Partial permutation decoding for $\mathbb{Z}_{2^k}$-linear Hadamard codes

Roland D. Barrolleta and **Mercè Villanueva**

Departament d'Enginyeria de la Informació i de les Comunicacions
Universitat Autònoma de Barcelona, Spain

Universitat Autònoma de Barcelona

5th Workshop on Real and Complex Hadamard Matrices and Applications

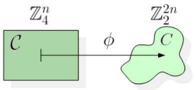
July 10-14, 2017

1. Introduction
2. PD-sets for binary linear Hadamard codes
3. PD-sets for $\mathbb{Z}_4$-linear Hadamard codes
4. PD-sets for $\mathbb{Z}_{2^k}$-linear Hadamard codes
5. Conclusions and further reseach

- A **binary code** C of length n is a subset of $\mathbb{Z}_2^n$.
- A **binary linear code** C of length n is a subgroup of $\mathbb{Z}_2^n$.
- A **quaternary linear code** $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is a subgroup of $\mathbb{Z}_4^n$ isomorphic to $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$.
- Let $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ be the usual **Gray map** defined as

$$\phi(x_1, \ldots, x_n) \to (\varphi(x_1), \ldots, \varphi(x_n)),$$

  where $\varphi(0) = (0,0), \varphi(1) = (0,1), \varphi(2) = (1,1)$ and $\varphi(3) = (1,0)$.
- If $\mathcal{C}$ is a quaternary linear code of length n and type $2^\gamma 4^\delta$, then the binary code $C = \phi(\mathcal{C})$ is a $\mathbb{Z}_4$**-linear code** of length $2n$ and type $2^\gamma 4^\delta$.

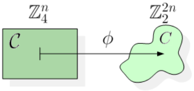


  - Examples: Kerdock, Preparata, extended perfect, **Hadamard**, Reed-Muller, extended dualized Kerdock codes...

- A **binary code** C of length n is a subset of $\mathbb{Z}_2^n$.
- A **binary linear code** C of length n is a subgroup of $\mathbb{Z}_2^n$.
- A **quaternary linear code** $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is a subgroup of $\mathbb{Z}_4^n$ isomorphic to $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$.
- Let $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ be the usual **Gray map** defined as

$$\phi(x_1, \dots, x_n) \to (\varphi(x_1), \dots, \varphi(x_n)),$$

  where $\varphi(0) = (0,0), \varphi(1) = (0,1), \varphi(2) = (1,1)$ and $\varphi(3) = (1,0)$.
- If $\mathcal{C}$ is a quaternary linear code of length n and type $2^\gamma 4^\delta$, then the binary code $C = \phi(\mathcal{C})$ is a $\mathbb{Z}_4$**-linear code** of length $2n$ and type $2^\gamma 4^\delta$.



  - Examples: Kerdock, Preparata, extended perfect, **Hadamard**, Reed-Muller, extended dualized Kerdock codes...

Let C be a binary code of length n.

- The ***permutation automorphism group*** of C is

$$\mathrm{PAut}(C) = \{\sigma \in \mathrm{Sym}(n) : \sigma(C) = C\}.$$

- A set $I \subseteq \{1, \ldots, n\}$ of k coordinates is an ***information set*** for C if $|C_I| = |C| = 2^k$, where $C_I = \{v_I : v \in C\}$ and v_I is the restriction of v to the coordinates in I. If such a set I exists, C is a ***systematic code***.
  - ▷ $\mathbb{Z}_4$-linear codes are systematic.

J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes and Cryptogr.*, **76**(2): 269–279, 2015.

- Let C be a systematic t-error correcting code with information set I. A subset $S \subseteq \mathrm{PAut}(C)$ is an **s-PD-*set*** for C if every s-set J of coordinate positions is moved out of I by at least one element of S, $1 \le s \le t$.
  If $s = t$, S is a **PD-*set***. $\Rightarrow \sigma(J) \cap I = \emptyset$ for at least one $\sigma \in S$.

Let C be a binary code of length n.

- The ***permutation automorphism group*** of C is

$$\mathrm{PAut}(C) = \{\sigma \in \mathrm{Sym}(n) : \sigma(C) = C\}.$$

- A set $I \subseteq \{1, \dots, n\}$ of k coordinates is an ***information set*** for C if $|C_I| = |C| = 2^k$, where $C_I = \{v_I : v \in C\}$ and v_I is the restriction of v to the coordinates in I. If such a set I exists, C is a ***systematic code***.
  - ▷ $\mathbb{Z}_4$-linear codes are systematic.

J. J. BERNAL, J. BORGES, C. FERNÁNDEZ-CÓRBODA, AND M. VILLANUEVA, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes and Cryptogr.*, **76**(2): 269–279, 2015.

- Let C be a systematic t-error correcting code with information set I. A subset $S \subseteq \mathrm{PAut}(C)$ is an **s-PD-*set*** for C if every s-set J of coordinate positions is moved out of I by at least one element of S, $1 \leq s \leq t$. If $s = t$, S is a **PD-*set***. $\Rightarrow \sigma(J) \cap I = \emptyset$ for at least one $\sigma \in S$.

