

On the equivalence of \mathbb{Z}_{p^s} -linear generalized Hadamard codes

Dipak K. Bhunia¹ · Cristina Fernández-Córdoba¹ · Carlos Vela² · Mercè Villanueva¹

Received: 13 November 2022 / Revised: 13 October 2023 / Accepted: 16 October 2023 © The Author(s) 2023

Abstract

Linear codes of length n over \mathbb{Z}_{p^s} , p prime, called \mathbb{Z}_{p^s} -additive codes, can be seen as subgroups of $\mathbb{Z}_{p^s}^n$. A \mathbb{Z}_{p^s} -linear generalized Hadamard (GH) code is a GH code over \mathbb{Z}_p which is the image of a \mathbb{Z}_{p^s} -additive code under a generalized Gray map. It is known that the dimension of the kernel allows to classify these codes partially and to establish some lower and upper bounds on the number of such codes. Indeed, in this paper, for $p \geq 3$ prime, we establish that some \mathbb{Z}_{p^s} -linear GH codes of length p^t having the same dimension of the kernel are equivalent to each other, once t is fixed. This allows us to improve the known upper bounds. Moreover, up to t = 10 if p = 3 or t = 8 if t = 5, this new upper bound coincides with a known lower bound based on the rank and dimension of the kernel.

Keywords Generalized Hadamard code \cdot Gray map $\cdot \mathbb{Z}_{p^s}$ -linear code \cdot Rank \cdot Kernel \cdot Classification

Mathematics Subject Classification 94B25 · 94B60

Communicated by V. D. Tonchev.

The material in this paper was presented in part at the international conference Algebraic and Combinatorial Methods for Coding and Cryptography (ALCOCRYPT), 20–24 February 2023, Marseille, France.

This work has been partially supported by the Spanish Ministerio de Ciencia e Innovación under Grants PID2019-104664GB-I00, PID2022-137924NB-I00, and RED2022-134306-T (AEI / 10.13039/501100011033); by the Catalan AGAUR scholarship 2020 FI SDUR 00475 and Grant 2021 SGR 00643; and by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UIDB/04106/2020.

☑ Dipak K. Bhunia dipak.bhunia@uab.cat

Published online: 18 November 2023

Extended author information available on the last page of the article



1 Introduction

Let \mathbb{Z}_{p^s} be the ring of integers modulo p^s with p prime and $s \geq 1$. Let $\mathbb{Z}_{p^s}^n$ be the set of n-tuples over \mathbb{Z}_{p^s} . In this paper, the elements of $\mathbb{Z}_{p^s}^n$ will also be called *vectors*. The *order* of a vector \mathbf{u} over \mathbb{Z}_{p^s} , denoted by $o(\mathbf{u})$, is the smallest positive integer m such that $m\mathbf{u}=(0,\ldots,0)$. A *code over* \mathbb{Z}_p of length n is a nonempty subset of \mathbb{Z}_p^n , and it is called *linear* if it is a subspace of \mathbb{Z}_p^n . Similarly, a nonempty subset of $\mathbb{Z}_{p^s}^n$ is a \mathbb{Z}_{p^s} -additive code if it is a subgroup of $\mathbb{Z}_{p^s}^n$. When p=2 and s=1, a \mathbb{Z}_{p^s} -additive code is a binary linear code and, when p=2 and s=2, it is a quaternary linear code or a linear code over \mathbb{Z}_4 .

The usual Gray map ϕ from \mathbb{Z}_4 to \mathbb{Z}_2^2 , that is, the map such that $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$ and $\phi(3) = (1,0)$ [14], has been generalized to different maps, which go from \mathbb{Z}_{p^s} to $\mathbb{Z}_p^{p^{s-1}}$ [4, 8, 9, 13, 17, 19, 25]. In this paper, we consider the following generalization of Carlet's Gray map [13]:

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

where $u \in \mathbb{Z}_{p^s}$, $[u_0, u_1, \dots, u_{s-1}]_p$ is the p-ary expansion of u, that is, $u = \sum_{i=0}^{s-1} p^i u_i$ $(u_i \in \mathbb{Z}_p)$, and Y_{s-1} is a $(s-1) \times p^{s-1}$ matrix whose columns are all the different elements of \mathbb{Z}_p^{s-1} . We assume, without loss of generality, that the columns of Y_{s-1} are ordered in ascending order, by considering them as the p-ary expansions of the elements of the ring $\mathbb{Z}_{p^{s-1}}$. Then, we define $\Phi_s : \mathbb{Z}_p^n \to \mathbb{Z}_p^{np^{s-1}}$ as the component-wise Gray map ϕ_s .

Let \mathcal{C} be a \mathbb{Z}_{p^s} -additive code of length n. The Gray map image of \mathcal{C} , $\mathcal{C} = \Phi_s(\mathcal{C})$, is called a \mathbb{Z}_{p^s} -linear code. Note that the length of \mathcal{C} is $p^{s-1}n$. As a subgroup of $\mathbb{Z}_{p^s}^n$, \mathcal{C} is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_p^{t_s}$, and we say that \mathcal{C} , or equivalently $\mathcal{C} = \Phi_s(\mathcal{C})$, is of type $(n; t_1, \ldots, t_s)$. Note that $|\mathcal{C}| = p^{st_1} p^{(s-1)t_2} \cdots p^{t_s}$. A \mathbb{Z}_{p^s} -additive code \mathcal{C} can also be seen as a \mathbb{Z}_{p^s} -submodule of $\mathbb{Z}_{p^s}^n$. As a \mathbb{Z}_{p^s} -module, \mathcal{C} is free only if it is of type $(n; t_1, 0, \ldots, 0)$. For linear codes over rings which are not free, there does not exist a basis. However, for any linear code over \mathbb{Z}_{p^s} , there does exist a generator matrix having minimum number of rows, that is, with $t_1 + \cdots + t_s$ rows. Note that the rows of this generator matrix contain t_i codewords of order p^{s-i+1} , for $i \in \{1, \ldots, s\}$.

Let S_n be the symmetric group of permutations on the set $\{1, \ldots, n\}$. Two \mathbb{Z}_{p^s} -additive codes of length n, C_1 and C_2 , are permutation equivalent if there is a permutation of coordinates $\pi \in S_n$ such that $C_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in C_1\}$. Two codes of length n over \mathbb{Z}_p , C_1 and C_2 , are equivalent if there is a vector $\mathbf{a} \in \mathbb{Z}_p^n$ and a permutation of coordinates $\pi \in S_n$ such that $C_2 = \{\mathbf{a} + \pi(\mathbf{c}) : \mathbf{c} \in C_1\}$.

Let C be a code over \mathbb{Z}_p . The *rank* of C is the dimension of its linear span, $\langle C \rangle$, and it is denoted by $\operatorname{rank}(C)$. The *kernel* of C is $\operatorname{K}(C) = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x} + C = C\}$ [2, 20], and its dimension is denoted by $\operatorname{ker}(C)$. If the all-zero vector belongs to C, then $\operatorname{K}(C)$ is a linear subcode of C. Note also that if C is linear, then $\operatorname{K}(C) = C = \langle C \rangle$. The values of $\operatorname{rank}(C)$ and $\operatorname{ker}(C)$ can be used to distinguish between nonequivalent codes over \mathbb{Z}_p , since equivalent ones have the same rank and dimension of the kernel.

A generalized Hadamard (GH) matrix $H(p, \lambda) = (h_{ij})$ of order $n = p\lambda$ over \mathbb{Z}_p is a $p\lambda \times p\lambda$ matrix with entries from \mathbb{Z}_p with the property that for every $i, j, 1 \le i < j \le p\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \le s \le p\lambda\}$ contains every element of \mathbb{Z}_p exactly λ times [15]. An ordinary Hadamard matrix of order 4μ corresponds to a GH matrix $H(2, \lambda)$ over \mathbb{Z}_2 , where $\lambda = 2\mu$ [1]. Two GH matrices H_1 and H_2 of order n are said to be 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 or in a 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*. Let H be a normalized GH matrix. We also denote by H the set of rows of H. The code $C_H = \bigcup_{\alpha \in \mathbb{Z}_p} (H + \alpha \mathbf{1})$, where $H + \alpha \mathbf{1} = \{\mathbf{h} + \alpha \mathbf{1} : \mathbf{h} \in H\}$ and $\mathbf{1}$ denotes the all-one vector, is called *generalized Hadamard* (GH) code [10]. Note that C_H is generally a nonlinear code over \mathbb{Z}_p . If C is a \mathbb{Z}_{p^s} -additive code such that $\Phi_s(C)$ is a GH code, then we say that C is a \mathbb{Z}_{p^s} -additive GH code and $\Phi_s(C)$ is a \mathbb{Z}_{p^s} -linear GH code. Note that a GH code over \mathbb{Z}_p of length N has pN codewords and minimum distance N(p-1)/p.

GH matrices over \mathbb{Z}_p are also known as Butson Hadamard matrices, introduced in [5], since p is prime. They can also be seen as square difference matrices. Difference matrices, introduced in [6], are matrices whose elements belong to a finite group, such that in the difference of two distinct row vectors each element of the group occurs equally often. In [23], three different constructions of difference matrices (the direct method, the iterative procedure and the Kronecker product construction) were considered. They also studied the codes induced by these matrices, and showed that these codes are optimal. In [27], binary Hadamard codes obtained by using a general concatenation construction given in [28] are studied. Unlike the \mathbb{Z}_{p^s} -linear GH codes, the codes from [27] come from codes over \mathbb{Z}_q which are not necessarily linear, after applying not necessarily the same generalized Gray map in each coordinate.

