Partial permutation decoding for $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes

Josep Rifà Adrián Torres-Martín Mercè Villanueva

Department of Information and Communications Engineering
Combinatorics, Coding and Security Group

UAB
Universitat Autònoma de Barcelona

Rijeka Conference on Combinatorial Objects and Their Applications

Outline

1. Introduction
   - $\mathbb{Z}_{p^s}$-linear codes
   - Permutation decoding
   - $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes

2. r-PD-sets for $\mathbb{Z}_{p^s}$-linear GH codes
   - Information sets
   - Permutation automorphism group
   - Criterion for r-PD-sets

3. Constructions of r-PD-sets of size r+1
   - Explicit construction of r-PD-sets of size $r+1$
   - Recursive constructions of r-PD-sets

Contents

$\mathbb{Z}_{p^s}$-additive codes

Definition

A nonempty subset of $\mathbb{Z}_{p^s}^n$ is a $\mathbb{Z}_{p^s}$-**additive code** of length n if it is a subgroup of $\mathbb{Z}_{p^s}^n$.

- Isomorphic to $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{2^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_p^{t_s}$ and we say that it is of **type** $(n; t_1, \ldots, t_s)$. Permutation equivalent to a $\mathbb{Z}_{p^s}$-additive code with generator matrix in **standard form**:

$$\mathcal{G} = \begin{pmatrix} Id_{t_1} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,s} \\ \mathbf{0} & pId_{t_2} & pA_{1,2} & 2A_{1,3} & \cdots & \cdots & pA_{1,s} \\ \mathbf{0} & \mathbf{0} & p^2Id_{t_3} & p^2A_{2,3} & \cdots & \cdots & p^2A_{2,s} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & p^{s-1}Id_{t_s} & p^{s-1}A_{s-1,s} \end{pmatrix}$$

$\mathbb{Z}_{p^s}$-linear codes

Definition

Generalization of Carlet's **Gray map**. $\Phi_s : \mathbb{Z}_{p^s} \longrightarrow \mathbb{Z}_p^{p^{s-1}}$,

$$\Phi_s(u) = (u_{s-1}, \dots, u_{s-1}) + (u_0, \dots, u_{s-2})Y_{s-1},$$

where $u = [u_0, u_1, \dots, u_{s-1}]_2$ is the p-ary expansion of u and Y_{s-1} has the elements of $\mathbb{Z}_p^{s-1}$ as columns.

Definition

If $\mathcal{C}$ is a $\mathbb{Z}_{p^s}$-additive code of length n, then $\Phi_s(\mathcal{C})$ is called a $\mathbb{Z}_{p^s}$-**linear code** of length $p^{s-1}n$.

- $\Phi_s(\mathcal{C})$ is a code over $\mathbb{Z}_p$ which may not be linear. That is, it may not be a linear subspace of $\mathbb{Z}_p^{p^{s-1}n}$.

Permutation decoding. Basic definitions

Let C be a t-error correcting code over $\mathbb{Z}_p$ of length n.

Definition

- If C has p^k codewords, a set $I \subseteq \{1, \ldots, n\}$ of k coordinate positions is an **information set** if $C_I = \{\mathbf{u}|_I : \mathbf{u} \in C\}$ satisfies $|C_I| = |C| = p^k$. If such a set exists, then C is called a **systematic code**.
- The **permutation automorphism group** of C is

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

- A subset $P \subseteq \mathrm{PAut}(C)$ is called an r-**PD-set** if every r-set of coordinate positions is moved out of the information set by at least one element in P. If $r = t$, then P is called a **PD-set**.

Permutation decoding

Permutation decoding: Use a suitable element in a PD-set to move the errors out of the information coordinates in order to decode.

- Originally designed by Prange (1962), and developed by MacWilliams (1964), for linear codes.
- An alternative permutation decoding method was proposed, which can be used for any systematic code.

  J. J. Bernal, J. Borges, C. Fernández-Córdoba, and M. Villanueva. Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. *Designs, Codes and Cryptography*, 76(2):269–277, 2015.

- $\mathbb{Z}_{p^s}$-linear codes were proved to be systematic.