Let C be a binary code of length n.

- The ***permutation automorphism group*** of C is

$$\mathrm{PAut}(C) = \{\sigma \in \mathrm{Sym}(n) : \sigma(C) = C\}.$$

- A set $I \subseteq \{1, \dots, n\}$ of k coordinates is an ***information set*** for C if $|C_I| = |C| = 2^k$, where $C_I = \{v_I : v \in C\}$ and v_I is the restriction of v to the coordinates in I. If such a set I exists, C is a ***systematic code***.
  - ▷ $\mathbb{Z}_4$-linear codes are systematic.

J. J. BERNAL, J. BORGES, C. FERNÁNDEZ-CÓRBODA, AND M. VILLANUEVA, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes and Cryptogr.*, **76**(2): 269–279, 2015.

- Let C be a systematic t-error correcting code with information set I. A subset $S \subseteq \mathrm{PAut}(C)$ is an **s-PD-*set*** for C if every s-set J of coordinate positions is moved out of I by at least one element of S, $1 \leq s \leq t$.
  If $s = t$, S is a **PD-*set***. $\Rightarrow \sigma(J) \cap I = \emptyset$ for at least one $\sigma \in S$.

Permutation Decoding

Move errors in the received vector $y = x + e$ out of I by using $\sigma \in S \subseteq \mathrm{PAut}(C)$ in such a way that $\sigma(y)_I = x_I$, where $x \in C$ and $\mathrm{wt}(e) \leq s$.

- Permutation decoding for **linear codes** was first defined by Prange (1962) and developed by MacWilliams (1964).
  - PD-sets for some families of linear codes are known.
- An alternative permutation decoding for $\mathbb{Z}_4$-linear codes (and **systematic nonlinear codes**) was presented in 2015.

  Let f be a systematic encoding. Then $y_I = x_I \iff \mathrm{wt}(y + f(y_I)) \leq s$.

J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes and Cryptogr.*, **76**(2), 269–279, 2015.

  - Find s-PD-sets (of small size) for families of $\mathbb{Z}_{2^k}$-linear codes!!

Permutation Decoding

Move errors in the received vector $y = x + e$ out of I by using $\sigma \in S \subseteq \mathrm{PAut}(C)$ in such a way that $\sigma(y)_I = x_I$, where $x \in C$ and $\mathrm{wt}(e) \leq s$.

- Permutation decoding for **linear codes** was first defined by Prange (1962) and developed by MacWilliams (1964).
  - ▷ PD-sets for some families of linear codes are known.
- An alternative permutation decoding for $\mathbb{Z}_4$-linear codes (and **systematic nonlinear codes**) was presented in 2015.

  Let f be a systematic encoding. Then $y_I = x_I \;\Leftrightarrow \mathrm{wt}(y + f(y_I)) \leq s$.

J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva,
"Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes,"
Des. Codes and Cryptogr., **76**(2), 269–279, 2015.

  - ▷ Find s-PD-sets (of small size) for families of $\mathbb{Z}_{2^k}$-linear codes!!

A **binary Hadamard code** of length n is a binary code with $2n$ codewords and minimum Hamming distance $n/2$.

Let H_m be the binary linear Hadamard code of length $n = 2^m$ generated by

$$G_m = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & G' \end{pmatrix},$$

where G' has the $2^m - 1$ nonzero vectors from $\mathbb{Z}_2^m$ as columns with the vectors e_i in the first m positions. H_m is the first order Reed–Muller code.

Note that $I_m = \{1, \dots, m+1\}$ is an information set for H_m.

Example

Let H_2 be the binary linear Hadamard code of length 4 generated by

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The set $I_2 = \{1, 2, 3\}$ is an information set for H_2.

A **binary Hadamard code** of length n is a binary code with $2n$ codewords and minimum Hamming distance $n/2$.

Let H_m be the binary linear Hadamard code of length $n = 2^m$ generated by

$$G_m = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & G' \end{pmatrix},$$

where G' has the $2^m - 1$ nonzero vectors from $\mathbb{Z}_2^m$ as columns with the vectors e_i in the first m positions. H_m is the first order Reed–Muller code.

Note that $I_m = \{1, \ldots, m+1\}$ is an information set for H_m.

Example

Let H_2 be the binary linear Hadamard code of length 4 generated by

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The set $I_2 = \{1, 2, 3\}$ is an information set for H_2.

A **binary Hadamard code** of length n is a binary code with $2n$ codewords and minimum Hamming distance $n/2$.

Let H_m be the binary linear Hadamard code of length $n = 2^m$ generated by

$$G_m = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & G' \end{pmatrix},$$

where G' has the $2^m - 1$ nonzero vectors from $\mathbb{Z}_2^m$ as columns with the vectors e_i in the first m positions. H_m is the first order Reed–Muller code.

Note that $I_m = \{1, \dots, m+1\}$ is an information set for H_m.

Example

Let H_2 be the binary linear Hadamard code of length 4 generated by

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The set $I_2 = \{1, 2, 3\}$ is an information set for H_2.

