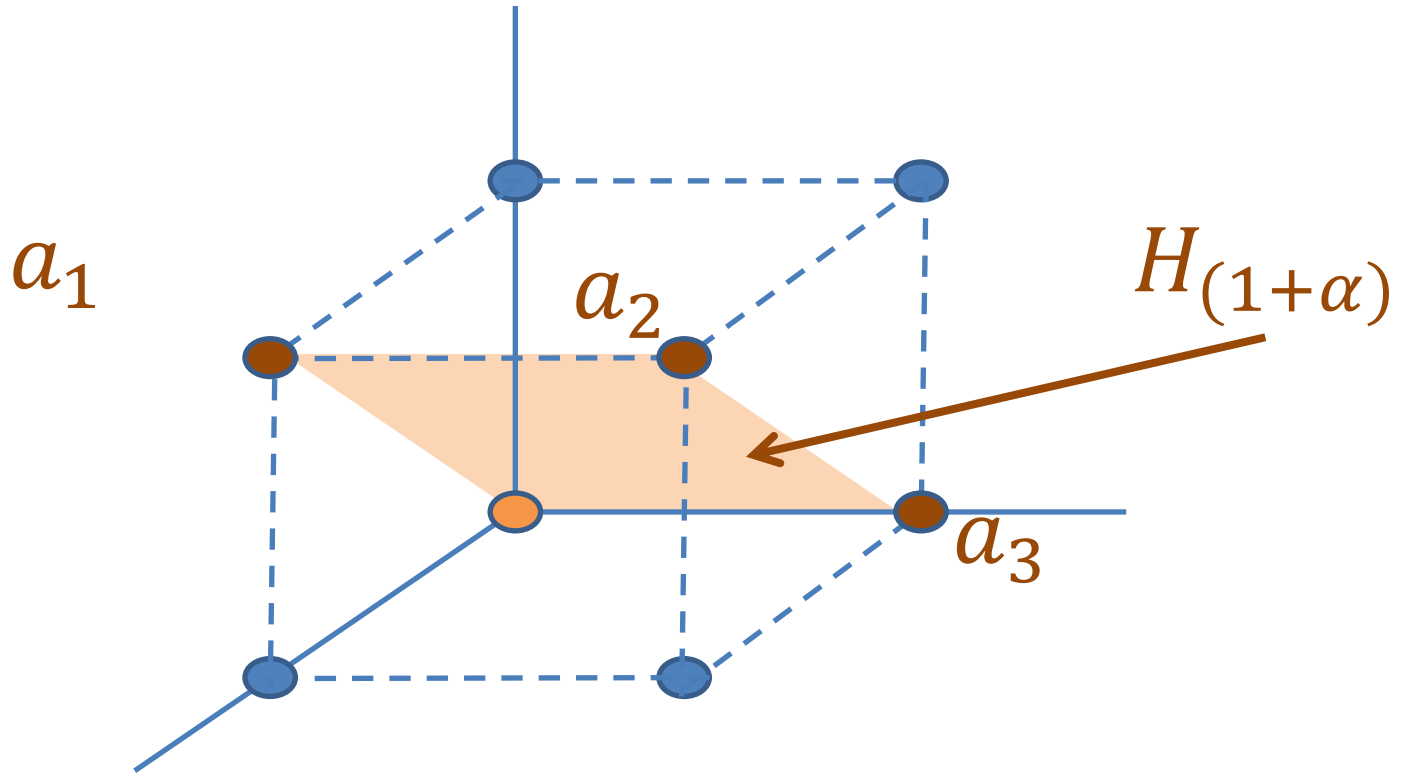


$H_\beta = \{x \epsilon GF(2^3) \mid Tr^3(\beta x) = 0\}$

Code construction

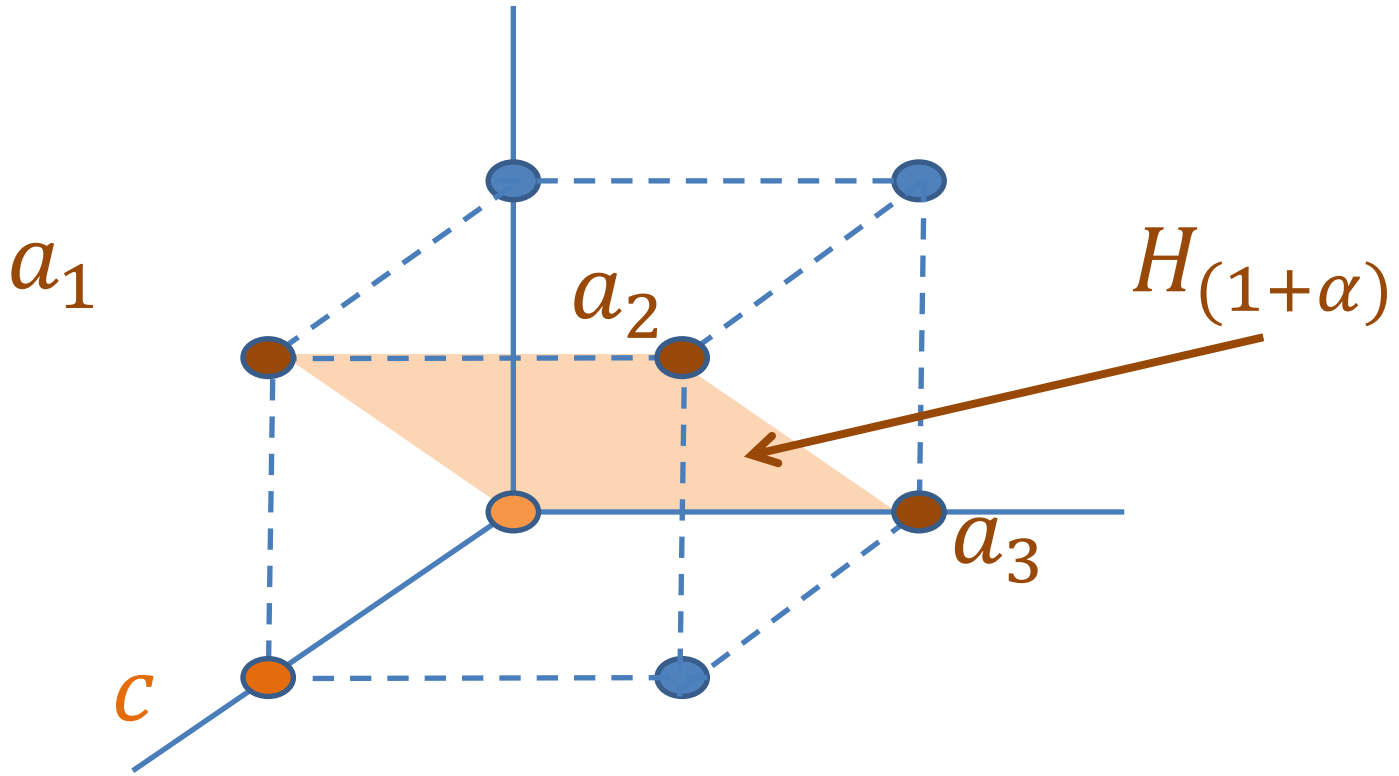
$k = 2^{m-1} - 1,$

