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

Dipak K. Bhunia, **Cristina Fernández-Córdoba**, Carlos Vela, Mercè Villanueva

Algebraic and combinatorial methods for coding and cryptography (ALCOCRYPT)
February 20-24, 2023

Universitat Autònoma de Barcelona

CCSG
Combinatorics, Coding and Security Group

Outline

Outline

Hadamard Codes
$(n, 2n, n/2)$

$\Downarrow$

$\mathbb{Z}_4$-linear and $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes

D. S. Krotov.
$\mathbb{Z}_4$-linear Hadamard and extended perfect codes.
IEEE Transaction on Information Theory, vol. 6, pp. 107-112, **2001**.

K. T. Phelps, J. Rifà, and M. Villanueva.
On the additive $\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear Hadamard codes: rank and kernel.
IEEE Transactions on Information Theory, vol. 52, pp. 316-319, 2006.

D. S. Krotov, M. Villanueva.
Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups.
IEEE Transactions on Information, vol. 61, pp. 887-894, **2015.**

⇓

$\mathbb{Z}_{2^s}$-linear Hadamard codes and partial classification

C. Fernández-Córdoba, C. Vela, and M. Villanueva
On $\mathbb{Z}_{2^s}$-linear Hadamard Codes: kernel and partial classification.
Designs, Codes and Cryptography, vol. 87, no. 2-3, pp. 417–435, 2019.

C. Fernández-Córdoba, C. Vela, and M. Villanueva
Equivalences among $\mathbb{Z}_{2^s}$-linear Hadamard codes.
Discrete Mathematics, vol. 343, no. 3, pp. 111721, 2020.

⇓

$\mathbb{Z}_{p^s}$-linear GH codes and partial classification

D. K. Bhunia, C. Fernández-Córdoba, M. Villanueva
On the Linearity and Classification of $\mathbb{Z}_{p^s}$-Linear Generalized Hadamard Codes.
Designs, Codes and Cryptography, vol. 90, pp. 1037–1058, 2022.

⇓

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

Outline

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

A code over $\mathbb{Z}_{p^s}$ of length n is a nonempty subset $\mathcal{C}$ of $\mathbb{Z}_{p^s}^n$.

If $\mathcal{C}$ has group structure, then it is called a $\mathbb{Z}_{p^s}$-additive code. In this case, $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{p^s}^n$, and it is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \mathbb{Z}_p^{t_s}$.
We say that $\mathcal{C}$ is of type $(n; t_1, \ldots, t_s)$.

A generator matrix (with minimum number of rows) has

- t_1 generators of order p^s,
- t_2 generators of order p^{s-1},

$\vdots$

- t_s generators of order p.

Generalized Hadamard (GH) codes

A generalized Hadamard (GH) matrix over $\mathbb{Z}_p$, $H(p,\lambda) = (h_{ij})$, is a $p\lambda \times p\lambda$ matrix over $\mathbb{Z}_p$ with the property that for every i, j, $1 \leq i < j \leq p\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \leq s \leq p\lambda\}$ contains every element of $\mathbb{Z}_p$ exactly λ times.

Two GH matrices H_1 and H_2 of order n are equivalent if one can be obtained from the other by a permutation of the rows and columns and adding the same element of $\mathbb{Z}_p$ to all the coordinates in a row/column.

We can always change the first row and column of a GH matrix into zeros and we obtain an equivalent GH matrix which is called normalized GH matrix.

D. Jungnickel
On difference matrices, resolvable designs and generalized Hadamard matrices
Math Z., vol. 167, pp. 49–60, 1979.

Let F_H be the code generated by the normalized GH matrix H, and $C_H = \bigcup_{\alpha \in \mathbb{Z}_p} (F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$.

The code C_H over $\mathbb{Z}_p$ is called generalized Hadamard (GH) code. If the length of C_H is N, then it is a $(N, pN, \frac{N(p-1)}{p})$ code.