Proposition (Gordon-Schönheim bound)

If S is a PD-set for a systematic t-error correcting code C of length n, size $|C| = 2^k$ and $r = n - k$, then

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \dots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \dots \right\rceil \right\rceil \right\rceil.$$

D.M. GORDON,
"Minimal permutation sets for decoding the binary Golay codes,"
IEEE Trans. Inf. Theory, vol. 28(3), 541–543, 1994.

Proposition

If S is an s-PD-set for systematic binary Hadamard code of length 2^m, then

- $|S| \geq s+1$ *and*
- $f_m = \max\{s \,:\, 2 \leq s,\ |S| = s+1\} = \left\lfloor \frac{2^m}{1+m} \right\rfloor - 1.$

$$\begin{aligned}\mathrm{PAut}(H_m) &\cong \mathrm{AGL}(m,2)\\ &\cong \{A \in \mathrm{GL}(m+1,2) : \text{first column is } (1,0,\ldots,0)\}\end{aligned}$$

Let M be a binary matrix with r rows and let m_i be the ith row of M, $i \in \{1,\ldots,r\}$. We define M^* from M as follows

$$M = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} \qquad M^* = \begin{pmatrix} m_1 \\ m_1+m_2 \\ \vdots \\ m_1+m_r \end{pmatrix}.$$

Theorem

A set $P_s = \{M_i \; : \; 0 \leq i \leq s\} \subseteq \mathrm{PAut}(H_m)$ is an s-PD-set of size $s+1$ for H_m with information set I_m $\Leftrightarrow$ no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common.

$$\begin{aligned}\mathrm{PAut}(H_m) &\cong \mathrm{AGL}(m,2)\\ &\cong \{A \in \mathrm{GL}(m+1,2) : \text{first column is } (1,0,\dots,0)\}\end{aligned}$$

Let M be a binary matrix with r rows and let m_i be the ith row of M, $i \in \{1,\dots,r\}$. We define M^* from M as follows

$$M = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} \qquad M^* = \begin{pmatrix} m_1 \\ m_1+m_2 \\ \vdots \\ m_1+m_r \end{pmatrix}.$$

Theorem

A set $P_s = \{M_i \ : \ 0 \le i \le s\} \subseteq \mathrm{PAut}(H_m)$ is an s-PD-set of size $s+1$ for H_m with information set I_m $\Leftrightarrow$ no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common.

Let $\alpha \in \mathbb{Z}_2[x]/(f(x))$ be a root of a primitive polynomial $f(x)$ of degree m.

Consider the $(m+1)\times(m+1)$ binary matrices, $i \in \{1,\ldots,f_m\}$:

$$N_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & \alpha^{m-1} \end{pmatrix} \quad \text{and} \quad N_i = \begin{pmatrix} 1 & \alpha^{(m+1)i-1} \\ 0 & \alpha^{(m+1)i} - \alpha^{(m+1)i-1} \\ \vdots & \vdots \\ 0 & \alpha^{(m+1)i+m-1} - \alpha^{(m+1)i-1} \end{pmatrix}.$$

Theorem

The set $P_s = \{M_i = N_i^{-1} \;:\; 0 \le i \le s\}$ is an s-PD-set of size $s+1$ for H_m with information set I_m for all $m \ge 4$ and $2 \le s \le f_m$.

Example

Let $\alpha \in \mathbb{Z}_2[x]/(f(x))$ be a root of the primitive polynomial $f(x) = x^4 + x + 1$.

Example

Let $\alpha \in \mathbb{Z}_2[x]/(f(x))$ be a root of the primitive polynomial $f(x) = x^4 + x + 1$. The set $P_2 = \{N_0^{-1}, N_1^{-1}, N_2^{-1}\}$ is a 2-PD-set of size 3 for H_4, where N_0, N_1 and N_2 are:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & \alpha \\ 0 & \alpha^2 \\ 0 & \alpha^3 \end{pmatrix}, \begin{pmatrix} 1 & \alpha^4 \\ 0 & \alpha^5 - \alpha^4 \\ 0 & \alpha^6 - \alpha^4 \\ 0 & \alpha^7 - \alpha^4 \\ 0 & \alpha^8 - \alpha^4 \end{pmatrix}, \begin{pmatrix} 1 & \alpha^9 \\ 0 & \alpha^{10} - \alpha^9 \\ 0 & \alpha^{11} - \alpha^9 \\ 0 & \alpha^{12} - \alpha^9 \\ 0 & \alpha^{13} - \alpha^9 \end{pmatrix}$$

Example

Let $\alpha \in \mathbb{Z}_2[x]/(f(x))$ be a root of the primitive polynomial $f(x) = x^4 + x + 1$. The set $P_2 = \{N_0^{-1}, N_1^{-1}, N_2^{-1}\}$ is a 2-PD-set of size 3 for H_4, where N_0, N_1 and N_2 are:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Example

Let $\alpha \in \mathbb{Z}_2[x]/(f(x))$ be a root of the primitive polynomial $f(x) = x^4 + x + 1$. The set $P_2 = \{N_0^{-1}, N_1^{-1}, N_2^{-1}\}$ is a 2-PD-set of size 3 for H_4, where N_0, N_1 and N_2 are:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Indeed, the matrices $N_0^* = \mathrm{Id}_5^*$, N_1^* and N_2^* have no rows in common:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

A generator matrix G_{m+1} for H_{m+1} can be constructed as follows:

$$G_{m+1} = \begin{pmatrix} G_m & G_m \\ \mathbf{0} & \mathbf{1} \end{pmatrix}.$$

Given $\sigma_i \in \mathrm{Sym}(n_i)$, we define $(\sigma_1|\sigma_2) \in \mathrm{Sym}(n_1+n_2)$, where

- σ_1 acts on $\{1,\ldots,n_1\}$ and
- σ_2 acts on $\{n_1+1,\ldots,n_1+n_2\}$.