  A. Torres-Martín and M. Villanueva. Systematic encoding and permutation decoding for $\mathbb{Z}_{p^s}$-linear codes. *IEEE Transactions on Information Theory*, 68(7):4435–4443, 2022.

$\mathbb{Z}_{p^s}$-linear generalized Hadamard codes

Definition

A **generalized Hadamard (GH) code** C over $\mathbb{Z}_p$ of length N is defined as $C = \bigcup_{\alpha\in\mathbb{Z}_p}\{\mathbf{h}+\alpha\mathbf{1} : \mathbf{h}\in F_H\}$, where F_H is the code consisting of the rows of a generalized Hadamard matrix of order N over $\mathbb{Z}_p$.

Proposition

A GH code over $\mathbb{Z}_p$ of length N has pN codewords and minimum distance $\frac{(p-1)N}{p}$.

- $\mathbb{Z}_{p^s}$-linear GH codes allow for an easier approach to the PAut. In particular, r-PD-sets for $\mathbb{Z}_4$-linear Hadamard codes have been studied.

R. D. Barrolleta and M. Villanueva. Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes. *Des. Codes Cryptogr.*, 86(3):569–586, 2018.

$\mathbb{Z}_{p^s}$-linear generalized Hadamard codes

- Consider the matrix $\mathcal{G}^{t_1,\dots,t_s}$ whose columns are all the elements in $\{1\} \times \mathbb{Z}_{p^s}^{t_1-1} \times (p\mathbb{Z}_{p^s})^{t_2} \times \cdots \times (p^{s-1}\mathbb{Z}_{p^s})^{t_s}$.

Example

For $p = 3$ and $s = 3$, $\mathcal{G}^{2,0,1}$ is the following matrix over $\mathbb{Z}_{27}$:

$$\mathcal{G}^{2,0,1} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & 26 & 0 & 1 & 2 & \cdots & 26 & 0 & 1 & 2 & \cdots & 26 \\ 0 & 0 & 0 & \cdots & 0 & 9 & 9 & 9 & \cdots & 9 & 18 & 18 & 18 & \cdots & 18 \end{pmatrix}.$$

Definition

Let $\mathcal{H}^{t_1,\dots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive code generated by $\mathcal{G}^{t_1,\dots,t_s}$, and let $H^{t_1,\dots,t_s} = \Phi(\mathcal{H}^{t_1,\dots,t_s})$ be the corresponding $\mathbb{Z}_{p^s}$-linear code. $H^{t_1,\dots,t_s}$ is a generalized Hadamard code.

Contents

Information sets

Definition

$\mathcal{I} = \{i_1, \ldots, i_{t_1+\cdots+t_s}\} \subseteq \{1, \ldots, n\}$ is an **additive information set** for a $\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ of type $(n; t_1, \ldots, t_s)$ if $|\mathcal{C}_\mathcal{I}| = p^{st_1+(s-1)t_2+\cdots+t_s}$.

Proposition. [Torres-Martín and Villanueva, 2022]

From an additive information set $\mathcal{I}$ for $\mathcal{C}$, we can obtain an information set $I = \Phi(\mathcal{I})$ for $C = \Phi(\mathcal{C})$.

Example

$\mathcal{I} = \{1, 2, 9\}$ is an additive information set for $\mathcal{H}^{2,0,1}$.

$$\mathcal{G}^{2,0,1} = \left(\begin{array}{cccccccc c cccccccc} \boxed{1} & \boxed{1} & 1 & 1 & 1 & 1 & 1 & 1 & & \boxed{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \boxed{0} & \boxed{1} & 2 & 3 & 4 & 5 & 6 & 7 & & \boxed{0} & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \boxed{0} & \boxed{0} & 0 & 0 & 0 & 0 & 0 & 0 & & \boxed{4} & 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{array}\right).$$

$\Phi(\mathcal{I}) = \{1, 2, 3, 5, 6, 7, 33\}$ is an information set for $H^{2,0,1} = \Phi(\mathcal{H}^{2,0,1})$.