Example

For $p = 3$ and $\lambda = 1$, we consider the following normalized GH matrix:

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

Then, we have that $F_H = \{(0,0,0), (0,1,2), (0,2,1)\}$, and

$$\begin{aligned} C_H = \{&(0,0,0), (0,1,2), (0,2,1), \\ &(1,1,1), (1,2,0), (1,0,2), \\ &(2,2,2), (2,0,1), (2,1,0)\}. \end{aligned}$$

Note that C_H has parameters $(3, 9, 2)$.

Generalized Gray map

Let $u \in \mathbb{Z}_{p^s}$. The generalized Gray map image of u is

$$\phi(u) = (u_s, \dots, u_s) + (u_1, \dots, u_{s-1})Y \in \mathbb{Z}_p^{p^{s-1}}, \quad \text{where}$$

- $[u_1, u_2, \dots, u_s]_p$ is the p-ary expansion of u, and
- Y is a $(s-1) \times p^{s-1}$ matrix which columns are the elements of $\mathbb{Z}_p^{s-1}$.

C. Carlet

$\mathbb{Z}_{2^k}$-linear codes

IEEE Transaction on Information Theory, vol. 44, pp. 1543-1547, **1998**.

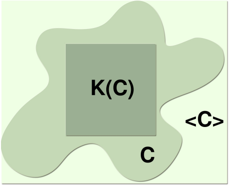
Let Φ be the component-wise extended map of ϕ.

If $\mathcal{C}$ is a $\mathbb{Z}_{p^s}$-additive code, $\Phi(\mathcal{C})$ is called a $\mathbb{Z}_{p^s}$-linear code.

Invariants: rank and dimension of kernel

The linear span of C is the subspace spanned by C over $\mathbb{Z}_p$, $\langle C \rangle$, and its dimension is called rank and denoted by $\text{rank}(C)$.

The kernel of C is define as $K(C) = \{x \in \mathbb{Z}_p^n : C + x = C\}$. If $\mathbf{0} \in C$, $K(C)$ is a linear subcode of C and its dimension is denoted by $\ker(C)$.



Outline

Let t_1, t_2,…,t_s be nonnegative integers with $t_1 \geq 1$.

- Start with the matrix $A^{1,0,\dots,0} = (1)$.
- Recursively, given a matrix $A^{t_1,\dots,t_s}$, we construct

$$A^{t'_1,\dots,t'_s} = \begin{pmatrix} A^{t_1,\dots,t_s} & A^{t_1,\dots,t_s} & \dots & A^{t_1,\dots,t_s} \\ 0 \cdot \mathbf{p}^{i-1} & 1 \cdot \mathbf{p}^{i-1} & \dots & (p^{s-i+1}-1) \cdot \mathbf{p}^{i-1} \end{pmatrix}$$

where $i \in \{1,\dots,s\}$, $t'_j = t_j$ for $j \neq i$ and $t'_i = t_i + 1$.

Examples of $\mathbb{Z}_{3^3}$-additive GH codes

Example

$$A^{1,0,0} = (\,1\,), \quad A^{1,0,1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 9 & 18 \end{pmatrix}, \quad A^{1,1,0} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{pmatrix},$$

$$A^{2,0,0} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{pmatrix},$$

$$A^{1,1,1} = \begin{pmatrix} A^{1,1,0} & A^{1,1,0} & A^{1,1,0} \\ \mathbf{0} & \mathbf{9} & \mathbf{18} \end{pmatrix}, \quad A^{2,0,1} = \begin{pmatrix} A^{2,0,0} & A^{2,0,0} & A^{2,0,0} \\ \mathbf{0} & \mathbf{9} & \mathbf{18} \end{pmatrix},$$

$$A^{2,1,0} = \begin{pmatrix} A^{2,0,0} & A^{2,0,0} & A^{2,0,0} & A^{2,0,0} & A^{2,0,0} & A^{2,0,0} & A^{2,0,0} & A^{2,0,0} & A^{2,0,0} \\ \mathbf{0} & \mathbf{3} & \mathbf{6} & \mathbf{9} & \mathbf{12} & \mathbf{15} & \mathbf{18} & \mathbf{21} & \mathbf{24} \end{pmatrix}.$$

Denote $\mathcal{H}^{t_1,\ldots,t_s}$ the $\mathbb{Z}_{p^s}$-additive code of type $(n; t_1, \ldots, t_s)$ generated by $A^{t_1,\ldots,t_s}$ and $H^{t_1,\ldots,t_s} = \Phi(\mathcal{H}^{t_1,\ldots,t_s})$ the corresponding $\mathbb{Z}_{p^s}$-linear code.