Proposition

Let S be an s-PD-set of size ℓ for H_m with information set I, $m \geq 4$. Then

$$(S|S) = \{(\sigma|\sigma) : \sigma \in S\}$$

is an s-PD-set of size ℓ for H_{m+1} with information set $I' = I \cup \{i+2^m\},\ i \in I$.

A code $\mathcal{C}$ is a **quaternary linear Hadamard code** if $C = \phi(\mathcal{C})$ is a binary Hadamard code. We say that C is a $\mathbb{Z}_4$-**linear Hadamard code**.

Any quaternary linear Hadamard code $\mathcal{H}_{\gamma,\delta}$ of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$, is generated by $\mathcal{G}_{\gamma,\delta}$ obtained by applying

$$\mathcal{G}_{\gamma+1,\delta} = \begin{pmatrix} \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} \\ \mathbf{0} & \mathbf{2} \end{pmatrix},$$

$$\mathcal{G}_{\gamma,\delta+1} = \begin{pmatrix} \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix},$$

recursively over $\mathcal{G}_{0,1} = (1)$, where $\mathbf{0}, \mathbf{1}, \mathbf{2}$ and $\mathbf{3}$ means the repetition of the symbol 0, 1, 2, 3, respectively.

The $\mathbb{Z}_4$-linear Hadamard code $H_{\gamma,\delta} = \phi(\mathcal{H}_{\gamma,\delta})$ has binary length $2\beta = 2^m$.

A code $\mathcal{C}$ is a **quaternary linear Hadamard code** if $C = \phi(\mathcal{C})$ is a binary Hadamard code. We say that C is a $\mathbb{Z}_4$-**linear Hadamard code**.

Any quaternary linear Hadamard code $\mathcal{H}_{\gamma,\delta}$ of length $\beta = 2^{m-1}$ and type $2^\gamma 4^\delta$, where $m = \gamma + 2\delta - 1$, is generated by $\mathcal{G}_{\gamma,\delta}$ obtained by applying

$$\mathcal{G}_{\gamma+1,\delta} = \begin{pmatrix} \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} \\ \mathbf{0} & \mathbf{2} \end{pmatrix},$$

$$\mathcal{G}_{\gamma,\delta+1} = \begin{pmatrix} \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} & \mathcal{G}_{\gamma,\delta} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix},$$

recursively over $\mathcal{G}_{0,1} = (1)$, where $\mathbf{0}, \mathbf{1}, \mathbf{2}$ and $\mathbf{3}$ means the repetition of the symbol 0, 1, 2, 3, respectively.

The $\mathbb{Z}_4$-linear Hadamard code $H_{\gamma,\delta} = \phi(\mathcal{H}_{\gamma,\delta})$ has binary length $2\beta = 2^m$.

Let $\mathcal{C}$ be a quaternary linear code of length β and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$.

- An ordered set $\mathcal{I} = \{i_1, \ldots, i_{\delta+\gamma}\} \subseteq \{1, \ldots, \beta\}$ of $\gamma + \delta$ coordinate positions is a **quaternary information set** for $\mathcal{C}$ if $|\mathcal{C}_\mathcal{I}| = 2^\gamma 4^\delta$.
- If $|\mathcal{C}_{\{i_1,\ldots,i_\delta\}}| = 4^\delta$, then

$$\phi(\mathcal{I}) = \{2i_1 - 1, 2i_1, \ldots, 2i_\delta - 1, 2i_\delta, 2i_{\delta+1} - 1, \ldots, 2i_{\delta+\gamma} - 1\}$$

is an information set for C.

Proposition

If $\mathcal{I}$ is a quaternary information set for $\mathcal{H}_{\gamma,\delta}$ of length β, then $\mathcal{I} \cup \{\beta + 1\}$ is a quaternary information set for $\mathcal{H}_{\gamma+1,\delta}$ and $\mathcal{H}_{\gamma,\delta+1}$.

Let $\mathcal{I}_{\gamma,\delta}$ be the quaternary information set for $\mathcal{H}_{\gamma,\delta}$ of length β obtained recursively from $\mathcal{I}_{0,1} = \{1\}$.

Let $\mathcal{C}$ be a quaternary linear code of length β and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$.