Let $A_{t,s,p}$ and $A_{t,p}$ be the number of nonequivalent \mathbb{Z}_{p^s} -linear GH codes of length p^t , when both t and s are fixed, and when just t is fixed, respectively. The \mathbb{Z}_4 -linear Hadamard codes of length 2^t can be classified by using either the rank or the dimension of the kernel [16, 21]. There are exactly $A_{t,2,2} = \lfloor \frac{t-1}{2} \rfloor$ nonequivalent such codes for all $t \geq 2$. In [11], it is proved that the dimension of the kernel for \mathbb{Z}_{2^s} -linear Hadamard codes provides a complete classification giving $A_{t,s,2}$ for all values of t and s, except for $t \geq 8$ and $s \leq s \leq t - 5$. This partial classification is improved in [3], by giving $A_{t,s,2}$ also for any $s \leq t \leq 1$ and $s \geq 2$. In [12], for $s \geq 2$, it is established that some \mathbb{Z}_{2^s} -linear Hadamard codes of length $s \geq 2$ are equivalent, once only $s \geq 2$ is fixed, and this fact improved the known upper bounds for $s \geq 2$. Moreover, the authors showed that, up to $s \geq 1$, this new upper bound coincides with the known lower bound (based on the rank and dimension of the kernel).

For s > 2 and p > 3 prime, an iterative construction and the dimension of the kernel for \mathbb{Z}_{p^s} -linear GH codes of length p^t are established in [3], and it is also proved that this invariant only provides a complete classification for certain values of t and s. Lower and upper bounds are also established for $A_{t,s,p}$ and $A_{t,p}$. From [3], we can observe that there are nonlinear codes having the same rank and dimension of the kernel for different values of s, once the length p^t is fixed, at least for all $4 \le t \le 10$ if p = 3 and $4 \le t \le 8$ if p = 5. In this paper, we show that, for all $t \ge 4$ and $p \ge 3$ prime, some \mathbb{Z}_{p^s} -linear GH codes of length p^t having different values of s are permutation equivalent to each other, once t is fixed. Moreover, for all $t \le 10$ if p = 3 and $t \le 8$ if p = 5, the codes that are permutation equivalent are, in fact, those having the same pair of invariants, rank and dimension of the kernel. For example, in Table 3, the codes in bold type have the same rank and dimension of the kernel and are, in fact, permutation equivalent. These results allow us to obtain a more accurate classification of the \mathbb{Z}_{p^s} -linear GH codes, than the one given in [3]. \mathbb{Z}_{p^s} -additive codes have also been studied in [24, 26] as two-weight codes over \mathbb{Z}_{p^s} by considering the homogeneous weight. Recently, rank and pairs of rank and dimension of the kernel for $\mathbb{Z}_p\mathbb{Z}_{p^2}$ -linear codes have been studied in [18].

The paper is organized as follows. In Sect. 2, we recall the recursive construction of \mathbb{Z}_{p^s} -linear GH codes, the known partial classification, and some bounds on the number of nonequivalent such codes, presented in [3]. In Sect. 3, we prove some equivalence relations among the \mathbb{Z}_{p^s} -linear GH codes of the same length p^t . Later, in Sect. 4, we improve the



classification given in [3] by refining the known bounds. Finally, in Sect. 5, we give some conclusions and further research on this topic.

2 Preliminaries and known partial classification

In this section, we provide some known results for \mathbb{Z}_{p^s} -linear GH codes of length p^t with $t \geq 3$ and p prime. These results were presented mainly in [3, 11, 12] and are related to the recursive construction, partial classification, and bounds on the number of such nonequivalent codes.

Let $T_i = \{j \cdot p^{i-1} : j \in \{0, 1, \dots, p^{s-i+1} - 1\}\}$ for all $i \in \{1, \dots, s\}$. Note that $T_1 = \{0, \dots, p^s - 1\}$. Let t_1, t_2, \dots, t_s be nonnegative integers with $t_1 \ge 1$. Consider the matrix $A_p^{t_1, \dots, t_s}$ whose columns are exactly all the vectors of the form \mathbf{z}^T , $\mathbf{z} \in \{1\} \times T_1^{t_1-1} \times T_2^{t_2} \times \dots \times T_s^{t_s}$. Let $\mathbf{0}, \mathbf{1}, \mathbf{2}, \dots, \mathbf{p}^s - \mathbf{1}$ be the vectors having the same element $0, 1, 2, \dots, p^s - 1$ from \mathbb{Z}_{p^s} in all its coordinates, respectively.

Any matrix $A_p^{t_1,\ldots,t_s}$ can also be obtained by applying the following recursive construction. We start with $A_p^{1,0,\ldots,0}=(1)$. Then, if we have a matrix $A=A_p^{t_1,\ldots,t_s}$, for any $i\in\{1,\ldots,s\}$, we may construct the matrix

$$A_i = \begin{pmatrix} A & A & \cdots & A \\ p^{i-1} \cdot \mathbf{0} & p^{i-1} \cdot \mathbf{1} & \cdots & p^{i-1} \cdot (\mathbf{p^{s-i+1}} - \mathbf{1}) \end{pmatrix}.$$
 (2)

Finally, permuting the rows of A_i , we obtain a matrix $A_p^{t_1',\dots,t_s'}$, where $t_j'=t_j$ for $j\neq i$ and $t_i'=t_i+1$. Note that any permutation of columns of A_i gives also a matrix $A_p^{t_1',\dots,t_s'}$. Along this paper, we consider that the matrices $A_p^{t_1,\dots,t_s}$ are constructed recursively starting from $A_p^{1,0,\dots,0}$ in the following way. First, we add t_1-1 rows of order p^s , up to obtain $A_p^{t_1,0,\dots,0}$; then t_2 rows of order p^{s-1} up to generate $A_p^{t_1,t_2,\dots,0}$; and so on, until we add t_s rows of order p to achieve $A_p^{t_1,\dots,t_s}$. See [3] for examples.

Let $\mathcal{H}_p^{t_1,\dots,t_s}$ be the \mathbb{Z}_{p^s} -additive code of type $(n;t_1,\dots,t_s)$ generated by the matrix $A_p^{t_1,\dots,t_s}$, where t_1,\dots,t_s are nonnegative integers with $t_1 \geq 1$ and p prime. Let $n=p^{t-s+1}$, where $t=\left(\sum_{i=1}^s(s-i+1)\cdot t_i\right)-1$. The code $\mathcal{H}_p^{t_1,\dots,t_s}$ has length n, and the corresponding \mathbb{Z}_{p^s} -linear code $H_p^{t_1,\dots,t_s} = \Phi_s(\mathcal{H}_p^{t_1,\dots,t_s})$ is a GH code of length p^t [3].

In order to classify the \mathbb{Z}_{p^s} -linear GH codes of length p^t , we can focus on $t \geq 5$ and $2 \leq s \leq t-2$ when p=2 [11], and on $t \geq 4$ and $2 \leq s \leq t-1$ when $p \geq 3$ prime [3]. Moreover, as shown in the following three theorems, for any $t \geq 5$ and $2 \leq s \leq t-2$, there are two \mathbb{Z}_{2^s} -linear Hadamard codes of length 2^t which are linear; and for any $t \geq 4$, $2 \leq s \leq t-1$ and $p \geq 3$ prime, there is a unique \mathbb{Z}_{p^s} -linear GH code of length p^t which is linear.

Theorem 1 [16] The codes H_2^{1,t_2} and H_2^{2,t_2} , with $t_2 \ge 0$, are the only \mathbb{Z}_4 -linear Hadamard codes which are linear over \mathbb{Z}_2 .

Theorem 2 [11] The codes $H_2^{1,0,\ldots,0,t_s}$ and $H_2^{1,0,\ldots,0,1,t_s}$, with s > 2 and $t_s \ge 0$, are the only \mathbb{Z}_{2^s} -linear Hadamard codes which are linear over \mathbb{Z}_2 .

Theorem 3 [3] The \mathbb{Z}_{p^s} -linear GH codes $H_p^{1,0,\dots,0,t_s}$, with $p \geq 3$ prime, $s \geq 2$ and $t_s \geq 0$, are the only \mathbb{Z}_{p^s} -linear GH codes which are linear over \mathbb{Z}_p .



Table 1 All linear \mathbb{Z}_{2^s} -linear GH codes of length 2^t and dimension $t + t$. 1	
---	-----	--

	$t=4 (t_1,\ldots,t_s)$	$t=5 (t_1,\ldots,t_s)$	$t = 6$ (t_1, \dots, t_s)	$t = 7$ (t_1, \ldots, t_s)
\mathbb{Z}_4	(1, 3)	(1, 4)	(1, 5)	(1, 6)
	(2, 1)	(2, 2)	(2, 3)	(2, 4)
\mathbb{Z}_{2^3}	(1, 0, 2)	(1, 0, 3)	(1, 0, 4)	(1, 0, 5)
_	(1, 1, 0)	(1, 1, 1)	(1, 1, 2)	(1, 1, 3)
\mathbb{Z}_{2^4}	(1, 0, 0, 1)	(1, 0, 0, 2)	(1, 0, 0, 3)	(1, 0, 0, 4)
-		(1, 0, 1, 0)	(1, 0, 1, 1)	(1, 0, 1, 2)
\mathbb{Z}_{2^5}	(1, 0, 0, 0, 0)	(1, 0, 0, 0, 1)	(1, 0, 0, 0, 2)	(1, 0, 0, 0, 3)
-			(1, 0, 0, 1, 0)	(1, 0, 0, 1, 1)
\mathbb{Z}_{2^6}		(1, 0, 0, 0, 0, 0)	(1, 0, 0, 0, 0, 1)	(1, 0, 0, 0, 0, 2)
-				(1, 0, 0, 0, 1, 0)
\mathbb{Z}_{2^7}			(1, 0, 0, 0, 0, 0, 0)	(1, 0, 0, 0, 0, 0, 1)
\mathbb{Z}_{2^8}				(1, 0, 0, 0, 0, 0, 0, 0, 0)

Table 2 All linear \mathbb{Z}_{p^s} -linear GH codes of length p^t with $p \geq 3$ prime and dimension t+1

	$t = 4$ (t_1, \ldots, t_s)	$t = 5$ (t_1, \dots, t_s)	$t = 6$ (t_1, \dots, t_s)	$t = 7$ (t_1, \dots, t_s)
\mathbb{Z}_{p^2}	(1, 3)	(1, 4)	(1, 5)	(1, 6)
\mathbb{Z}_{p^3}	(1, 0, 2)	(1, 0, 3)	(1, 0, 4)	(1, 0, 5)
\mathbb{Z}_{p^4}	(1, 0, 0, 1)	(1, 0, 0, 2)	(1, 0, 0, 3)	(1, 0, 0, 4)
\mathbb{Z}_{p^5}	(1, 0, 0, 0, 0)	(1, 0, 0, 0, 1)	(1, 0, 0, 0, 2)	(1, 0, 0, 0, 3)
\mathbb{Z}_{p^6}		(1, 0, 0, 0, 0, 0)	(1, 0, 0, 0, 0, 1)	(1, 0, 0, 0, 0, 2)
\mathbb{Z}_{p^7}			(1, 0, 0, 0, 0, 0, 0)	(1, 0, 0, 0, 0, 0, 1)
\mathbb{Z}_{p^8}				(1, 0, 0, 0, 0, 0, 0, 0)

Tables 1 and 2 show the values of t_1, \ldots, t_s for all linear \mathbb{Z}_{p^s} -linear GH codes $H_p^{t_1, \ldots, t_s}$ of length p^t with $4 \le t \le 7$ and p prime, given by Theorems 1, 2, and 3. Note that the case p = 2 is different from the case $p \ge 3$ prime.