Permutation automorphism group

Let $\mathcal{L}$ be the set of matrices over $\mathbb{Z}_{p^s}$ of the form

$$\begin{pmatrix} 1 & a_1 & pa_2 & \cdots & p^{s-2}a_{s-1} & p^{s-1}a_s \\ \mathbf{0} & A_{1,1} & pA_{1,2} & \cdots & p^{s-2}A_{1,s-1} & p^{s-1}A_{1,s} \\ \mathbf{0} & A_{2,1} & A_{2,2} & \cdots & p^{s-3}A_{2,s-1} & p^{s-2}A_{2,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & A_{s-1,1} & A_{s-1,2} & \cdots & A_{s-1,s-1} & pA_{s-1,s} \\ \mathbf{0} & A_{s,1} & A_{s,2} & \cdots & A_{s,s-1} & A_{s,s} \end{pmatrix},$$

where $A_{i,i}$ are invertible matrices.

Permutation automorphism group

Let $\pi(\mathcal{L})$ be the set of matrices over $\mathbb{Z}_{p^s}$ of the form

$$\begin{array}{r} \\ \\ \text{mod } p^{s-1} \longrightarrow \\ \vdots \\ \text{mod } p^{2} \longrightarrow \\ \text{mod } p \longrightarrow \end{array} \begin{pmatrix} 1 & a_1 & pa_2 & \cdots & p^{s-2}a_{s-1} & p^{s-1}a_s \\ \mathbf{0} & A_{1,1} & pA_{1,2} & \cdots & p^{s-2}A_{1,s-1} & p^{s-1}A_{1,s} \\ \mathbf{0} & A_{2,1} & A_{2,2} & \cdots & p^{s-3}A_{2,s-1} & p^{s-2}A_{2,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & A_{s-1,1} & A_{s-1,2} & \cdots & A_{s-1,s-1} & pA_{s-1,s} \\ \mathbf{0} & A_{s,1} & A_{s,2} & \cdots & A_{s,s-1} & A_{s,s} \end{pmatrix},$$

where $A_{i,i}$ are invertible matrices.

Permutation automorphism group

Let $\pi(\mathcal{L})$ be the set of matrices over $\mathbb{Z}_{p^s}$ of the form

$$\begin{array}{r} \\ \\ \bmod p^{s-1} \longrightarrow \\ \vdots \\ \bmod p^2 \longrightarrow \\ \bmod p \longrightarrow \end{array} \begin{pmatrix} 1 & a_1 & pa_2 & \cdots & p^{s-2}a_{s-1} & p^{s-1}a_s \\ \mathbf{0} & A_{1,1} & pA_{1,2} & \cdots & p^{s-2}A_{1,s-1} & p^{s-1}A_{1,s} \\ \mathbf{0} & A_{2,1} & A_{2,2} & \cdots & p^{s-3}A_{2,s-1} & p^{s-2}A_{2,s} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & A_{s-1,1} & A_{s-1,2} & \cdots & A_{s-1,s-1} & pA_{s-1,s} \\ \mathbf{0} & A_{s,1} & A_{s,2} & \cdots & A_{s,s-1} & A_{s,s} \end{pmatrix},$$

where $A_{i,i}$ are invertible matrices.

Lemma

$\pi(\mathcal{L}) \subseteq \mathrm{GL}(t_1 + \cdots + t_s, \mathbb{Z}_{p^s})$ *is a group with the operation* $\mathcal{M} * \mathcal{N} = \pi(\mathcal{M}\mathcal{N})$, *for all* $\mathcal{M}, \mathcal{N} \in \pi(\mathcal{L})$.

Theorem

$\mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ *is isomorphic to* $\pi(\mathcal{L})$.

Permutation automorphism group

- A matrix $\mathcal{M} \in \mathrm{PAut}(\mathcal{H}^{t_1,\ldots,t_s})$ sends columns of $\mathcal{G}^{t_1,\ldots,t_s}$ to other columns of $\mathcal{G}^{t_1,\ldots,t_s}$. Therefore $\mathcal{M}$ can be seen as a permutation $\tau \in \mathrm{Sym}(n)$, such that $\tau(i) = j$ iff $w_j = w_i\mathcal{M}$, where w_i, w_j are the columns i, j in $\mathcal{G}^{t_1,\ldots,t_s}$.