- An ordered set $\mathcal{I} = \{i_1, \ldots, i_{\delta+\gamma}\} \subseteq \{1, \ldots, \beta\}$ of $\gamma + \delta$ coordinate positions is a **quaternary information set** for $\mathcal{C}$ if $|\mathcal{C}_\mathcal{I}| = 2^\gamma 4^\delta$.
- If $|\mathcal{C}_{\{i_1,\ldots,i_\delta\}}| = 4^\delta$, then

$$\phi(\mathcal{I}) = \{2i_1 - 1, 2i_1, \ldots, 2i_\delta - 1, 2i_\delta, 2i_{\delta+1} - 1, \ldots, 2i_{\delta+\gamma} - 1\}$$

is an information set for C.

Proposition

If $\mathcal{I}$ is a quaternary information set for $\mathcal{H}_{\gamma,\delta}$ of length β, then $\mathcal{I} \cup \{\beta + 1\}$ is a quaternary information set for $\mathcal{H}_{\gamma+1,\delta}$ and $\mathcal{H}_{\gamma,\delta+1}$.

Let $\mathcal{I}_{\gamma,\delta}$ be the quaternary information set for $\mathcal{H}_{\gamma,\delta}$ of length β obtained recursively from $\mathcal{I}_{0,1} = \{1\}$.

Let $\mathcal{C}$ be a quaternary linear code of length β and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$.

- An ordered set $\mathcal{I} = \{i_1, \dots, i_{\delta+\gamma}\} \subseteq \{1, \dots, \beta\}$ of $\gamma + \delta$ coordinate positions is a **quaternary information set** for $\mathcal{C}$ if $|\mathcal{C}_\mathcal{I}| = 2^\gamma 4^\delta$.
- If $|\mathcal{C}_{\{i_1,\dots,i_\delta\}}| = 4^\delta$, then

$$\phi(\mathcal{I}) = \{2i_1 - 1, 2i_1, \dots, 2i_\delta - 1, 2i_\delta, 2i_{\delta+1} - 1, \dots, 2i_{\delta+\gamma} - 1\}$$

  is an information set for C.

Proposition

If $\mathcal{I}$ is a quaternary information set for $\mathcal{H}_{\gamma,\delta}$ of length β, then $\mathcal{I} \cup \{\beta+1\}$ is a quaternary information set for $\mathcal{H}_{\gamma+1,\delta}$ and $\mathcal{H}_{\gamma,\delta+1}$.

Let $\mathcal{I}_{\gamma,\delta}$ be the quaternary information set for $\mathcal{H}_{\gamma,\delta}$ of length β obtained recursively from $\mathcal{I}_{0,1} = \{1\}$.

Example

- The quaternary linear Hadamard code $\mathcal{H}_{0,3}$ of length 16 is generated by

$$\mathcal{G}_{0,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

- The set $\mathcal{I}_{0,3} = \{1, 2, 5\}$ is a quaternary information set for $\mathcal{H}_{0,3}$.
- Quaternary linear Hadamard codes $\mathcal{H}_{1,3}$ and $\mathcal{H}_{0,4}$ of length 32 and 64, respectively, are generated by

$$\mathcal{G}_{1,3} = \begin{pmatrix} \mathcal{G}_{0,3} & \mathcal{G}_{0,3} \\ \mathbf{0} & \mathbf{2} \end{pmatrix},$$

$$\mathcal{G}_{0,4} = \begin{pmatrix} \mathcal{G}_{0,3} & \mathcal{G}_{0,3} & \mathcal{G}_{0,3} & \mathcal{G}_{0,3} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}.$$

- $\mathcal{I}_{0,3} \cup \{17\} = \{1, 2, 5, 17\}$ is a quaternary information set for $\mathcal{H}_{1,3}$, $\mathcal{H}_{0,4}$.

Example

- The quaternary linear Hadamard code $\mathcal{H}_{0,3}$ of length 16 is generated by

$$\mathcal{G}_{0,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

- The set $\mathcal{I}_{0,3} = \{1, 2, 5\}$ is a quaternary information set for $\mathcal{H}_{0,3}$.
- Quaternary linear Hadamard codes $\mathcal{H}_{1,3}$ and $\mathcal{H}_{0,4}$ of length 32 and 64, respectively, are generated by

$$\mathcal{G}_{1,3} = \begin{pmatrix} \mathcal{G}_{0,3} & \mathcal{G}_{0,3} \\ \mathbf{0} & \mathbf{2} \end{pmatrix},$$

$$\mathcal{G}_{0,4} = \begin{pmatrix} \mathcal{G}_{0,3} & \mathcal{G}_{0,3} & \mathcal{G}_{0,3} & \mathcal{G}_{0,3} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}.$$

- $\mathcal{I}_{0,3} \cup \{17\} = \{1, 2, 5, 17\}$ is a quaternary information set for $\mathcal{H}_{1,3}$, $\mathcal{H}_{0,4}$.

$$\mathrm{PAut}(\mathcal{H}_{0,\delta}) \cong \{\begin{pmatrix} 1 & \eta \\ \mathbf{0} & A \end{pmatrix} : A \in \mathrm{GL}(\delta-1,\mathbb{Z}_4), \eta \in \mathbb{Z}_4^{\delta-1}\} \subseteq \mathrm{GL}(\delta,\mathbb{Z}_4)$$

- Let $\phi : \mathrm{Sym}(\beta) \to \mathrm{Sym}(2\beta)$ be the map defined as

$$\phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau(\frac{i+1}{2}) - 1 & \text{if } i \text{ is odd,} \end{cases}$$

  for all $\tau \in \mathrm{Sym}(\beta)$ and $i \in \{1,\ldots,2\beta\}$.