Tables 3 and 4, for $4 \le t \le 10$ and $2 \le s \le t - 1$, show all possible values of (t_1, \ldots, t_s) for which there exists a nonlinear \mathbb{Z}_{p^s} -linear GH code $H_p^{t_1, \ldots, t_s}$ of length p^t with $p \ge 3$ prime. For each one of them, taking p = 3, the values (r, k) are shown, where r is the rank (computed by using the computer algebra system Magma [7, 22]) and k is the dimension of the kernel (determined in [3]). Note that the values of k are the same for any k is prime, but the values of k are only given for k and k is the dimension of the kernel given in these tables, it is easy to see that this invariant does not always give a classification. For example, in Table 4, for k and k there are two k and k are GH codes with the same dimension of the kernel, k and k are nonequivalent since they have different rank, k and k are 16. On the other hand, considering only the values of the rank given in these tables, it is easy to note that the rank does give a classification, since all the codes have different values of the rank, once k and k are fixed, at least when k and k and k are fixed, at least when k and k are 10 and k and k are fixed, at least when k and k are 10 and k are fixed, at least when k and k are 10 and k are fixed, at least when k and k are 10 and k are fixed, at least when k are fixed.



	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}_9	(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)	(34,2)	
							(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}_{36}							(1, 0, 0, 0, 1, 0)	(9,6)	

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

Similarly, Table 5 shows that this also happens for p = 5 when $4 \le t \le 8$; and Tables 1 and 3 given in [11] show that it is also true for p = 2 when $4 \le t \le 11$.

Let $X_{t,s,p}$ be the number of nonnegative integer solutions $(t_1, \ldots, t_s) \in \mathbb{N}^s$ of the equation $t = \left(\sum_{i=1}^s (s-i+1) \cdot t_i\right) - 1$ with $t_1 \geq 1$. This gives the number of sequences (t_1, \ldots, t_s) such that $H_p^{t_1, \ldots, t_s}$ is a \mathbb{Z}_{p^s} -linear GH codes of length p^t . Let $\mathcal{A}_{t,s,p}$ be the number of nonequivalent \mathbb{Z}_{p^s} -linear GH codes of length p^t and a fixed $s \geq 2$. Then, for any $t \geq 5$ and $1 \leq s \leq t-1$, we have that $1 \leq t-1$, we have that $1 \leq t-1$ and $1 \leq t-1$, we have that $1 \leq t-1$ and $1 \leq t-1$, we have that $1 \leq t-1$ and $1 \leq t-1$ are there is exactly one code which is linear. Moreover, these bounds are tight for $1 \leq t-1$ if $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t-1$ are $1 \leq t-1$ and $1 \leq t$

A partial classification for the \mathbb{Z}_{p^s} -linear GH codes of length p^t is given for p=2 in [11], and for $p\geq 3$ prime in [3]. Specifically, lower and upper bounds on the number of nonequivalent such codes, once only t is fixed, are established. Let $\mathcal{A}_{t,p}$ be the number of nonequivalent \mathbb{Z}_{p^s} -linear GH codes of length p^t . We first consider the case p=2.

Theorem 4 [11] *For* $t \ge 3$,

$$A_{t,2} \le 1 + \sum_{s=2}^{t-2} (X_{t,s,2} - 2) \tag{3}$$

and

$$A_{t,2} \le 1 + \sum_{s=2}^{t-2} (A_{t,s,2} - 1).$$
 (4)

The upper bounds (3) and (4) on $A_{t,2}$ are improved in [12], where it is proved that, for a fixed t, there are \mathbb{Z}_{2^s} -linear Hadamard codes of length 2^t that are equivalent. It is also



Table 4 Rank and kernel for all nonlinear \mathbb{Z}_{3^s} -linear GH codes of length 3^t

	t = 8		t = 9		t = 10	
	(t_1,\ldots,t_s)	(r,k)	(t_1,\ldots,t_s)	(r,k)	(t_1,\ldots,t_s)	(r,k)
\mathbb{Z}_9	(3, 3)	(14,6)	(3, 4)	(15,7)	(3, 5)	(16,8)
	(4, 1)	(22,5)	(4, 2)	(23,6)	(4, 3)	(24,7)
	(2, 5)	(10,7)	(5,0)	(36,5)	(5, 1)	(37,6)
			(2, 6)	(11,8)	(2, 7)	(12,9)
\mathbb{Z}_{3^3}	(1, 2, 2)	(14,6)	(1, 2, 3)	(15,7)	(1, 2, 4)	(16,8)
	(1, 3, 0)	(22,5)	(1, 3, 1)	(23,6)	(1, 3, 2)	(24,7)
	(2, 0, 3)	(16,5)	(2, 0, 4)	(17,6)	(1, 4, 0)	(37,6)
	(2, 1, 1)	(26,4)	(2, 1, 2)	(27,5)	(2, 0, 5)	(18,7)
	(3, 0, 0)	(48,3)	(2, 2, 0)	(43,4)	(2, 1, 3)	(28,6)
	(1, 1, 4)	(10,7)	(3, 0, 1)	(49,4)	(2, 2, 1)	(44,5)
			(1, 1, 5)	(11,8)	(3, 0, 2)	(50,5)
					(3, 1, 0)	(82,4)
					(1, 1, 6)	(12,9)
\mathbb{Z}_{3^4}	(1, 0, 2, 1)	(14,6)	(1, 0, 2, 2)	(15,7)	(1, 0, 2, 3)	(16,8)
	(1, 1, 0, 2)	(16,5)	(1, 0, 3, 0)	(23,6)	(1, 0, 3, 1)	(24,7)
	(1, 1, 1, 0)	(26,4)	(1, 2, 0, 0)	(49,4)	(1, 1, 0, 4)	(18,7)
	(2, 0, 0, 1)	(35,3)	(1, 1, 0, 3)	(17,6)	(1, 1, 1, 2)	(28,6)
	(1, 0, 1, 3)	(10,7)	(1, 1, 1, 1)	(27,5)	(1, 1, 2, 0)	(44,5)
			(2, 0, 0, 2)	(36,4)	(1, 2, 0, 1)	(50,5)
			(2, 0, 1, 0)	(64,3)	(2, 0, 0, 3)	(37,5)
			(1, 0, 1, 4)	(11,8)	(2, 0, 1, 1)	(65,4)
					(2, 1, 0, 0)	(121,3)
					(1, 0, 1, 5)	(12,9)
\mathbb{Z}_{3^5}	(1, 0, 0, 2, 0)	(14,6)	(1, 0, 0, 2, 1)	(15,7)	(1, 0, 0, 2, 2)	(16,8)
	(1, 0, 1, 0, 1)	(16,5)	(1, 0, 1, 0, 2)	(17,6)	(1, 0, 0, 3, 0)	(24,7)
	(1, 1, 0, 0, 0)	(35,3)	(1, 0, 1, 1, 0)	(27,5)	(1, 0, 1, 0, 3)	(18,7)
	(1, 0, 0, 1, 2)	(10,7)	(1, 1, 0, 0, 1)	(36,4)	(1, 0, 1, 1, 1)	(28,6)
			(2, 0, 0, 0, 0)	(96,2)	(1, 0, 2, 0, 0)	(50,5)
			(1, 0, 0, 1, 3)	(11,8)	(1, 1, 0, 0, 2)	(37,5)
					(1, 1, 0, 1, 0)	(65,4)
					(2, 0, 0, 0, 1)	(97,3)
					(1, 0, 0, 1, 4)	(12,9)
\mathbb{Z}_{36}	(1, 0, 0, 1, 0, 0)	(16,5)	(1, 0, 0, 0, 2, 0)	(15,7)	(1, 0, 0, 0, 2, 1)	(16,8)
-	(1, 0, 0, 0, 1, 1)	(10,7)	(1,0,0,1,0,1)	(17,6)	(1, 0, 0, 1, 0, 2)	(18,7)
			(1, 0, 1, 0, 0, 0)	(36,4)	(1, 0, 0, 1, 1, 0)	(28,6)