Definition

Let $\Phi : \mathrm{Sym}(n) \to \mathrm{Sym}(p^{s-1}n)$ be the map defined as

$$\Phi(\tau)(i) = p^{s-1}\left[\tau\left(\left\lfloor \frac{i-1}{p^{s-1}} \right\rfloor + 1\right) - 1\right] + (i \mod p^{s-1}),$$

Example. $p = 2$, $s = 2$

$\tau = (1,2) \in \mathrm{Sym}(n) \Longrightarrow \Phi(\tau) = (1,5)(2,6)(3,7)(4,8) \in \mathrm{Sym}(4n)$

- We define $\Phi(\mathcal{M}) = \Phi(\tau) \in \mathrm{Sym}(p^{s-1}n)$.

Criterion for r-PD-sets

Theorem

$\mathcal{P}_r = \{\mathcal{M}_i : 0 \leq i \leq r\} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$. $\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for $H^{t_1,\dots,t_s}$ iif no two matrices $(\mathcal{M}_i^{-1})^*$ and $(\mathcal{M}_j^{-1})^*$, $i \neq j$, have a row in common.

$$\mathcal{M} = \begin{pmatrix} m_1 \\ \vdots \\ m_{t_1+\cdots+t_s} \end{pmatrix} \xrightarrow{*} \mathcal{M}^* = \begin{pmatrix} m_1 \\ m_1 + m_2 \\ \vdots \\ m_1 + m_{t_1} \\ m_1 + pm_{t_1+1} \\ \vdots \\ m_1 + pm_{t_1+t_2} \\ \vdots \\ m_1 + p^{s-1} m_{t_1+\cdots+t_{s-1}+1} \\ \vdots \\ m_1 + p^{s-1} m_{t_1+\cdots+t_s} \end{pmatrix}$$

- **Upper bound:** $r \leq f_p^{t_1,\dots,t_s} = \left\lfloor \frac{p^{st_1+(s-1)t_2+\cdots+t_s-s} - t_1 - t_2 - \cdots - t_s}{t_1+t_2+\cdots+t_s} \right\rfloor$.

Contents

Explicit construction of r-PD-sets of size $r+1$

Goal: Find a set of matrices $\{\mathcal{M}_0^*, \dots, \mathcal{M}_r^*\}$, $r \leq f_p^{t_1,\dots,t_s}$, with no row in common such that $\{\mathcal{M}_0^{-1}, \dots, \mathcal{M}_r^{-1}\} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,\dots,t_s})$.

- $\mathrm{GR}(p^{s(t_1-1)}) \cong \mathbb{Z}_{p^s}[x]/(h(x))$, $h(x)$ monic basic primitive of degree t_1-1, $h(x) \mid x^l - 1$, where $l = p^{t_1-1} - 1$.
- α root of $h(x)$ of order l. $T = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{l-1}\}$.
- **p-adic representation:** $y = a_1 + pa_2 + p^2 a_3 + \cdots + p^{s-1} a_s$, $a_i \in T$
- $\mathcal{R} = \mathbb{Z}_{p^s}[x]/(h(x)) = \{y_1, \dots, y_{p^{s(t_1-1)}}\}$, with lexicographical order.
- **Additive representation:** $y = \sum_{i=0}^{t_1-2} b_i \alpha^i$, $b_i \in \mathbb{Z}_{p^s}$. Represented as $(b_0, \dots, b_{t_1-2})$.

Explicit construction of r-PD-sets of size $r+1$

- Define the set of matrices $\mathcal{P}_r = \{\mathcal{M}_0^{-1}, \ldots, \mathcal{M}_r^{-1}\}$, where

$$\mathcal{M}_i^* = \begin{pmatrix} 1 & y_{t_1 i+1} \\ \vdots & \vdots \\ 1 & y_{t_1(i+1)} \end{pmatrix}.$$

- Note that there are $\lfloor \frac{p^{s(t_1-1)}}{t_1} \rfloor = f_p^{t_1,0,\ldots,0} + 1$. Therefore r can reach the bound $f_p^{t_1,0,\ldots,0}$.