$a_1, \ldots, a_k$ all the nonzero elements in H_β



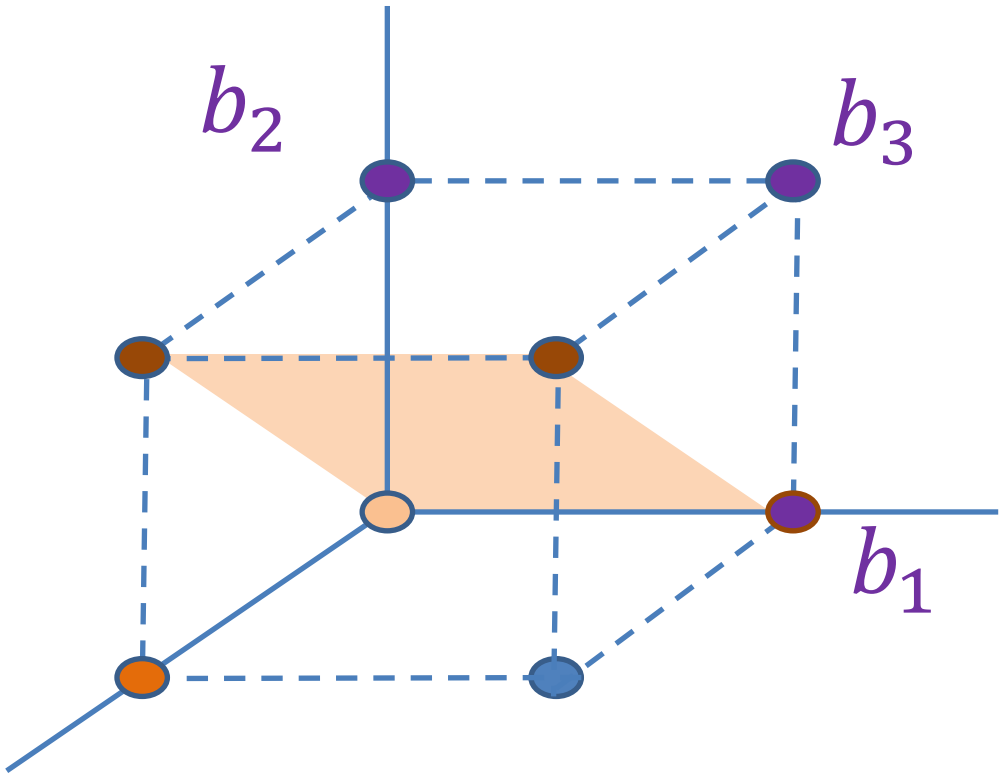
Code construction

Select any constant $c \notin H_\beta$



Code construction