  - Example: If $(1,2,3) \in \mathrm{Sym}(4)$, then $\phi((1,2,3)) = (1,3,5)(2,4,6) \in \mathrm{Sym}(8)$.

- Define $\phi(\mathcal{M}) = \phi(\tau) \in \mathrm{Sym}(2\beta)$ for any $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ and consider $\phi(\mathcal{P}) = \{\phi(\mathcal{M}) : \mathcal{M} \in \mathcal{P}\} \subseteq \mathrm{Sym}(2\beta)$ for any $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$.

$$\mathrm{PAut}(\mathcal{H}_{0,\delta}) \cong \{\begin{pmatrix} 1 & \eta \\ \mathbf{0} & A \end{pmatrix} : A \in \mathrm{GL}(\delta-1,\mathbb{Z}_4), \eta \in \mathbb{Z}_4^{\delta-1}\} \subseteq \mathrm{GL}(\delta,\mathbb{Z}_4)$$

- Let $\phi : \mathrm{Sym}(\beta) \to \mathrm{Sym}(2\beta)$ be the map defined as

$$\phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau(\frac{i+1}{2}) - 1 & \text{if } i \text{ is odd,} \end{cases}$$

  for all $\tau \in \mathrm{Sym}(\beta)$ and $i \in \{1,\dots,2\beta\}$.

  - Example: If $(1,2,3) \in \mathrm{Sym}(4)$, then $\phi((1,2,3)) = (1,3,5)(2,4,6) \in \mathrm{Sym}(8)$.

- Define $\phi(\mathcal{M}) = \phi(\tau) \in \mathrm{Sym}(2\beta)$ for any $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ and consider $\phi(\mathcal{P}) = \{\phi(\mathcal{M}) : \mathcal{M} \in \mathcal{P}\} \subseteq \mathrm{Sym}(2\beta)$ for any $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$.

$$\mathrm{PAut}(\mathcal{H}_{0,\delta}) \cong \{\begin{pmatrix} 1 & \eta \\ \mathbf{0} & A \end{pmatrix} : A \in \mathrm{GL}(\delta-1,\mathbb{Z}_4), \eta \in \mathbb{Z}_4^{\delta-1}\} \subseteq \mathrm{GL}(\delta,\mathbb{Z}_4)$$

- Let $\phi : \mathrm{Sym}(\beta) \to \mathrm{Sym}(2\beta)$ be the map defined as

$$\phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau(\frac{i+1}{2}) - 1 & \text{if } i \text{ is odd,} \end{cases}$$

  for all $\tau \in \mathrm{Sym}(\beta)$ and $i \in \{1,\dots,2\beta\}$.

  - Example: If $(1,2,3) \in \mathrm{Sym}(4)$, then $\phi((1,2,3)) = (1,3,5)(2,4,6) \in \mathrm{Sym}(8)$.

- Define $\phi(\mathcal{M}) = \phi(\tau) \in \mathrm{Sym}(2\beta)$ for any $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ and consider $\phi(\mathcal{P}) = \{\phi(\mathcal{M}) : \mathcal{M} \in \mathcal{P}\} \subseteq \mathrm{Sym}(2\beta)$ for any $\mathcal{P} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$.

Let $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ and let m_i be the ith row of $\mathcal{M}$, $i \in \{1, \dots, \delta+\gamma\}$. Define

$$\mathcal{M}^* = \begin{pmatrix} m_1 \\ m_1 + m_2 \\ \vdots \\ m_1 + m_\delta \\ m_1 + 2m_{\delta+1} \\ \vdots \\ m_1 + 2m_{\gamma+\delta} \end{pmatrix}.$$

Theorem

Let $\mathcal{P}_s = \{\mathcal{M}_i \ : \ 0 \leq i \leq s\} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$. Then, $\phi(\mathcal{P}_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$ with information set $\phi(\mathcal{I}_{\gamma,\delta}) \Leftrightarrow$ no two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$ for $i \neq j$ have a row in common.

Corollary

If $\phi(\mathcal{P}_s)$ is an s-PD-set of size $s+1$ for $H_{\gamma,\delta}$, then $s \leq f_{\gamma,\delta} = \left\lfloor \frac{2^{\gamma+2\delta-2}}{\gamma+\delta} \right\rfloor - 1.$

Let $h(x)$ be a primitive basic irreducible of degree $\delta - 1$ dividing $x^\ell - 1$, $\ell = 2^\delta - 1$. Let $\mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ and α be a root of $h(x)$. Any $r \in \mathcal{R}$ is written uniquely as $r = a + 2b$, where $a, b \in \{0, 1, \alpha, \dots, \alpha^{\ell-1}\}$.