_							
12	n	ιΔ /	LC	On	tin	med	ı

	t = 8		t = 9		t = 10			
	(t_1,\ldots,t_s)	(r, k)	(t_1,\ldots,t_s)	(r, k)	(t_1,\ldots,t_s)	(r, k)		
			(1, 0, 0, 0, 1, 2)	(11,8)	(1, 0, 1, 0, 0, 1)	(37,5)		
					(1, 1, 0, 0, 0, 0)	(97,3)		
					(1, 0, 0, 0, 1, 3)	(12,9)		
\mathbb{Z}_{37}	(1, 0, 0, 0, 0, 1, 0)	(10,7)	(1, 0, 0, 0, 1, 0, 0)	(17,6)	(1, 0, 0, 0, 0, 2, 0)	(16,8)		
			(1, 0, 0, 0, 0, 1, 1)	(11,8)	(1, 0, 0, 0, 1, 0, 1)	(18,7)		
					(1, 0, 0, 1, 0, 0, 0)	(37,5)		
					(1, 0, 0, 0, 0, 1, 2)	(12,9)		
\mathbb{Z}_{38}			(1, 0, 0, 0, 0, 0, 1, 0)	(11,8)	(1, 0, 0, 0, 0, 1, 0, 0)	(18,7)		
					(1, 0, 0, 0, 0, 0, 1, 1)	(12,9)		
\mathbb{Z}_{39}					(1, 0, 0, 0, 0, 0, 0, 1, 0)	(12,9)		

proved that, for $5 \le t \le 11$, the improved upper bounds are equal and give the exact value of $A_{t,2}$. Let $\tilde{X}_{t,s,2} = |\{(t_1, \ldots, t_s) \in \mathbb{N}^s : t+1 = \sum_{i=1}^s (s-i+1)t_i, \ t_1 \ge 2\}|$ for $s \in \{3, \ldots, \lfloor (t+1)/2 \rfloor \}$ and $\tilde{X}_{t,2,2} = |\{(t_1, t_2) \in \mathbb{N}^2 : t+1 = 2t_1 + t_2, \ t_1 \ge 3\}|$.

Theorem 5 [12] *For* $t \ge 3$,

$$\mathcal{A}_{t,2} \le 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} \tilde{X}_{t,s,2} \tag{5}$$

and

$$A_{t,2} \le 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} (A_{t,s,2} - 1). \tag{6}$$

Moreover, for $3 \le t \le 11$ *, the upper bounds* (5) *and* (6) *coincide and are tight.*

Now, we consider the case $p \ge 3$ prime. In this case, we only have the following upper bounds.

Theorem 6 [3] For $t \ge 3$ and $p \ge 3$ prime,

$$A_{t,p} \le 1 + \sum_{s=2}^{t-1} (X_{t,s,p} - 1) \tag{7}$$

and

$$A_{t,p} \le 1 + \sum_{s=2}^{t-1} (A_{t,s,p} - 1).$$
 (8)

In this paper, in order to improve the upper bounds (7) and (8), we analyze the equivalence relations among the \mathbb{Z}_{p^s} -linear GH codes with the same length p^t and different values of s. We prove that some of them are indeed permutation equivalent. For $5 \le t \le 11$ if p = 2, for $4 \le t \le 10$ if p = 3, and for $4 \le t \le 8$ if p = 5, the ones that are permutation equivalent



(25,6) (58,5) (32,5) (85,4)

(1, 0, 0, 0, 0, 1, 0)(1, 0, 0, 1, 0, 0)(1, 0, 1, 0, 1)(1, 1, 0, 0, 0)(1, 0, 0, 1, 2)(1, 0, 0, 2, 0) (t_1,\ldots,t_s) (1, 0, 2, 1)(2, 0, 0, 1)(1, 0, 1, 3)(1, 1, 0, 2)(1, 1, 1, 0)(2, 0, 3)(1, 3, 0)(3, 0, 0)(1, 1, 4)t = 8(134,2)(31,4)(31,4)(11,6) (24,5) (57,4)(11,6) (24,5) (31,4)(84,3) (r, k)(1, 0, 0, 0, 1, 0)(1, 0, 1, 0, 0)(1, 0, 0, 1, 1) (t_1,\ldots,t_s) 1, 0, 2, 0(1, 1, 0, 1)(2, 0, 0, 0)(1, 2, 1)(2, 0, 2)(2, 1, 0)(2, 4) t = 7(4, 0) (23,4)(23,4)(10,5)(10,5)(30,3)(30,3)(10,5)(r, k)(10,5)(1,0,0,1,0) (t_1,\ldots,t_s) (1, 1, 0, 0)(2, 0, 1) (1, 1, 2) t = 6(3, 1)**Table 5** Rank and kernel for all nonlinear \mathbb{Z}_{5^s} -linear GH codes of length 5^t (r, k)(22,3) (29,2)(9,4) (9,4) (9,4) (t_1,\ldots,t_s) (2, 0, 0)t = 5(2, 2) (3, 0) (r,k)(8,3) (8,3) (t_1,\ldots,t_s) t = 4(2, 1) \mathbb{Z}_{25} \mathbb{Z}_{5^3} \mathbb{Z}_{56} \mathbb{Z}_{57} \mathbb{Z}_{54} \mathbb{Z}_55

(135,3)

(85,4)

(25,6)

(7,3)

(32,5)

(135,3)

(12,7) (32,5) (12,7)

(32,5)

(12,7) (25,6)

coincide with the ones having the same invariants, rank and dimension of the kernel, that is, the same pair (r, k). Finally, by using these equivalence relations, we improve the upper bounds on the number $\mathcal{A}_{t,p}$ of nonequivalent \mathbb{Z}_{p^s} -linear GH codes of length p^t with $p \geq 3$ prime given by Theorem 6. This allows us to determine the exact value of $\mathcal{A}_{t,p}$ for all t, $1 \leq t \leq 11$, if $1 \leq t \leq 11$, if 1

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

In this section, we give some properties of the generalized Gray map ϕ_s . We also prove that, for $p \ge 3$ prime, some of the \mathbb{Z}_{p^s} -linear GH codes of the same length p^t , having different values of s are permutation equivalent. Moreover, we see that they coincide with the ones having the same rank and dimension of the kernel for all t, $4 \le t \le 10$, when p = 3; and for all t, $4 \le t \le 8$, when p = 5.

Lemma 1 Let $s \geq 2$ and $\lambda_i \in \mathbb{Z}_p$, $i \in \{0, \ldots, s-1\}$. Then,

$$\sum_{i=0}^{s-1} \lambda_i \phi_s(p^i) = \phi_s(\sum_{i=0}^{s-1} \lambda_i p^i).$$

Proof Straightforward from the definition of ϕ_s .

Let $\gamma_s \in \mathcal{S}_{p^{s-1}}$ be the permutation defined as follows: for a coordinate $k = jp^{s-2} + i + 1 \in \{1, 2, ..., p^{s-1}\}$, where $j \in \{0, ..., p-1\}$ and $i \in \{0, ..., p^{s-2} - 1\}$, γ_s moves coordinate k to coordinate j + ip + 1. Therefore, we can write γ_s as

$$\begin{pmatrix} 1 & 2 & \dots & p^{s-2} & p^{s-2} + 1 & p^{s-2} + 2 & \dots & p^{s-2} + p^{s-2} & \dots \\ 1 & p+1 & \dots & (p^{s-2}-1)p+1 & 2 & p+2 & \dots & (p^{s-2}-1)p+2 & \dots \\ \dots & (p-1)p^{s-2} + 1 & (p-1)p^{s-2} + 2 & \dots & p^{s-1} \\ \dots & p & p+p & \dots & p^{s-1} \end{pmatrix}.$$

Example 1 For p = 3 and s = 3,

$$\gamma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 7 & 2 & 5 & 8 & 3 & 6 & 9 \end{pmatrix} = (2, 4)(3, 7)(6, 8) \in \mathcal{S}_9.$$

and for p = 3 and s = 4,

$$\gamma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 \\ 1 & 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 2 & 5 & 8 & 11 & 14 & 17 & 20 & 23 & 26 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \end{pmatrix}$$

$$= (2, 4, 10)(3, 7, 19)(5, 13, 11)(6, 16, 20)(8, 22, 12)(9, 25, 21)(15, 17, 23)$$

$$(18, 26, 24) \in \mathcal{S}_{27}.$$

Lemma 2 Let
$$s \ge 2$$
, $u = (\mathbf{0}, \mathbf{1}, \dots, \mathbf{p} - \mathbf{1}) \in \mathbb{Z}_p^{p^{s-1}}$, and $v = (0, 1, \dots, p-1) \in \mathbb{Z}_p^p$. Then, $\gamma_s(u) = (v, p^{s-2}, v)$.

Proof Straightforward from the definition of γ_s .



Then, we can define the map $\tau_s: \mathbb{Z}_{p^s} \to \mathbb{Z}_{p^{s-1}}^p$ as

$$\tau_s(u) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(u))), \tag{9}$$

where $u \in \mathbb{Z}_{p^s}$.