$b_s = a_s(a_s + c)$, *s=1,…,k*



Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

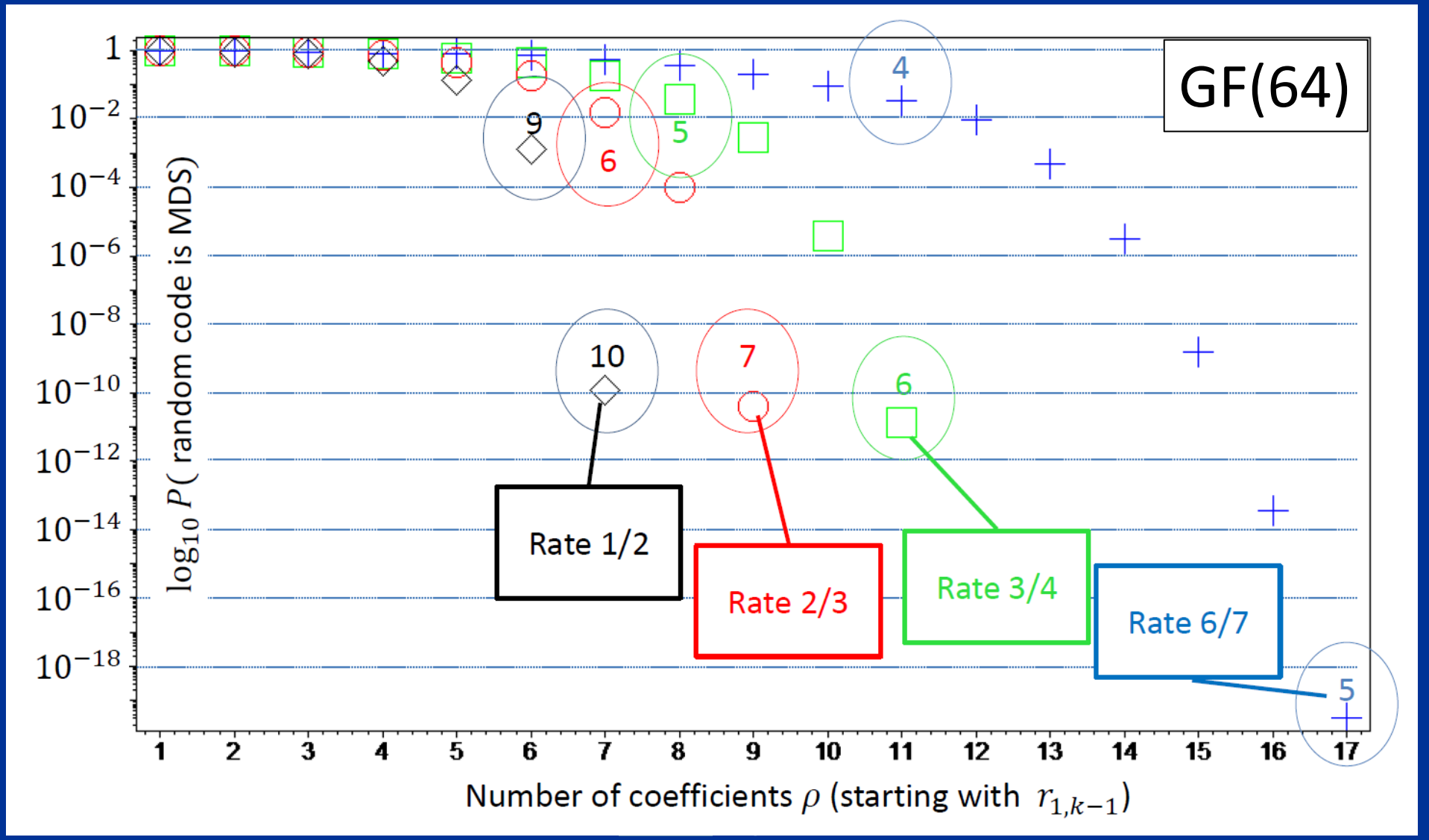
$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Code construction