Take $\mathcal{R}$ as the following ordered set:

$$\begin{aligned}\mathcal{R} &= \{r_1, \dots, r_{4^\delta - 1}\} \\ &= \{0 + 2\cdot 0, \dots, \alpha^{\ell-1} + 2\cdot 0, \dots, 0 + 2\cdot\alpha^{\ell-1}, \dots, \alpha^{\ell-1} + 2\cdot\alpha^{\ell-1}\}.\end{aligned}$$

Consider the $\delta \times \delta$ quaternary matrices, $i \in \{0, \dots, f_{0,\delta}\}$:

$$\mathcal{N}_i^* = \begin{pmatrix} 1 & r_{\delta i+1} \\ \vdots & \vdots \\ 1 & r_{\delta(i+1)} \end{pmatrix}.$$

Theorem

Let $\mathcal{P}_s = \{\mathcal{M}_i = \mathcal{N}_i^{-1} \ : \ 0 \leq i \leq s\}$*. Then* $\phi(\mathcal{P}_s)$ *is an* s-PD*-set of size* $s+1$ *for the* $\mathbb{Z}_4$*-linear Hadamard code* $H_{0,\delta}$ *of length* $2^{2\delta-1} = 2^m$ *with information set* $\phi(\mathcal{I}_{0,\delta})$*, for all* $\delta \geq 3$ *and* $2 \leq s \leq f_{0,\delta} = f_m$*.*

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$

$$\begin{aligned} &= \{r_1, \dots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$
$$\begin{aligned} &= \{r_1, \dots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & r_1 \\ 1 & r_2 \\ 1 & r_3 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & r_4 \\ 1 & r_5 \\ 1 & r_6 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & r_7 \\ 1 & r_8 \\ 1 & r_9 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & r_{10} \\ 1 & r_{11} \\ 1 & r_{12} \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & r_{13} \\ 1 & r_{14} \\ 1 & r_{15} \end{pmatrix}.$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$

$$\begin{aligned} &= \{r_1, \ldots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$

$$\begin{aligned} \mathcal{R} &= \{r_1, \dots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$
$$\begin{aligned} &= \{r_1, \dots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take
$$\begin{aligned}\mathcal{R} &= \{r_1, \dots, r_{16}\}\\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha\\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}.\end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$
$$\begin{aligned} &= \{r_1, \dots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Example

- Let $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ be a primitive basic irreducible dividing $x^3 - 1$.
- Let $\alpha \in \mathcal{R} = \mathbb{Z}_4[x]/(h(x))$ be a root of $h(x)$.

We take $\mathcal{R}$

$$\begin{aligned} \mathcal{R} &= \{r_1, \ldots, r_{16}\} \\ &= \{0, 1, \alpha, 3+3\alpha, 2, 3, 2+\alpha, 1+3\alpha, 2\alpha, 1+2\alpha \\ &\quad 3\alpha, 3+\alpha, 2+2\alpha, 3+2\alpha, 2+3\alpha, 1+\alpha\}. \end{aligned}$$

Then

$$\mathcal{N}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathcal{N}_1^* = \begin{pmatrix} 1 & 3 & 3 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \quad \mathcal{N}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 3 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{N}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 3 & 1 \end{pmatrix} \text{ and } \mathcal{N}_4^* = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

The set $\phi(\mathcal{P}_4)$ is a 4-PD-set of size 5 for $H_{0,3}$, where

$$\mathcal{P}_4 = \{\mathcal{N}_0^{-1}, \mathcal{N}_1^{-1}, \mathcal{N}_2^{-1}, \mathcal{N}_3^{-1}, \mathcal{N}_4^{-1}\} \subseteq \mathrm{PAut}(\mathcal{H}_{0,3})$$

Let $2S = 2^1 S$ denote the set $(S|S)$ and, recursively, $2^i S = 2(2^{i-1} S)$.

Proposition

Let $\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}_{\gamma,\delta})$ such that $\phi(\mathcal{S})$ is an s-PD-set of size ℓ for $H_{\gamma,\delta}$ with information set I. Then

$$\phi(2^{i+2j}\mathcal{S})$$

is an s-PD-set of size ℓ for $H_{\gamma+i,\delta+j}$ with information set obtained from I recursively.

Maximum s for which s-PD-sets of size $s+1$ are found computationally for some codes $H_{\gamma,\delta}$.

δ	γ	$f_{0,\delta}$	s	$f_{\gamma,\delta}$	f_m	t_m
3	0	4	**4**	4	4	7
	1	4	**6**	7	8	15
	2	4	**10**	11	15	31
	3	4	**16**	20	27	63
	4	4	**26**	35	50	127
4	0	15	**15**	15	15	31
	1	15	**23**	24	27	63
	2	15	**36**	41	50	127
	3	15	**56**	72	92	255
	4	15	**91**	127	169	511
5	0	50	**50**	50	50	127
	1	50	**72**	84	92	255
	2	50	**116**	145	169	511
	3	50	**187**	255	314	1023
	4	50	**312**	454	584	2047

Maximum s for which s-PD-sets of size $s+1$ are found computationally for some codes $H_{\gamma,\delta}$.