Example 2 For p = 3 and s = 3, we have

```
\phi_3(0) = (0, 0, 0, 0, 0, 0, 0, 0, 0) = \gamma_3(0, 0, 0, 0, 0, 0, 0, 0, 0) = \gamma_3(\Phi_2(0, 0, 0)),
 \phi_3(1) = (0, 1, 2, 0, 1, 2, 0, 1, 2) = \gamma_3(0, 0, 0, 1, 1, 1, 2, 2, 2) = \gamma_3(\Phi_2(0, 3, 6)),
 \phi_3(2) = (0, 2, 1, 0, 2, 1, 0, 2, 1) = \gamma_3(0, 0, 0, 2, 2, 2, 1, 1, 1) = \gamma_3(\Phi_2(0, 6, 3)),
 \phi_3(3) = (0, 0, 0, 1, 1, 1, 2, 2, 2) = \gamma_3(0, 1, 2, 0, 1, 2, 0, 1, 2) = \gamma_3(\Phi_2(1, 1, 1)),
 \phi_3(4) = (0, 1, 2, 1, 2, 0, 2, 0, 1) = \gamma_3(0, 1, 2, 1, 2, 0, 2, 0, 1) = \gamma_3(\Phi_2(1, 4, 7))
 \phi_3(5) = (0, 2, 1, 1, 0, 2, 2, 1, 0) = \gamma_3(0, 1, 2, 2, 0, 1, 1, 2, 0) = \gamma_3(\Phi_2(1, 7, 4)),
 \phi_3(6) = (0, 0, 0, 2, 2, 2, 1, 1, 1) = \gamma_3(0, 2, 1, 0, 2, 1, 0, 2, 1) = \gamma_3(\Phi_2(2, 2, 2)),
\phi_3(7) = (0, 1, 2, 2, 0, 1, 1, 2, 0) = \gamma_3(0, 2, 1, 1, 0, 2, 2, 1, 0) = \gamma_3(\Phi_2(2, 5, 8)),
\phi_3(8) = (0, 2, 1, 2, 1, 0, 1, 0, 2) = \gamma_3(0, 2, 1, 2, 1, 0, 1, 0, 2) = \gamma_3(\Phi_2(2, 8, 5)),
\phi_3(9) = (1, 1, 1, 1, 1, 1, 1, 1, 1) = \gamma_3(1, 1, 1, 1, 1, 1, 1, 1, 1) = \gamma_3(\Phi_2(3, 3, 3)),
\phi_3(10) = (1, 2, 0, 1, 2, 0, 1, 2, 0) = \gamma_3(1, 1, 1, 2, 2, 2, 0, 0, 0) = \gamma_3(\Phi_2(3, 6, 0)),
\phi_3(11) = (1, 0, 2, 1, 0, 2, 1, 0, 2) = \gamma_3(1, 1, 1, 0, 0, 0, 2, 2, 2) = \gamma_3(\Phi_2(3, 0, 6)),
\phi_3(12) = (1, 1, 1, 2, 2, 2, 0, 0, 0) = \gamma_3(1, 2, 0, 1, 2, 0, 1, 2, 0) = \gamma_3(\Phi_2(4, 4, 4)),
\phi_3(13) = (1,2,0,2,0,1,0,1,2) = \gamma_3(1,2,0,2,0,1,0,1,2) = \gamma_3(\Phi_2(4,7,1)),
\phi_3(14) = (1, 0, 2, 2, 1, 0, 0, 2, 1) = \gamma_3(1, 2, 0, 0, 1, 2, 2, 0, 1) = \gamma_3(\Phi_2(4, 1, 7)),
\phi_3(15) = (1, 1, 1, 0, 0, 0, 2, 2, 2) = \gamma_3(1, 0, 2, 1, 0, 2, 1, 0, 2) = \gamma_3(\Phi_2(5, 5, 5)),
\phi_3(16) = (1, 2, 0, 0, 1, 2, 2, 0, 1) = \gamma_3(1, 0, 2, 2, 1, 0, 0, 2, 1) = \gamma_3(\Phi_2(5, 8, 2)),
\phi_3(17) = (1, 0, 2, 0, 2, 1, 2, 1, 0) = \gamma_3(1, 0, 2, 0, 2, 1, 2, 1, 0) = \gamma_3(\Phi_2(5, 2, 8)),
\phi_3(18) = (2, 2, 2, 2, 2, 2, 2, 2, 2) = \gamma_3(2, 2, 2, 2, 2, 2, 2, 2, 2) = \gamma_3(\Phi_2(6, 6, 6)),
\phi_3(19) = (2, 0, 1, 2, 0, 1, 2, 0, 1) = \gamma_3(2, 2, 2, 0, 0, 0, 1, 1, 1) = \gamma_3(\Phi_2(6, 0, 3)),
\phi_3(20) = (2, 1, 0, 2, 1, 0, 2, 1, 0) = \gamma_3(2, 2, 2, 1, 1, 1, 0, 0, 0) = \gamma_3(\Phi_2(6, 3, 0)),
\phi_3(21) = (2, 2, 2, 0, 0, 0, 1, 1, 1) = \gamma_3(2, 0, 1, 2, 0, 1, 2, 0, 1) = \gamma_3(\Phi_2(7, 7, 7)),
\phi_3(22) = (2, 0, 1, 0, 1, 2, 1, 2, 0) = \gamma_3(2, 0, 1, 0, 1, 2, 1, 2, 0) = \gamma_3(\Phi_2(7, 1, 4)),
\phi_3(23) = (2, 1, 0, 0, 2, 1, 1, 0, 2) = \gamma_3(2, 0, 1, 1, 2, 0, 0, 1, 2) = \gamma_3(\Phi_2(7, 4, 1)),
\phi_3(24) = (2, 2, 2, 1, 1, 1, 0, 0, 0) = \gamma_3(2, 1, 0, 2, 1, 0, 2, 1, 0) = \gamma_3(\Phi_2(8, 8, 8)),
\phi_3(25) = (2, 0, 1, 1, 2, 0, 0, 1, 2) = \gamma_3(2, 1, 0, 0, 2, 1, 1, 0, 2) = \gamma_3(\Phi_2(8, 2, 5)),
\phi_3(26) = (2, 1, 0, 1, 0, 2, 0, 2, 1) = \gamma_3(2, 1, 0, 1, 0, 2, 0, 2, 1) = \gamma_3(\Phi_2(8, 5, 2)).
```

These equalities define the map $\tau_3:\mathbb{Z}_{27}\to\mathbb{Z}_9^3$ as

$$\begin{array}{llll} \tau_3(0)=(0,0,0), & \tau_3(9)=(3,3,3), & \tau_3(18)=(6,6,6), \\ \tau_3(1)=(0,3,6), & \tau_3(10)=(3,6,0), & \tau_3(19)=(6,0,3), \\ \tau_3(2)=(0,6,3), & \tau_3(11)=(3,0,6), & \tau_3(20)=(6,3,0), \\ \tau_3(3)=(1,1,1), & \tau_3(12)=(4,4,4), & \tau_3(21)=(7,7,7), \\ \tau_3(4)=(1,4,7), & \tau_3(13)=(4,7,1), & \tau_3(22)=(7,1,4), \\ \tau_3(5)=(1,7,4), & \tau_3(14)=(4,1,7), & \tau_3(23)=(7,4,1), \\ \tau_3(6)=(2,2,2), & \tau_3(15)=(5,5,5), & \tau_3(24)=(8,8,8), \\ \tau_3(7)=(2,5,8), & \tau_3(16)=(5,8,2), & \tau_3(25)=(8,2,5), \\ \tau_3(8)=(2,8,5), & \tau_3(17)=(5,2,8), & \tau_3(26)=(8,5,2). \end{array}$$

Lemma 3 [3] Let $s \geq 2$ and $\lambda \in \mathbb{Z}_p$. Then, $\phi_s(\lambda p^{s-1}) = (\lambda, \stackrel{p^{s-1}}{\dots}, \lambda)$.

Lemma 4 Let s > 2. Then,

(i)
$$\tau_s(1) = (0, p^{s-2}, \dots, (p-1)p^{s-2}),$$

(ii) $\tau_s(p^i u) = p^{i-1}(u, \stackrel{p}{\dots}, u)$ for $i \in \{1, \dots, s-1\}$ and $u \in \{0, 1, \dots, p^{s-1} - 1\} \subseteq \mathbb{Z}_{p^s}.$

Proof First, let $v = (0, 1, ..., p - 1) \in \mathbb{Z}_p^p$. Then,

$$\begin{aligned} \tau_s(1) &= \varPhi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(1))) \\ &= \varPhi_{s-1}^{-1}(\gamma_s^{-1}(v, \stackrel{p^{s-2}}{\dots}, v)) \\ &= \varPhi_{s-1}^{-1}(\mathbf{0}, \mathbf{1}, \dots, \mathbf{p-1}), \text{ by Lemma 2.} \end{aligned}$$

Finally, by Lemma 3, $\tau_s(1) = (0, p^{s-2}, ..., (p-1)p^{s-2})$, and (i) holds.

In order to prove (ii), let $u \in \mathbb{Z}_{p^s}$ and $[u_0, \ldots, u_{s-1}]_p$ be its p-ary expansion. The p-ary expansion of p^iu is $[0, ..., 0, u_0, \ldots, u_{s-i-1}]_p$ and we have that $\phi_s(p^iu) = (u_{s-i-1}, \stackrel{p^{s-1}}{\dots}, u_{s-i-1}) + (0, ..., 0, u_0, \ldots, u_{s-i-2})Y_{s-1}$. Recall that the matrix Y_{s-1} given in (1), related to the definition of ϕ_s , is a matrix of size $(s-1) \times p^{s-1}$ whose columns are the elements of \mathbb{Z}_p^{s-1} . Moreover, we consider that the columns of Y_{s-1} are ordered in ascending order, by considering the elements of \mathbb{Z}_p^{s-1} as the p-ary expansions of the elements of $\mathbb{Z}_{p^{s-1}}$. Therefore, Y_s is also the matrix obtained recursively from $Y_1 = (0 \ 1 \ \cdots \ p-1)$ and

$$Y_s = \begin{pmatrix} Y_{s-1} & Y_{s-1} & \cdots & Y_{s-1} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p-1} \end{pmatrix}.$$

By Lemma 2, we can write

$$\gamma_s^{-1}(Y_{s-1}) = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p-1} \\ Y_{s-2} & Y_{s-2} & \cdots & Y_{s-2} \end{pmatrix}.$$

Then, we have that

$$\gamma_{s}^{-1}(\phi_{s}(p^{i}u))
= (u_{s-i-1}, \stackrel{p^{s-1}}{\dots}, u_{s-i-1}) + (0, \stackrel{i}{\dots}, 0, u_{0}, \dots, u_{s-i-2}) \begin{pmatrix} \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p} - \mathbf{1} \\ Y_{s-2} & Y_{s-2} & \cdots & Y_{s-2} \end{pmatrix}
= (u_{s-i-1}, \stackrel{p^{s-1}}{\dots}, u_{s-i-1}) + (0, \stackrel{i}{\dots}, 0, u_{0}, \dots, u_{s-i-2}) (Y_{s-2} & Y_{s-2} & \cdots & Y_{s-2})
= (\phi_{s-1}(p^{i-1}u), \stackrel{p}{\dots}, \phi_{s-1}(p^{i-1}u)) = \phi_{s-1}(p^{i-1}(u, \stackrel{p}{\dots}, u)).$$

Therefore, $\tau_s(p^i u) = \Phi_{s-1}^{-1}(\gamma_s^{-1}(\phi_s(p^i u))) = p^{i-1}(u, ..., u)$, and (ii) holds.