$$H^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 & & & & \\ b_1 & b_2 & b_3 & 0 & a_1 & a_2 & a_3 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H'^{(2)} = \begin{pmatrix} 1 & 1 & 1 & & & & & & \\ a_1 & a_2 & a_3 & 1 & 1 & 1 & & & \\ b_1 & b_2 & b_3 & a_1 & a_2 & a_3 & 1 & 1 & 1 \end{pmatrix}$$

Rate k/(k+1) Syst. m-MDS CCs



Bounds on convolutional codes

– Superregular matrices: B&Y 2018, «Upper bounds»

Theorem 23: For rate $(n-1)/n$ *codes over* $GF(q)$ *with* $CDP = [2, 3, \ldots, \mathcal{D} = D+2]$, $n-1 \leq (q-1)/(\mathcal{D}-2)$.

Proof: Recall that all the $r_{i,j}$ coefficients are nonzero.

For $\mathcal{D} = 3$, since this requires

$$\begin{vmatrix} 1 & 1 \\ r_{1,s} & r_{1,t} \end{vmatrix} \neq 0, \quad \text{for } s \neq t \tag{11}$$

it is clear that we need at least $k = n-1$ different nonzero elements in the field.

For $\mathcal{D} = 4$. Consider the 2×2 minors of type

$$\begin{vmatrix} 1 & 1 \\ r_{1,s} & r_{1,t} \end{vmatrix} = r_{1,s} - r_{1,t}, \quad \begin{vmatrix} r_{1,s} & r_{1,t} \\ r_{2,s} & r_{2,t} \end{vmatrix} = r_{1,s}r_{2,t} - r_{1,t}r_{2,s},$$

and

$$\begin{vmatrix} r_{1,s} & 1 \\ r_{2,s} & r_{1,t} \end{vmatrix} = r_{2,s} - r_{1,s}r_{1,t}. \tag{12}$$

From the conditions on the 2×2 proper minors, since all those minors have to be nonzero, it follows that in order to have $\mathcal{D} > 3$, the values in the sets $\{r_{1,1}, \ldots, r_{1,k}\}$ and $\{r_{2,1}/r_{1,1}, \ldots, r_{2,k}/r_{1,k}\}$ must be $2k$ distinct values in $GF(q) \setminus \{0\}$.