Theorem (BFV22)

Let $t_1, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. The $\mathbb{Z}_{p^s}$-linear code $H^{t_1,\ldots,t_s}$ of type $(n; t_1, \ldots, t_s)$ is a GH code over $\mathbb{Z}_p$ of length $N = p^t$, where $t = (\sum_{i=1}^{s}(s-i+1) \cdot t_i) - 1$ and $n = p^{t-s+1}$.

If the $\mathbb{Z}_{p^s}$-linear code $\Phi(\mathcal{C})$ is GH code, then then

- $\mathcal{C}$ is called a $\mathbb{Z}_{p^s}$-additive GH code,
- $\Phi(\mathcal{C})$ is called a $\mathbb{Z}_{p^s}$-linear GH code.

We define the order of $\mathcal{H}^{t_1,\dots,t_s}$ or equivalently, of $H^{t_1,\dots,t_s}$ as σ, where

$$\sigma = \begin{cases} 1, & \text{if } t_1 \geq 2, \\ s, & \text{if } t_1 = 1, t_2 = \dots = t_s = 0, \\ \min\{i : t_i > 0, i \in \{2,\dots,s\}\}, & \text{otherwise} \end{cases}$$

We denote $o(H^{t_1,\dots,t_s}) = o(\mathcal{H}^{t_1,\dots,t_s}) = \sigma$.

Example

- $o(H^{2,0,0}) = o(H^{3,1,1}) = o(H^{2,0,1}) = 1$,
- $o(H^{1,0,0}) = 3$,
- $o(H^{1,2,1}) = 2$, $o(H^{1,1,0}) = 2$, $o(H^{1,0,1}) = 3$.

Outline

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

Theorem (DFV22)

The $\mathbb{Z}_{p^s}$-linear GH codes $H^{1,0,\dots,0,t_s}$, with $p \geq 3$, $s \geq 2$ and $t_s \geq 0$, are the only $\mathbb{Z}_{p^s}$-linear GH codes which are linear.

Example

Let $t = 4$ and $s = 3$. Consider the equation $4 = 3t_1 + 2t_2 + t_3 - 1$. The $\mathbb{Z}_{27}$-linear GH codes of length $3^4 = 81$ are the following: $H^{1,0,2}$ and $H^{1,1,0}$. Then

- $H^{1,0,2}$ is linear,
- $H^{1,1,0}$ is nonlinear.

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

Theorem (DFV22)

Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ *be the* $\mathbb{Z}_{p^s}$*-additive GH code of type* $(n; t_1, \ldots, t_s)$ *and order* σ *with* $p \geq 3$*. Let* $\mathbf{w}_i$ *be the ith row of* $A^{t_1,\ldots,t_s}$ *and* $\tau = \sum_{i=1}^{s} t_i$*.*
Let $Q = \{(\mathrm{ord}(\mathbf{w}_q)/p)\mathbf{w}_q\}_{q=1}^{\tau}$ *and* $M = \{\mathbf{p^m}\}_{m=0}^{\sigma-2}$ *if* $\sigma \geq 2$*, and* $M = \emptyset$ *if* $\sigma = 1$*.*

Then, $\{\Phi(Q), \Phi(M)\}$ *is a basis of* $K(\Phi(\mathcal{H}))$ *and* $\ker(\Phi(\mathcal{H})) = \sum_{i=1}^{s} t_i + \sigma - 1$*.*