Theorem

$\Phi(\mathcal{P}_r)$ is an r-PD-set of size $r+1$ for the $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,0,\ldots,0}$, for all $t_1 \geq 3$ and $2 \leq r \leq f_p^{t_1,0,\ldots,0}$.

Explicit construction of r-PD-sets of size $r+1$

Example. r-PD-sets for $H^{3,0,0}$, $p=2$

- $\mathcal{R} = \mathbb{Z}_8[x]/(h(x))$, $h(x) = x^2 + x + 1$.
- α root of $h(x)$. $T = \{0, 1, \alpha, \alpha^2\}$.
- $\mathcal{R} = \{0, 1, \alpha, 7\alpha + 7, 2, 3, \dots, 2 + 2\alpha, 3 + 2\alpha, 2 + 3\alpha, 1 + \alpha\}$.
- **Example:** $y = \alpha^2 = -1 - \alpha = 7 + 7\alpha \longleftrightarrow (7, 7)$.
- $r \le f_2^{3,0,0} = \lfloor \frac{2^6 - 3}{3} \rfloor = 20$

$$\mathcal{M}_0^* = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \mathcal{M}_1^* = \begin{pmatrix} 1 & 7 & 7 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix}, \mathcal{M}_2^* = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 7 \\ 1 & 0 & 2 \end{pmatrix},$$

$$\mathcal{M}_3^* = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 3 \\ 1 & 7 & 1 \end{pmatrix}, \mathcal{M}_4^* = \begin{pmatrix} 1 & 6 & 6 \\ 1 & 7 & 6 \\ 1 & 6 & 7 \end{pmatrix}, \mathcal{M}_5^* = \begin{pmatrix} 1 & 5 & 5 \\ 1 & 4 & 0 \\ 1 & 5 & 0 \end{pmatrix},$$

$$\mathcal{M}_6^* = \begin{pmatrix} 1 & 4 & 1 \\ 1 & 3 & 7 \\ 1 & 6 & 0 \end{pmatrix}, \mathcal{M}_7^* = \begin{pmatrix} 1 & 7 & 0 \\ 1 & 6 & 1 \\ 1 & 5 & 7 \end{pmatrix}, \mathcal{M}_8^* = \begin{pmatrix} 1 & 4 & 2 \\ 1 & 5 & 2 \\ 1 & 4 & 3 \end{pmatrix}.$$

Explicit construction of r-PD-sets of size $r+1$

Example. r-PD-sets for $H^{3,0,0}$

- $\mathcal{P}_8 = \{\mathcal{M}_0^{-1}, \dots, \mathcal{M}_8^{-1}\} \subseteq \mathrm{PAut}(\mathcal{H}^{3,0,0})$.
- $\Phi(\mathcal{P}_8) \subseteq \mathrm{Sym}(256)$ is an 8-PD-set of size 9 for $H^{3,0,0}$ with information set $\Phi(\mathcal{I}_{3,0,0}) = \{1,2,3,5,6,7,33,34,35\}$.

$$\mathcal{M}_1^* = \begin{pmatrix} 1 & 7 & 7 \\ 1 & 2 & 0 \\ 1 & 3 & 0 \end{pmatrix} \longrightarrow \mathcal{M}_1 = \begin{pmatrix} 1 & 7 & 7 \\ 0 & 3 & 1 \\ 0 & 4 & 1 \end{pmatrix} \longrightarrow \mathcal{M}_1^{-1} = \begin{pmatrix} 1 & 3 & 6 \\ 0 & 7 & 1 \\ 0 & 4 & 5 \end{pmatrix}$$

$$\begin{aligned} \longrightarrow \tau_1 = &(1,52,57,16,17,4,9,32,33,20,25,48,49,36,41,64) \\ &(2,59,30,19,18,11,46,35,34,27,62,51,50,43,14,3) \\ &(5,24,61,44,21,40,13,60,37,56,29,12,53,8,45,28) \\ &(6,31,26,55,22,47,42,7,38,63,58,23,54,15,10,39) \in \mathrm{Sym}(64) \end{aligned}$$

$$\begin{aligned} \longrightarrow \Phi(\tau_1) = &(1,205,225,61,65,13,33,125,129,77,97,189,193,141,161,253) \\ &\dots \\ &(24,124,104,220,88,188,168,28,152,252,232,92,216,60,40,156) \in \mathrm{Sym}(256) \end{aligned}$$

Recursive construction. Permutation representation

Main idea: r-PD-sets for $H^{t_1,t_2,t_3} \longrightarrow r$-PD-sets for $H^{t_1+i_1,t_2+i_2,t_3+i_3}$.