Proposition 1 Let $s \ge 2$ and $\lambda_i \in \{0, 1, ..., p-1\}$, $i \in \{0, ..., s-1\}$. Then,

$$\phi_s \left(\sum_{i=0}^{s-1} \lambda_i \, p^i \right) = \gamma_s \left(\Phi_{s-1} \left(\sum_{i=0}^{s-1} \tau_s \left(\lambda_i \, p^i \right) \right) \right). \tag{10}$$

Proof By Lemma 4, we know that for all $i \in \{1, ..., s-1\}$, $\tau_s(p^i) = (p^{i-1}, ..., p^{i-1})$ and $\tau_s(1) = (0, p^{s-2}, ..., (p-1)p^{s-2})$. Then, by Lemma 1, we have that

$$\gamma_s\left(\Phi_{s-1}\left(\sum_{i=0}^{s-1}\tau_s(\lambda_i\,p^i)\right)\right)=\gamma_s\left(\sum_{i=0}^{s-1}\Phi_{s-1}\left(\tau_s(\lambda_i\,p^i)\right)\right).$$

Moreover, γ_s commutes with the addition. Therefore, by applying the definition of the map τ_s given in (9), we obtain that

$$\gamma_s\left(\Phi_{s-1}\left(\sum_{i=0}^{s-1}\tau_s(\lambda_i\,p^i)\right)\right) = \sum_{i=0}^{s-1}\gamma_s\left(\Phi_{s-1}\left(\tau_s(\lambda_i\,p^i)\right)\right) = \sum_{i=0}^{s-1}\phi_s\left(\lambda_i\,p^i\right),$$

which is equal to $\phi_s(\sum_{i=0}^{s-1} \lambda_i p^i)$ by Lemma 1.

Corollary 1 *Let* $s \ge 2$ *and* $\lambda_i \in \{0, 1, ..., p-1\}, i \in \{0, ..., s-1\}$. *Then,*

$$\tau_s \left(\sum_{i=0}^{s-1} \lambda_i \, p^i \right) = \sum_{i=0}^{s-1} \tau_s(\lambda_i \, p^i). \tag{11}$$



Proof By Proposition 1, we have that

$$\phi_s\left(\sum_{i=0}^{s-1}\lambda_i\,p^i\right) = \gamma_s\left(\Phi_{s-1}\left(\sum_{i=0}^{s-1}\tau_s(\lambda_i\,p^i)\right)\right),\,$$

and, therefore,

$$\Phi_{s-1}^{-1}\left(\gamma_s^{-1}\left(\phi_s(\sum_{i=0}^{s-1}\lambda_i\,p^i)\right)\right) = \sum_{i=0}^{s-1}\tau_s\left(\lambda_i\,p^i\right),$$

that is,
$$\tau_s(\sum_{i=0}^{s-1} \lambda_i p^i) = \sum_{i=0}^{s-1} \tau_s(\lambda_i p^i)$$
.

Now, we extend the permutation $\gamma_s \in \mathcal{S}_{p^{s-1}}$ to a permutation $\gamma_s \in \mathcal{S}_{p^{s-1}n}$ such that, if we restrict this extended permutation to each set of p^{s-1} coordinates $\{p^{s-1}i+1, p^{s-1}i+2, \ldots, p^{s-1}(i+1)\}$, $i \in \{0, \ldots, n-1\}$, it acts as $\gamma_s \in \mathcal{S}_{p^{s-1}}$. That is, the extended permutation $\gamma_s \in \mathcal{S}_{p^{s-1}n}$ can be seen as n consecutive copies of $\gamma_s \in \mathcal{S}_{p^{s-1}}$. Then, we component-wise extend function τ_s defined in (9) to $\tau_s : \mathbb{Z}_{p^s}^n \to \mathbb{Z}_{p^{s-1}}^{pn}$ and define $\tilde{\tau}_s = \rho^{-1} \circ \tau_s$, where $\rho \in \mathcal{S}_{pn}$ is defined as follows: for a coordinate $k = jn + i + 1 \in \{1, 2, \ldots, pn\}$, where $i \in \{0, \ldots, n-1\}$ and $j \in \{0, \ldots, p-1\}$, ρ moves coordinate k = j to c

$$\begin{pmatrix} 1 & 2 & \dots & n & n+1 & n+2 & \dots & 2n & \dots \\ 1 & p+1 & \dots & (n-1)p+1 & 2 & p+2 & \dots & (n-1)p+2 & \dots \\ & & \dots & pn-n+1 & pn-n+2 & \dots & pn \\ & \dots & p & p+p & \dots & pn \end{pmatrix}.$$

Example 3 For p = 3 and n = 2,

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 5 & 3 & 6 \end{pmatrix} \in \mathcal{S}_6.$$

and for p = 3 and n = 4,

$$\rho = \begin{pmatrix} 1 \ 2 \ 3 \ 4 & 5 \ 6 \ 7 & 8 & 9 \ 10 \ 11 \ 12 \\ 1 \ 4 \ 7 \ 10 & 2 \ 5 \ 8 \ 11 & 3 & 6 & 9 \ 12 \end{pmatrix} \in \mathcal{S}_{12}.$$

Remark 1 If $\mathbf{u} = (u_1, u_2, \dots, u_n) \in \mathbb{Z}_{p^s}^n$ and $\tau_s(u_i) = (u_{i,1}, u_{i,2}, \dots, u_{i,p})$ for all $i \in \{1, \dots, n\}$, then

$$\tau_s(\mathbf{u}) = (u_{1,1}, u_{1,2}, \dots, u_{1,p}, u_{2,1}, u_{2,2}, \dots, u_{2,p}, \dots, u_{n,1}, u_{n,2}, \dots, u_{n,p}),$$

and
$$\tilde{\tau}_s(\mathbf{u}) = (u_{1,1}, u_{2,1}, \dots, u_{n,1}, u_{1,2}, u_{2,2}, \dots, u_{n,2}, \dots, u_{1,p}, u_{2,p}, \dots, u_{n,p}).$$

Lemma 5 Let $s \geq 2$. Then, $\Phi_s(\mathbf{u}) = \gamma_s(\Phi_{s-1}(\rho(\tilde{\tau}_s(\mathbf{u}))))$ for all $\mathbf{u} \in \mathbb{Z}_{p^s}^n$.

Proof From the definition of τ_s given in (9) and the definition of $\tilde{\tau}_s = \rho^{-1} \circ \tau_s$, we have that $\tilde{\tau}_s(\mathbf{u}) = \rho^{-1}(\tau_s(\mathbf{u})) = \rho^{-1}(\Phi_{s-1}^{-1}(\gamma_s^{-1}(\Phi_s(\mathbf{u}))))$. Then, the result follows.

A *p*-linear combination of the elements of a set $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_r\} \subseteq \mathbb{Z}_{p^s}^n$ is $\sum_{i=1}^r \lambda_i \mathbf{b}_i$ for $\lambda_i \in \mathbb{Z}_p$. We say that \mathcal{B} is a *p*-basis of \mathcal{C} if the elements in \mathcal{B} are *p*-linearly independent and any $\mathbf{c} \in \mathcal{C}$ is a *p*-linear combination of the elements of \mathcal{B} . Let $\mathbf{w}_i^{(s)}$ be the *i*-th row of



 $A_p^{t_1,\dots,t_s}$, $1 \le i \le t_1 + \dots + t_s$. By construction, $\mathbf{w}_1^{(s)} = \mathbf{1}$ and $o(\mathbf{w}_i^{(s)}) \le o(\mathbf{w}_j^{(s)})$ if i > j. Let σ_i be the integer such that $o(\mathbf{w}_i^{(s)}) = p^{\sigma_i}$. Then, we have that $\mathcal{B}^{t_1,\dots,t_s} = \{p^{q_i}\mathbf{w}_i^{(s)} : 1 \le i \le t_1 + \dots + t_s, \ 0 \le q_i \le \sigma_i - 1\}$ is a p-basis of $\mathcal{H}_p^{t_1,\dots,t_s}$.

Example 4 Let $\mathcal{H}_3^{2,1}$ and $\mathcal{H}_3^{1,1,0}$ be the \mathbb{Z}_9 -additive and \mathbb{Z}_{27} -additive GH codes, which are generated by

$$A_3^{2,1} = \begin{pmatrix} \mathbf{w}_1^{(2)} \\ \mathbf{w}_2^{(2)} \\ \mathbf{w}_3^{(2)} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} \\ v & v & v \\ \mathbf{0} & \mathbf{3} & \mathbf{6} \end{pmatrix},$$

where v = (0, 1, 2, 3, 4, 5, 6, 7, 8), and

$$A_3^{1,1,0} = \begin{pmatrix} \mathbf{w}_1^{(3)} \\ \mathbf{w}_2^{(3)} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{pmatrix},$$

respectively. The corresponding 3-bases are

$$\mathcal{B}^{2,1} = \{ \mathbf{w}_{1}^{(2)}, 3\mathbf{w}_{1}^{(2)}, \mathbf{w}_{2}^{(2)}, 3\mathbf{w}_{2}^{(2)}, \mathbf{w}_{3}^{(2)} \}$$

$$= \{ \mathbf{1}, \mathbf{3}, (v, v, v), (0, 3, 6, ..., 0, 3, 6), (0, ..., 0, 3, ..., 3, 6, ..., 6) \}, \text{ and}$$

$$\mathcal{B}^{1,1,0} = \{ \mathbf{w}_{1}^{(3)}, 3\mathbf{w}_{1}^{(3)}, 9\mathbf{w}_{1}^{(3)}, \mathbf{w}_{2}^{(3)}, 3\mathbf{w}_{2}^{(3)} \}$$

$$= \{ \mathbf{1}, \mathbf{3}, \mathbf{9}, (0, 3, 6, 9, 12, 15, 18, 21, 24), (0, 9, 18, 0, 9, 18, 0, 9, 18) \}.$$

Lemma 6 Let $s \ge 2$ and $t_s \ge 1$. Let $\mathbf{w}_i^{(s)}$ and $\mathbf{w}_i^{(s+1)}$ be the *i*-th row of $A_p^{t_1, \dots, t_s}$ and $A_p^{1,t_1-1,t_2, \dots, t_{s-1}, t_s-1}$, respectively. Then, $(\mathbf{w}_i^{(s+1)}, \overset{p}{\dots}, \mathbf{w}_i^{(s+1)}) = p\mathbf{w}_i^{(s)}$ and $o(\mathbf{w}_i^{(s)}) = o(\mathbf{w}_i^{(s+1)}) = p^{\sigma_i}$.