Example

Let $H^{1,1,0}$ be the $\mathbb{Z}_{27}$-linear GH code. By Theorem 7, $\ker(H^{1,1,0}) = 3$, since $\sigma = 2$. We have that $Q = \{\mathbf{9}, (0,9,18,0,9,18,0,9,18)\}$ and $M = \{\mathbf{1}\}$. Thus,

$$K(H^{1,1,0}) = \langle \Phi(\mathbf{9}), \Phi((0,9,18,0,9,18,0,9,18)), \Phi(\mathbf{1}) \rangle.$$

Rank and kernel for all nonlinear $\mathbb{Z}_{3^s}$-linear GH codes of length 3^t

$\mathbb{Z}_{3^s}$	$t=4$		$t=5$		$t=6$		$t=7$	
	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)
$\mathbb{Z}_{3^2}$	$(2,1)$	(6,3)	$(2,2)$	(7,4)	$(3,1)$	(12,4)	$(3,2)$	(13,5)
			$(3,0)$	(11,3)	$(2,3)$	(8,5)	$(4,0)$	(21,4)
							$(2,4)$	(9,6)
$\mathbb{Z}_{3^3}$	$(1,1,0)$	(6,3)	$(2,0,0)$	(13,2)	$(1,2,0)$	(12,4)	$(1,2,1)$	(13,5)
			$(1,1,1)$	(7,4)	$(2,0,1)$	(14,3)	$(2,0,2)$	(15,4)
					$(1,1,2)$	(8,5)	$(2,1,0)$	(25,3)
							$(1,1,3)$	(9,6)
$\mathbb{Z}_{3^4}$			$(1,0,1,0)$	(7,4)	$(1,1,0,0)$	(14,3)	$(1,0,2,0)$	(13,5)
					$(1,0,1,1)$	(8,5)	$(1,1,0,1)$	(15,4)
							$(2,0,0,0)$	(14,2)
							$(1,0,1,2)$	(9,6)
$\mathbb{Z}_{3^5}$					$(1,0,0,1,0)$	(8,5)	$(1,0,1,0,0)$	(15,4)
							$(1,0,0,1,1)$	(9,6)
$\mathbb{Z}_{3^6}$							$(1,0,0,0,1,0)$	(9,6)

Known partial classification

Let $X_{t,s,p} = |\{(t_1, \ldots, t_s) \in \mathbb{N}^s : t = \left(\sum_{i=1}^{s} (s-i+1) \cdot t_i \right) - 1, \; t_1 \geq 1\}|$.

Let $\mathcal{A}_{t,s,p}$ be the number of nonequivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t and $s \geq 2$.

Let $\mathcal{A}_{t,p}$ be the number of nonequivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t.

Theorem (DFV22)

For $t \geq 3$ and $p \geq 3$ prime,

$$\mathcal{A}_{t,p} \leq 1 + \sum_{s=2}^{t-1} (X_{t,s,p} - 1) \tag{1}$$

and

$$\mathcal{A}_{t,p} \leq 1 + \sum_{s=2}^{t-1} (\mathcal{A}_{t,s,p} - 1). \tag{2}$$

Outline

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

$\mathbb{Z}_{3^s}$	$t=4$		$t=5$		$t=6$		$t=7$	
	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)	$(t_1,\dots,t_s)$	(r,k)
$\mathbb{Z}_{3^2}$	$(2,1)$	(6,3)	$(2,2)$ $(3,0)$	(7,4) (11,3)	$(3,1)$ $(2,3)$	(12,4) (8,5)	$(3,2)$ $(4,0)$ $(2,4)$	(13,5) (21,4) (9,6)
$\mathbb{Z}_{3^3}$	$(1,1,0)$	(6,3)	$(2,0,0)$ $(1,1,1)$	(13,2) (7,4)	$(1,2,0)$ $(2,0,1)$ $(1,1,2)$	(12,4) (14,3) (8,5)	$(1,2,1)$ $(2,0,2)$ $(2,1,0)$ $(1,1,3)$	(13,5) (15,4) (25,3) (9,6)
$\mathbb{Z}_{3^4}$			$(1,0,1,0)$	(7,4)	$(1,1,0,0)$ $(1,0,1,1)$	(14,3) (8,5)	$(1,0,2,0)$ $(1,1,0,1)$ $(2,0,0,0)$ $(1,0,1,2)$	(13,5) (15,4) (14,2) (9,6)
$\mathbb{Z}_{3^5}$					$(1,0,0,1,0)$	(8,5)	$(1,0,1,0,0)$ $(1,0,0,1,1)$	(15,4) (9,6)
$\mathbb{Z}_{3^6}$							$(1,0,0,0,1,0)$	(9,6)