Drawback: r does not increase, even when the bound $f_p^{t_1,t_2,t_3}$ does.

$$\begin{tikzcd}
\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,t_2,t_3}) \arrow[r] \arrow[d] & 2^2\mathcal{S} \subseteq \mathrm{PAut}(\mathcal{H}^{t_1,t_2+1,t_3}) \arrow[d] \\
\Phi(\mathcal{S}) \subseteq \mathrm{PAut}(H^{t_1,t_2,t_3}) & \Phi(2^2\mathcal{S}) \subseteq \mathrm{PAut}(H^{t_1,t_2+1,t_3})
\end{tikzcd}$$

Example

If $\sigma_1 = (1,2,3) \in \mathrm{Sym}(4)$ and $\sigma_2 = (1,2) \in \mathrm{Sym}(3)$, then

$$(\sigma_1 \,|\, \sigma_2) = (1,2,3)(5,6) \in \mathrm{Sym}(7).$$

Construction for non-free codes

$$\mathcal{M}_i^* = \begin{pmatrix} 1 & r_{i_1} & 0 & 0 \\ 1 & r_{i_2} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & r_{i_{t_1}} & 0 & 0 \\ 1 & r_{i_1} & & 0 \\ \vdots & \vdots & 2I_{t_2} & \vdots \\ 1 & r_{i_1} & & 0 \\ 1 & r_{i_1} & 0 & \\ \vdots & \vdots & \vdots & 4I_{t_3} \\ 1 & r_{i_1} & 0 & \end{pmatrix}, \quad \mathcal{M}_i = \begin{pmatrix} 1 & r_{i_1} & 0 & 0 \\ 0 & r_{i_2} - r_{i_1} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & r_{i_{t_1}} - r_{i_1} & 0 & 0 \\ 0 & 0 & & 0 \\ \vdots & \vdots & 2I_{t_2} & \vdots \\ 0 & 0 & & 0 \\ 0 & 0 & 0 & \\ \vdots & \vdots & \vdots & 4I_{t_3} \\ 0 & 0 & 0 & \end{pmatrix}$$

- $r_{i_1}, \dots, r_{i_{t_1}}$ consecutive in the ordered sequence $r_1, \dots, r_{8^{t_1}-1}$,

Construction for non-free codes

$$\mathcal{M}^*_{i,k} = \begin{array}{c} \begin{array}{cccc} & \phantom{r_{i_{t_1+t_2+t_3}}} & \overbrace{}^{+\mathbf{u}_k} & \overbrace{}^{+\mathbf{v}_k} \end{array} \\ \begin{pmatrix} 1 & r_{i_1} & 0 & 0 \\ 1 & r_{i_2} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & r_{i_{t_1}} & 0 & 0 \\ 1 & \mathbf{r_{i_{t_1+1}}} & & 0 \\ \vdots & \vdots & 2I_{t_2} & \vdots \\ 1 & \mathbf{r_{i_{t_1+t_2}}} & & 0 \\ 1 & \mathbf{r_{i_{t_i+t_2+1}}} & 0 & \\ \vdots & \vdots & \vdots & 4I_{t_3} \\ 1 & \mathbf{r_{i_{t_1+t_2+t_3}}} & 0 & \end{pmatrix} \end{array}, \mathcal{M}_{i,k} = \begin{pmatrix} 1 & r_{i_1} & \mathbf{u}_k & \mathbf{v}_k \\ 0 & r_{i_2} - r_{i_1} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & r_{i_{t_1}} - r_{i_1} & 0 & 0 \\ 0 & (r_{i_{t_1+1}} - r_{i_1})' & & 0 \\ \vdots & \vdots & 2I_{t_2} & \vdots \\ 0 & (r_{i_{t_1+t_2}} - r_{i_1})' & & 0 \\ 0 & (r_{i_{t_1+t_2+1}} - r_{i_1})'' & 0 & \\ \vdots & \vdots & \vdots & 4I_{t_3} \\ 0 & (r_{i_{t_1+t_2+t_3}} - r_{i_1})'' & 0 & \end{pmatrix}$$