δ	γ	$f_{0,\delta}$	s	$f_{\gamma,\delta}$	f_m	t_m
3	0	**4**	**4**	**4**	**4**	7
	1	4	**6**	7	8	15
	2	4	**10**	11	15	31
	3	4	**16**	20	27	63
	4	4	**26**	35	50	127
4	0	**15**	**15**	**15**	**15**	31
	1	15	**23**	24	27	63
	2	15	**36**	41	50	127
	3	15	**56**	72	92	255
	4	15	**91**	127	169	511
5	0	**50**	**50**	**50**	**50**	127
	1	50	**72**	84	92	255
	2	50	**116**	145	169	511
	3	50	**187**	255	314	1023
	4	50	**312**	454	584	2047

Maximum s for which s-PD-sets of size $s+1$ are found computationally for some codes $H_{\gamma,\delta}$.

δ	γ	$f_{0,\delta}$	s	$f_{\gamma,\delta}$	f_m	t_m
3	0	4	**4**	4	4	7
	1	4	**6**	**7**	8	15
	2	4	**10**	11	15	31
	3	4	**16**	20	27	63
	4	4	**26**	35	50	127
4	0	15	**15**	15	15	31
	1	15	**23**	**24**	27	63
	2	15	**36**	41	50	127
	3	15	**56**	72	92	255
	4	15	**91**	127	169	511
5	0	50	**50**	50	50	127
	1	50	**72**	84	92	255
	2	50	**116**	145	169	511
	3	50	**187**	255	314	1023
	4	50	**312**	454	584	2047

The Gray map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ can be generalized to $\phi : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^{2^{k-1}}$.

A code $\mathcal{C}$ is a $\mathbb{Z}_{2^k}$**-additive Hadamard code** if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^k}^{\beta}$ and $\phi(\mathcal{C})$ is a binary Hadamard code, which is called $\mathbb{Z}_{2^k}$**-linear Hadamard code**.

Let $\mathcal{H}_\delta$ be a $\mathbb{Z}_{2^k}$-additive Hadamard code of length β and type $(2^k)^\delta$. If $\mathcal{G}$ is a generator matrix for $\mathcal{H}_{\delta-1}$, then $\mathcal{G}_\delta$ is a generator matrix for $\mathcal{H}_\delta$, where

$$\mathcal{G}_\delta = \begin{pmatrix} \mathcal{G} & \mathcal{G} & \mathcal{G} & \cdots & \mathcal{G} \\ \mathbf{0} & \mathbf{1} & \mathbf{3} & \cdots & \mathbf{2^k-1} \end{pmatrix}.$$

- $\mathbb{Z}_{2^k}$-linear Hadamard codes are systematic and information sets can also be defined in a recursive way.
- $\mathrm{PAut}(\mathcal{H}_\delta) \cong \{\begin{pmatrix} 1 & \eta \\ \mathbf{0} & A \end{pmatrix} : A \in \mathrm{GL}(\delta-1, \mathbb{Z}_{2^k}), \eta \in \mathbb{Z}_{2^k}^{\delta-1}\} \subseteq \mathrm{GL}(\delta, \mathbb{Z}_{2^k})$
- Using the same approach, we can construct s-PD-sets of size $s+1$ for the $\mathbb{Z}_{2^k}$-linear Hadamard codes $\phi(\mathcal{H}_\delta)$.

We present a criterion on subsets of matrices of $\mathrm{GL}(m, \mathbb{Z}_n)$ to be an s-PD-set of minimum size $s+1$ for binary linear and $\mathbb{Z}_{2^k}$-linear Hadamard codes of length 2^m.

We provide explicit constructions of s-PD-sets of size $s+1$ for these codes.

Further research on this topic:

- Providing an explicit construction of s-PD-sets of size $s+1$ for $H_{\gamma,\delta}$ of length $2^{\gamma+2\delta-1}$ with $\gamma > 0$ and $\delta \geq 3$ for $f_{0,\delta} < s \leq f_m$.
- Finding s-PD-sets of size $s+i$ for $s \geq f_m$ and PD-sets.
- Finding s-PD-sets for other families of $\mathbb{Z}_4$-linear codes: Reed-Muller codes, extended dualized Kerdock codes, ...

We present a criterion on subsets of matrices of $\mathrm{GL}(m, \mathbb{Z}_n)$ to be an s-PD-set of minimum size $s+1$ for binary linear and $\mathbb{Z}_{2^k}$-linear Hadamard codes of length 2^m.

We provide explicit constructions of s-PD-sets of size $s+1$ for these codes.

Further research on this topic:

- Providing an explicit construction of s-PD-sets of size $s+1$ for $H_{\gamma,\delta}$ of length $2^{\gamma+2\delta-1}$ with $\gamma > 0$ and $\delta \geq 3$ for $f_{0,\delta} < s \leq f_m$.
- Finding s-PD-sets of size $s+i$ for $s \geq f_m$ and PD-sets.
- Finding s-PD-sets for other families of $\mathbb{Z}_4$-linear codes: Reed-Muller codes, extended dualized Kerdock codes, ...

THANK YOU FOR YOUR ATTENTION