Theorem

Let $s \geq 2$ and $t_s \geq 1$. The $\mathbb{Z}_{p^s}$-linear GH code $H^{t_1,\dots,t_s}$ is permutation equivalent to the $\mathbb{Z}_{p^{s+\ell}}$-linear GH code $H^{1,\mathbf{0}^{\ell-1},t_1-1,t_2,\dots,t_{s-1},t_s-\ell}$, for all $\ell \in \{1,\dots,t_s\}$.

Let $t_1, t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 2$, or $t_1 = 1$ and $s = 2$.

Let $C_p(t_1, \ldots, t_s) = [H_1 = H^{t_1,\ldots,t_s}, H_2, \ldots, H_\rho]$ be the sequence of all $\mathbb{Z}_{p^{s'}}$-linear GH codes of length p^t, where $t = (\sum_{i=1}^{s'} (s' - i + 1) \cdot t_i) - 1$, that are permutation equivalent to $H^{t_1,\ldots,t_s}$. We refer to $C_p(t_1, \ldots, t_s)$ as the chain of equivalences of $H_p^{t_1,\ldots,t_s}$.

We denote by $C_p(t_1, \ldots, t_s)[i]$ the ith code H_i in the sequence, for $1 \leq i \leq t_s + 1$:

$$C_p(t_1, \ldots, t_s)[i] = \begin{cases} H^{t_1,\ldots,t_s} & \text{if } i = 1, \\ H^{1,\mathbf{0}^{i-2},t_1-1,t_2,\ldots,t_{s-1},t_s-i+1} & \text{otherwise.} \end{cases}$$

Example

- $C_3(2,4) = [H^{2,4}, H^{1,1,3}, H^{1,0,1,2}, H^{1,0,0,1,1}, H^{1,0,0,0,1,0}]$
- $C_3(2,0,3) = [H^{2,0,3}, H^{1,1,0,2}, H^{1,0,1,0,1}, H^{1,0,0,1,0,0}]$

Corollary

For $t_1 \geq 2$, or $t_1 = 1$ and $s = 2$, we have $|C_p(t_1, \ldots, t_s)| = t_s + 1$.

Theorem

Let $H = H^{t_1,\dots,t_s}$, be a $\mathbb{Z}_{p^s}$-linear GH code with p prime, and $\sigma = o(H)$. Let $\ell \in \{1,\dots,s-1\}$ such that $H = H^{t_1,\mathbf{0}^{\ell-1},t_{\ell+1},\dots,t_s}$, where $t_{\ell+1} \neq 0$ if $\ell < s-1$. Then, H belongs to a unique chain of equivalences, and it satisfies one of the following conditions:

1. *if $t_1 \geq 2$, then $\sigma = 1$ and $H = C_p(t_1,\dots,t_s)[1]$.*
2. *if $t_1 = 1$ and $\ell = s-1$, then $\sigma = s$ and $H = C_p(1, t_s + \ell - 1)[\sigma - 1]$.*
3. *if $t_1 = 1$ and $\ell < s-1$, then $\sigma = \ell + 1$ and $H = C_p(t'_1,\dots,t'_{s'})[\sigma]$, where $(t'_1,\dots,t'_{s'}) = (t_\sigma + 1, t_{\sigma+1},\dots,t_{s-1}, t_s + \sigma - 1)$ and $s' = s - \sigma + 1$.*

Example

- $H^{3,1,1} = C_3(3,1,1)[1]$,
- $H^{1,0,0,2,1,2} = C_3(3,1,5)[4]$, $\ell = 3$, $s = 6$, $\sigma = 4$.