Proof Consider $A_p^{t_1,\dots,t_s}$ with $t_s \ge 1$, and $\mathbf{w}_i^{(s)}$ its i-th row for $i \in \{1,\dots,t_1+\dots+t_s\}$. Then, the matrix over $\mathbb{Z}_{p^{s+1}}$

$$\begin{pmatrix} \mathbf{w}_1^{(s)} \\ p\mathbf{w}_2^{(s)} \\ \vdots \\ p\mathbf{w}_{t_1+\dots+t_s}^{(s)} \end{pmatrix}$$

is, by definition, $A_p^{1,t_1-1,t_2,\dots,t_s}$. Moreover, by the construction given in (2), we have that $A_p^{1,t_1-1,t_2,\dots,t_s}$ is the matrix

$$\begin{pmatrix} A_p^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1} & A_p^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1} & \cdots & A_p^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1} \\ p^s \cdot \mathbf{0} & p^s \cdot \mathbf{1} & \cdots & p^s \cdot (\mathbf{p}-\mathbf{1}) \end{pmatrix}.$$

Therefore, if $\mathbf{w}_{i}^{(s+1)}$ is the *i*-th row of $A_{p}^{1,t_{1}-1,t_{2},...,t_{s-1},t_{s}-1}$ for $i \in \{2,...,t_{1}+t_{2}+\cdots+t_{s}-1\}$, we have that $(\mathbf{w}_{i}^{(s+1)},...^{p}..,\mathbf{w}_{i}^{(s+1)}) = p\mathbf{w}_{i}^{(s)}$ and $o(\mathbf{w}_{i}^{(s)}) = o(\mathbf{w}_{i}^{(s+1)}) = p^{\sigma_{i}}$.

Proposition 2 Let $s \geq 2$, $t_s \geq 1$, and $\mathcal{H}^{t_1,\dots,t_s}_p$ and $\mathcal{H}^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1}_p$ be the \mathbb{Z}_{p^s} -additive and $\mathbb{Z}_{p^{s+1}}$ -additive GH codes with generator matrices A^{t_1,\dots,t_s}_p and $A^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1}_p$, respectively. Let $\mathbf{w}^{(s)}_i$ and $\mathbf{w}^{(s+1)}_i$ be the i-th row of A^{t_1,\dots,t_s}_p and $A^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1}_p$, respectively. Then, we have that



- (i) $\tilde{\tau}_{s+1}(p^{q_i}\mathbf{w}_i^{(s+1)}) = p^{q_i}\mathbf{w}_i^{(s)}$, for all $i \in \{2, \dots, t_1 + \dots + t_s 1\}$ and $q_i \in \{0, \dots, \sigma_i 1\}$, where $o(\mathbf{w}_{i}^{(s)}) = p^{\sigma_{i}}$;
- (ii) $\tilde{\tau}_{s+1}(p^{j+1}\mathbf{w}_1^{(s+1)}) = p^j\mathbf{w}_1^{(s)}$, for all $j \in \{0, \dots, s-1\}$; (iii) $\tilde{\tau}_{s+1}(\mathbf{w}_1^{(s+1)}) = \mathbf{w}_{t_1+\dots+t_s}^{(s)}$.

Proof By Lemma 6, we have that $(\mathbf{w}_i^{(s+1)}, \overset{p}{\ldots}, \mathbf{w}_i^{(s+1)}) = p\mathbf{w}_i^{(s)}$ and $o(\mathbf{w}_i^{(s)}) = o(\mathbf{w}_i^{(s+1)}) = p^{\sigma_i}$. Let $\mathbf{v}_i^{(s+1)}$ be the vector over $\mathbb{Z}_{p^{s+1}}$ such that $\mathbf{w}_i^{(s+1)} = p\mathbf{v}_i^{(s+1)}$ and $\mathbf{w}_i^{(s)} = (\mathbf{v}_i^{(s+1)}, \overset{p}{\ldots})$. $(\mathbf{v}_i^{(s+1)})$. Let $(\mathbf{v}_i^{(s+1)})_j$ be the *j*th coordinate of $\mathbf{v}_i^{(s+1)}$. By the definition of $\tilde{\tau}_{s+1}$ and Lemma 4, for $q_i \in \{0, \dots, \sigma_i - 1\}$, we have that

$$\tilde{\tau}_{s+1}(p^{q_i}\mathbf{w}_i^{(s+1)}) = \rho^{-1}(\tau_{s+1}(p^{q_i}\mathbf{w}_i^{(s+1)})) = \rho^{-1}(\tau_{s+1}(p^{q_i+1}\mathbf{v}_i^{(s+1)}))
= \rho^{-1}(p^{q_i}((\mathbf{v}_i^{(s+1)})_1, ..., (\mathbf{v}_i^{(s+1)})_1, ..., (\mathbf{v}_i^{(s+1)})_n, ..., (\mathbf{v}_i^{(s+1)})_n, ..., (\mathbf{v}_i^{(s+1)})_n))
= p^{q_i}(\mathbf{v}_i^{(s+1)}, ..., \mathbf{v}_i^{(s+1)}) = p^{q_i}\mathbf{w}_i^{(s)},$$

and (i) holds.

Since $\mathbf{w}_1^{(s)} = (\mathbf{w}_1^{(s+1)}, \stackrel{p}{\dots}, \mathbf{w}_1^{(s+1)}) = \mathbf{1}$ and $\mathbf{w}_{t_1 + \dots + t_s}^{(s)} = (p^{s-1} \cdot \mathbf{0}, p^{s-1} \cdot \mathbf{1}, \dots, p^{s-1} \cdot (\mathbf{p} - \mathbf{1}))$, then the equalities in items (*ii*) and (*iii*) hold by the definition of $\tilde{\tau}_{s+1}$ and Lemma 4.

Note that, by Proposition 2, we have that $\tilde{\tau}_{s+1}$ is a bijection between the p-bases, $\mathcal{B}^{t_1,\dots,t_s}$ and $\mathcal{B}^{1,t_1-1,...,t_{s-1},t_s-1}$.

Example 5 Let $\mathcal{H}_3^{2,1}$ and $\mathcal{H}_3^{1,1,0}$ be the same codes considered in Example 4. The length of $\mathcal{H}_3^{1,1,0}$ is n=9. Then, the extension of $\gamma_3=(2,4)(3,7)(6,8)\in\mathcal{S}_9$ defined in Example 1 is

$$\gamma_3 = (2, 4)(3, 7)(6, 8)(11, 13)(12, 16)(15, 17)(20, 22)(21, 25)(24, 26)(29, 31)(30, 34)
(33, 35)(38, 40)(39, 43)(42, 44)(47, 49)(48, 52)(51, 53)(56, 58)(57, 61)(60, 62)
(65, 67)(66, 70)(69, 71)(74, 76)(75, 79)(78, 80) $\in S_{81}$,$$

and

In this case, by using the equalites given in Example 2, we have that

where u = (0, 3, 6), v = (0, 1, 2, 3, 4, 5, 6, 7, 8) and w = (0, 0, 0, 3, 3, 3, 6, 6, 6).



Since $\Phi_3(\mathbf{u}) = \gamma_3(\Phi_2(\rho(\tilde{\tau}_3(\mathbf{u}))))$ for all $\mathbf{u} \in \mathbb{Z}_{27}^9$, the map $\tilde{\tau}_3$ sends the elements of the 3-basis $\mathcal{B}^{1,1,0}$ into the elements of the 3-basis $\mathcal{B}^{2,1}$. That is, as it is shown in Proposition 2,

$$\begin{array}{lll} \tilde{\tau}_{3}(\mathbf{w}_{1}^{(3)}) & = & \tilde{\tau}_{3}(1,1,1,1,1,1,1,1,1) & = & (\mathbf{0},\mathbf{3},\mathbf{6}) & = \mathbf{w}_{3}^{(2)}, \\ \tilde{\tau}_{3}(3\mathbf{w}_{1}^{(3)}) & = & \tilde{\tau}_{3}(3,3,3,3,3,3,3,3,3,3,3) & = & (1,\frac{27}{1},1) & = & \mathbf{w}_{1}^{(2)}, \\ \tilde{\tau}_{3}(9\mathbf{w}_{1}^{(3)}) & = & \tilde{\tau}_{3}(9,9,9,9,9,9,9,9,9) & = & (3,\frac{27}{1},3) & = & 3\mathbf{w}_{1}^{(2)}, \\ \tilde{\tau}_{3}(\mathbf{w}_{2}^{(3)}) & = & \tilde{\tau}_{3}(0,3,6,9,12,15,18,21,24) & = & (v,v,v) & = & \mathbf{w}_{2}^{(2)}, \\ \tilde{\tau}_{3}(3\mathbf{w}_{2}^{(3)}) & = & \tilde{\tau}_{3}(0,9,18,0,9,18,0,9,18) & = & (u,\frac{9}{1},u) & = & 3\mathbf{w}_{2}^{(2)}, \end{array}$$

so $\tilde{\tau}_3$ is a bijection between both 3-bases.