Construction for non-free codes

$$
\mathcal{M}^*_{i,k} = \begin{array}{c}
\begin{array}{cccc} & \phantom{\mathbf{r}_{i_{t_1+t_2+t_3}}} & \overbrace{}^{+\mathbf{u}_k} & \overbrace{}^{+\mathbf{v}_k} \end{array} \\
\begin{pmatrix}
1 & r_{i_1} & 0 & 0 \\
1 & r_{i_2} & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots \\
1 & r_{i_{t_1}} & 0 & 0 \\
1 & \mathbf{r_{i_{t_1+1}}} & & 0 \\
\vdots & \vdots & 2I_{t_2} & \vdots \\
1 & \mathbf{r_{i_{t_1+t_2}}} & & 0 \\
1 & \mathbf{r_{i_{t_i+t_2+1}}} & 0 & \\
\vdots & \vdots & \vdots & 4I_{t_3} \\
1 & \mathbf{r_{i_{t_1+t_2+t_3}}} & 0 &
\end{pmatrix}
\end{array}
, \mathcal{M}_{i,k} = \begin{pmatrix}
1 & r_{i_1} & \mathbf{u}_k & \mathbf{v}_k \\
0 & r_{i_2} - r_{i_1} & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots \\
0 & r_{i_{t_1}} - r_{i_1} & 0 & 0 \\
0 & (r_{i_{t_1+1}} - r_{i_1})' & & 0 \\
\vdots & \vdots & 2I_{t_2} & \vdots \\
0 & (r_{i_{t_1+t_2}} - r_{i_1})' & & 0 \\
0 & (r_{i_{t_1+t_2+1}} - r_{i_1})'' & 0 & \\
\vdots & \vdots & \vdots & 4I_{t_3} \\
0 & (r_{i_{t_1+t_2+t_3}} - r_{i_1})'' & 0 &
\end{pmatrix}
$$

- $r_{i_1}, \ldots, r_{i_{t_1}}$ consecutive in the ordered sequence $r_1, \ldots, r_{8^{t_1}-1}$,
- $r_{i_{t_1+k}} - r_{i_1} \in (2) \subset \mathcal{R}$ for $1 \leq k \leq t_2$. $(2a)' = a$.
- $r_{i_{t_1+t_2+k}} - r_{i_1} \in (4) \subset \mathcal{R}$ for $1 \leq k \leq t_3$. $(4a)'' = a$.

Construction for non-free codes

Proposition

There exists an r-PD-set of size r+1 for H^{t_1,t_2,t_3} for every

$$r \leq 4^{t_2} 2^{t_3} \alpha - 1, \tag{1}$$

where $\alpha = \tau d_4$ is the maximum multiple of $d_4 = 2^{t_1-1} d_2$, with $d_2 = \lfloor \frac{2^{t_1-1}}{t_1} \rfloor$, such that the following conditions are satisfied:

$$\alpha \leq t_1 d_2 \left\lfloor \frac{4^{t_1-1} - 2^{t_1-1}\tau}{t_2+t_3} \right\rfloor \text{ when } t_2 + t_3 > 0, \tag{2}$$

$$\alpha \leq t_1 d_4 \left\lfloor \frac{2^{t_1-1} - \tau}{t_3} \right\rfloor \text{ when } t_3 > 0. \tag{3}$$

t_2	$r_{4,t_2,0}$	$f_2^{4,t_2,0}$	$r_{4,t_2,1}$	$f_2^{4,t_2,1}$	$r_{4,t_2,2}$	$f_2^{4,t_2,2}$	$r_{4,t_2,3}$	$f_2^{4,t_2,3}$
0	127	127	191	203	255	340	511	584
1	383	408	639	681	1023	1169	2047	2047
2	1279	1364	2047	2339	4095	4095	6143	7280
3	4095	4680	8191	8191	12287	14562	24575	26213

Thank You!