Now consider a code with $\mathcal{D} > 4$. Then, in addition to the conditions above, we have the following extra conditions derived from 2×2 minors:

$$\begin{vmatrix} r_{2,s} & r_{2,t} \\ r_{3,s} & r_{3,t} \end{vmatrix} = r_{2,s}r_{3,t} - r_{2,t}r_{3,s}, \quad \begin{vmatrix} r_{2,s} & 1 \\ r_{3,s} & r_{1,t} \end{vmatrix} = r_{2,s}r_{1,t} - r_{3,s},$$

and

$$\begin{vmatrix} r_{2,s} & r_{1,t} \\ r_{3,s} & r_{2,t} \end{vmatrix} = r_{2,s}r_{2,t} - r_{1,t}r_{3,s}. \tag{13}$$

Again they all have to be nonzero, and this implies that the set $\{r_{3,1}/r_{2,1}, \ldots, r_{3,k}/r_{2,k}\}$ is a new set of k different values, and they are all different from the values in the sets $\{r_{1,1}, \ldots, r_{1,k}\}$ and $\{r_{2,1}/r_{1,1}, \ldots, r_{2,k}/r_{1,k}\}$. So in order to have $\mathcal{D} \geq 5$ we need to have at least $3k$ different non zero elements in the field.

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

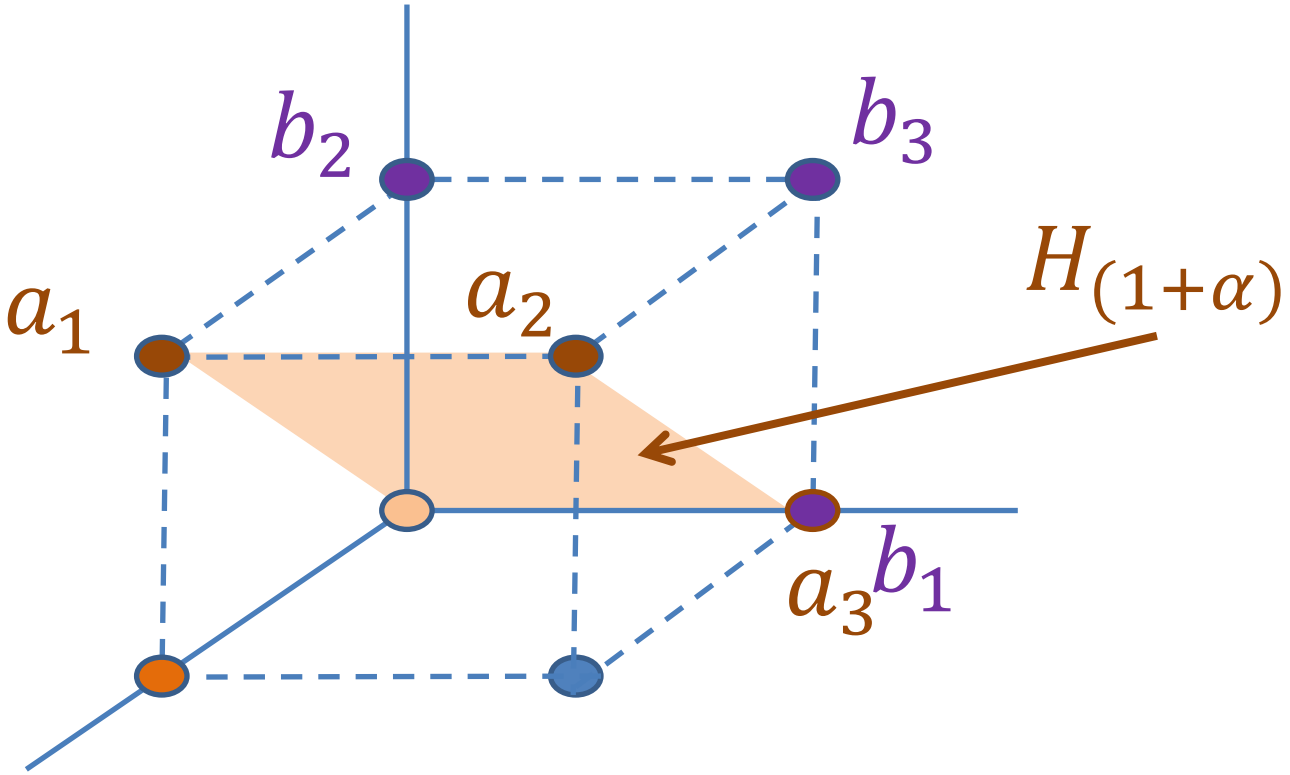
In previous episodes…

$H_\beta = \{x \epsilon GF(2^3) \mid Tr^3(\beta x) = 0\}$

$k = 2^{m-1} - 1,$

$a_1, \ldots, a_k$ all the nonzero elements in H_β

$b_s = a_s(a_s + c)$, *s=1,…,k*



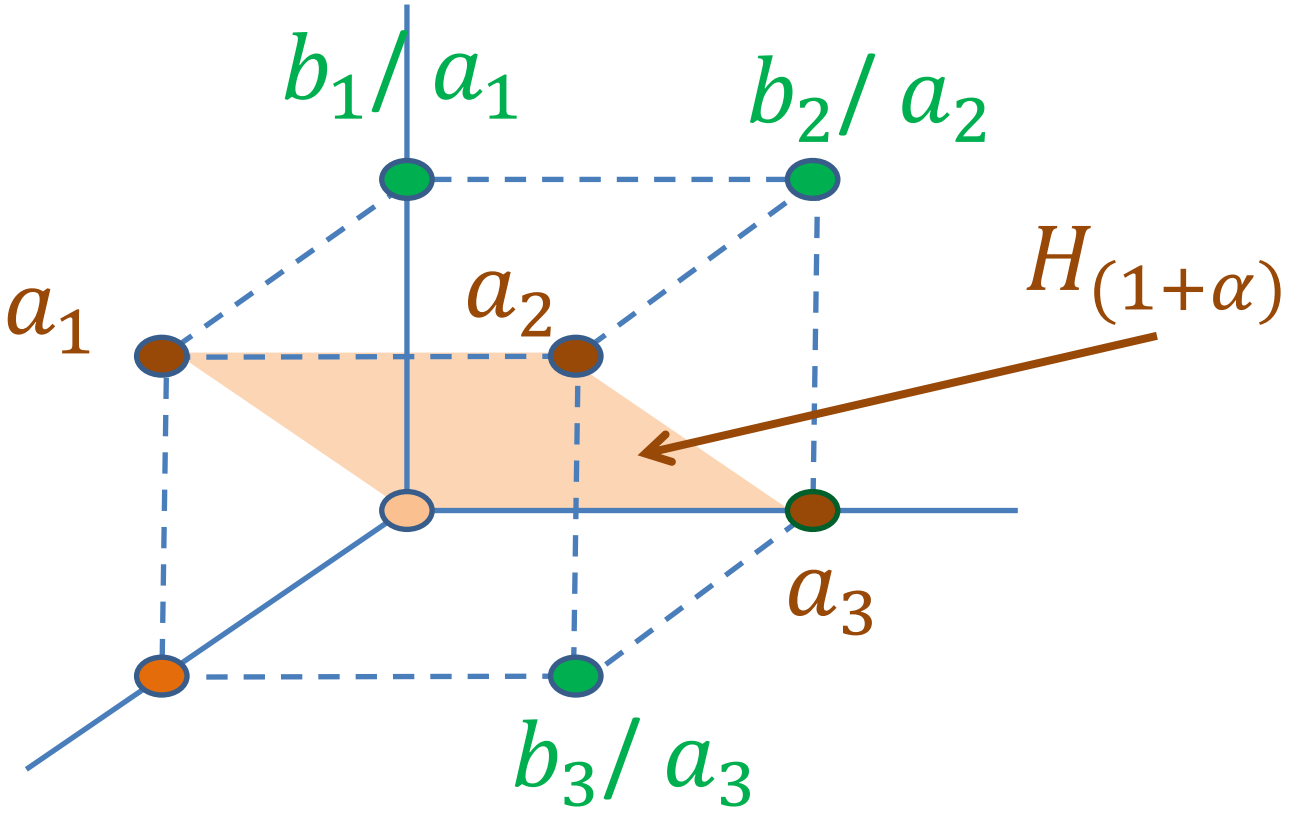
In previous episodes…

$H_\beta = \{x \epsilon GF(2^3) \mid Tr^3(\beta x) = 0\}$

$k = 2^{m-1} - 1,$

$a_1, \ldots, a_k$ all the nonzero elements in H_β

$b_s = a_s(a_s + c)$, *s=1,…,k*



Thank you! Questions, remarks?

Welcome to the

6th International Castle Meeting

on Coding Theory and its Applications

Schloss Reisenburg, Germany (near Ulm)

End of August 2020