Outline

Improvement of the known partial classification

Corollary

Let $H^{t_1,\ldots,t_s}$ *be a* **nonlinear** $\mathbb{Z}_{p^s}$*-linear GH code with* p *prime, and* $\sigma = o(H^{t_1,\ldots,t_s})$*. Then,* $H^{t_1,\ldots,t_s}$ *is permutation equivalent to* $t_s + \sigma$ $\mathbb{Z}_{p^{s'}}$*-linear GH codes, for* $s' \in \{s+1-\sigma, \ldots, s+t_s\}$*. Among them, there is exactly one* $H^{t'_1,\ldots,t'_{s'}}$ *with* $t'_1 \geq 2$*, and there is exactly one* $H^{t'_1,\ldots,t'_{s'}}$ *with* $t'_{s'} = 0$*.*

Corollary

Let H *be a* **nonlinear** $\mathbb{Z}_{p^s}$*-linear GH code of length* p^t *with* p *prime. If* $s \in \{\lfloor (t+1)/2 \rfloor + 1, \ldots, t+1\}$*, then there is a permutation equivalent* $\mathbb{Z}_{p^{s'}}$*-linear GH code of length* p^t *with* $s' \in \{2, \ldots, \lfloor (t+1)/2 \rfloor\}$*.*

Let $\tilde{X}_{t,s,p} = |\{(t_1,\ldots,t_s) \in \mathbb{N}^s : t = \left(\sum_{i=1}^{s}(s-i+1)t_i\right) - 1,\ \mathbf{t_1 \geq 2}\}|$.

Theorem

For all $t \geq 3$ and p prime,

$$\mathcal{A}_{t,p} \leq 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} \tilde{X}_{t,s,p} \tag{3}$$

and

$$\mathcal{A}_{t,p} \leq 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} (\mathcal{A}_{t,s,p} - 1). \tag{4}$$

Moreover, for any $3 \leq t \leq 11$ if $p = 2$, any $3 \leq t \leq 10$ if $p = 3$, and any $3 \leq t \leq 8$ if $p = 5$, the upper bound (3) is tight.

t	3	4	5	6	7	8	9	10
previous lower bound (r, k)	**2**	**2**	**4**	**4**	**7**	**8**	**12**	**14**
new upper bound (3)	**2**	**2**	**4**	**4**	**7**	**8**	**12**	**14**
new upper bound (4)	2	2	5	6	11	15	26	33
previous upper bounds (1) and (2)	2	2	6	9	15	22	33	46

Table 1: Bounds for the number $\mathcal{A}_{t,3}$ of nonequivalent $\mathbb{Z}_{3^s}$-linear GH codes of length 3^t for $3 \leq t \leq 10$.

t	3	4	5	6	7	8
previous lower bound (r, k)	**2**	**2**	**4**	**4**	**7**	**8**
new upper bound (3)	**2**	**2**	**4**	**4**	**7**	**8**
new upper bound (4)	2	2	5	6	11	15
previous upper bounds (1) and (2)	2	2	6	9	15	22

Table 2: Bounds for the number $\mathcal{A}_{t,5}$ of nonequivalent $\mathbb{Z}_{5^s}$-linear GH codes of length 5^t for $3 \leq t \leq 8$.

Conclusion and Future research

- For any $3 \leq t \leq 11$ if $p = 2$, any $3 \leq t \leq 10$ if $p = 3$, and any $3 \leq t \leq 8$ if $p = 5$, codes with the same value of (r, k) are equivalent and the upper bound (3) is tight.
- Future research: Determine the rank of the $\mathbb{Z}_{p^s}$-linear GH codes, and try to use it to classify them for some values of p and s.
- Conjecture: $\mathbb{Z}_{p^s}$-linear GH codes having the same pair (r, k) are in the same chain and are equivalent codes.

Thank you!