Lemma 7 Let $\mathcal{H}_s = \mathcal{H}_p^{t_1, \dots, t_s}$ be a \mathbb{Z}_{p^s} -additive GH code with $s \geq 2$ and $t_s \geq 1$. Then, $H_s = \Phi_s(\mathcal{H}_s)$ is permutation equivalent to $H_{s+1} = \Phi_{s+1}(\mathcal{H}_{s+1})$, where $\mathcal{H}_{s+1} = \mathcal{H}_p^{1,t_1-1,t_2,\dots,t_{s-1},t_s-1}$, which is a $\mathbb{Z}_{p^{s+1}}$ -linear GH code.

Proof Note that H_s and H_{s+1} both have the same length p^t . Let $\mathcal{B}_s = \{\mathbf{v}_1^{(s)}, \dots, \mathbf{v}_{t+1}^{(s)}\}$ and $\mathcal{B}_{s+1} = \{\mathbf{v}_1^{(s+1)}, \dots, \mathbf{v}_{t+1}^{(s+1)}\}$ be the p-basis of \mathcal{H}_s and \mathcal{H}_{s+1} , respectively. By Proposition 2, $\tilde{\tau}_{s+1}$ is a bijection between \mathcal{B}_s and \mathcal{B}_{s+1} . By the definition of $\tilde{\tau}_{s+1}$ and Corollary 1, we have that $\tilde{\tau}_{s+1}$ commutes with the addition, so $\tilde{\tau}_{s+1}(\mathcal{H}_{s+1}) = \mathcal{H}_s$.

Let $\rho_* \in \mathcal{S}_{p^t}$ be a permutation such that $\Phi_s(\rho(\mathbf{u})) = \rho_*(\Phi_s(\mathbf{u}))$ for all $\mathbf{u} \in \mathcal{H}_s$. Since $\mathcal{H}_s = \tilde{\tau}_{s+1}(\mathcal{H}_{s+1}) = \rho^{-1}(\Phi_s^{-1}(\gamma_{s+1}^{-1}(\Phi_{s+1}(\mathcal{H}_{s+1}))))$, we have that $\Phi_s(\mathcal{H}_s) = \rho_*^{-1}(\gamma_{s+1}^{-1}(\Phi_{s+1}(\mathcal{H}_{s+1})))$. Therefore, we obtain $H_s = (\gamma_{s+1} \circ \rho_*)^{-1}(H_{s+1})$, where $\gamma_{s+1} \circ \rho_* \in \mathcal{S}_{p^t}$.

Theorem 7 determines which $\mathbb{Z}_{p^{s'}}$ -linear GH codes are equivalent to a given \mathbb{Z}_{p^s} -linear GH code $H_p^{t_1,\dots,t_s}$. We denote by $\mathbf{0}^j$ the all-zero vector of length j.

Theorem 7 Let $H_p^{t_1,...,t_s}$ be a \mathbb{Z}_{p^s} -linear GH code with $s \geq 2$ and $t_s \geq 1$. Then, $H_p^{t_1,...,t_s}$ is permutation equivalent to the $\mathbb{Z}_{p^{s+\ell}}$ -linear GH code

$$H_p^{1,\mathbf{0}^{\ell-1},t_1-1,t_2,...,t_{s-1},t_s-\ell},$$

for all $\ell \in \{1, \ldots, t_s\}$.

Proof Consider $\mathcal{H}_0 = \mathcal{H}_p^{t_1, \dots, t_s}$ and $\mathcal{H}_\ell = \mathcal{H}_p^{1,0^{\ell-1}, t_1-1, t_2, \dots, t_{s-1}, t_s-\ell}$ for $\ell \in \{1, \dots, t_s\}$. By Lemma 7, we have that $H_i = \Phi(\mathcal{H}_i)$ is permutation equivalent to $H_{i+1} = \Phi(\mathcal{H}_{i+1})$ for all $i \in \{0, \dots, \ell-1\}$ and $\ell \in \{1, \dots, t_s\}$. Therefore, we have that H_0 and H_ℓ are permutation equivalent for all $\ell \in \{1, \dots, t_s\}$.

Let t_1, t_2, \ldots, t_s be nonnegative integers with $t_1 \ge 2$, or $t_1 = 1$ and s = 2. Let $C_p(t_1, \ldots, t_s) = [H_1 = H_p^{t_1, \ldots, t_s}, H_2, \ldots, H_\rho]$ 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 $H_p^{t_1, \ldots, t_s}$ by Theorem 7. We denote by $C_p(t_1, \ldots, t_s)[i]$ the i-th code H_i in the sequence, for $1 \le i \le t_s + 1$. We consider that the codes in $C_p(t_1, \ldots, t_s)$ are ordered as follows:

$$C_p(t_1, \dots, t_s)[i] = \begin{cases} H_p^{t_1, \dots, t_s} & \text{if } i = 1, \\ H_p^{1, \mathbf{0}^{i-2}, t_1 - 1, t_2, \dots, t_{s-1}, t_s - i + 1} & \text{otherwise.} \end{cases}$$
(12)

We refer to $C_p(t_1, \ldots, t_s)$ as the chain of equivalences of $H_p^{t_1, \ldots, t_s}$.



Remark 2 First, note that if $t_s = 0$, then $C_p(t_1, \ldots, t_s) = [H_p^{t_1, \ldots, t_s}]$. Moreover, there are no two different codes in the chain $C_p(t_1, \ldots, t_s)$ that have the same value of s. Finally, also by construction, if there is only one \mathbb{Z}_{p^2} -linear GH code in the chain $C_p(t_1, \ldots, t_s)$, then it is placed in the first position and s = 2.

Corollary 2 Let $C_p(t_1,...,t_s)$ be the chain of equivalences of $H_p^{t_1,...,t_s}$, where $t_1 \ge 2$, or $t_1 = 1$ and s = 2. Then,

$$|C_p(t_1,\ldots,t_s)| = t_s + 1.$$

Since all the codes in a given chain $C_p(t_1, \ldots, t_s)$ are equivalent, we have that if one of the codes in a chain is linear, then all the codes in that chain are also linear. The following result gives the conditions on the values t_1, \ldots, t_s so that the chain $C_p(t_1, \ldots, t_s)$ contains linear codes. In fact, we have that this chain contains linear \mathbb{Z}_{p^s} -linear codes of a certain length for any $s \in \{2, \ldots, t+1\}$.

Theorem 8 Let $C_p(t_1, ..., t_s)$ be the chain of equivalences of $H_p^{t_1, ..., t_s}$. Then, for all $H \in C_p(t_1, ..., t_s)$, H is linear if and only if s = 2 and one of the following conditions is satisfied:

- (i) p = 2 and $t_1 \in \{1, 2\}$,
- (ii) $p \ge 3$ prime and $t_1 = 1$.

Proof First, assume that H is linear for all $H \in C_p(t_1, \ldots, t_s)$. Let $H_p^{t_1', \ldots, t_{s'}'} \in C_p(t_1, \ldots, t_s)$. If s' = 2, then $(t_1, t_2) = (t_1', t_2')$ by Remark 2, and we have that p = 2 and $t_1' \in \{1, 2\}$ by Theorem 1, or $p \geq 3$ prime and $t_1' = 1$ by Theorem 3. Now, assume that s' > 2. By Theorems 2 and 3, we have that $H_p^{t_1', \ldots, t_{s'}'} = H_p^{1, 0^{s'-2}, t_{s'}'}$ for p prime, or $H_p^{t_1', \ldots, t_{s'}'} = H_2^{1, 0^{s'-3}, 1, t_{s'}'}$. By Theorem 7, $H_p^{1, 0^{s'-2}, t_{s'}'}$ is equivalent to $H_p^{1, t_{s'}' + s' - 2}$ for p prime, and $H_2^{1, 0^{s'-3}, 1, t_{s'}'}$ is equivalent to $H_2^{2, t_{s'}' + s' - 2}$. Therefore, by Remark 2, we have that s = 2 and one of the conditions in the statement is satisfied.

The converse result follows from the definition of the chain of equivalences $C_p(t_1, ..., t_s)$ and Theorems 1 and 3.

Corollary 3 Let $t \ge 2$. If p = 2, then there are two different linear chains of equivalences, $C_2(1, t - 1)$ and $C_2(2, t - 3)$. If $p \ge 3$ prime, then there is a unique linear chain of equivalences, $C_p(1, t - 1)$.

Proof From Theorem 8, if $C_p(t_1, \ldots, t_s)$ is a linear chain of equivalences, then s = 2. Moreover, we have that the codes in $C_p(t_1, t_2)$ are of length p^t , where $t = 2t_1 + t_2 - 1$. The possible values of t_1 are also given in Theorem 8 depending on the value of p as follows. First, if p = 2, we have that $t_1 \in \{1, 2\}$. Therefore, if $t_1 = 1$, then the chain is $C_2(1, t - 1)$; and if $t_1 = 2$, then the chain is $C_2(2, t - 3)$. Second, if $p \ge 3$ prime, then $t_1 = 1$ and the chain is $C_p(1, t - 1)$.

Example 6 The chain of equivalences of $H_3^{1,5}$ is

$$C_3(1,5) = [H_3^{1,5}, H_3^{1,0,4}, H_3^{1,0,0,3}, H_3^{1,0,0,0,2}, H_3^{1,0,0,0,0,1}, H_3^{1,0,0,0,0,0}]$$

and it contains exactly $t_2 + 1 = 6$ codes. Note that $(t_1, t_2) = (1, 5)$ satisfies the second condition of Theorem 8. Thus, this chain contains linear GH codes. They are all the linear GH codes over \mathbb{Z}_3 of length $3^t = 3^6$ and dimension t + 1 = 7 as seen in Table 2.



Example 7 From one hand, the chain of equivalences of $H_2^{1,4}$ is

$$C_2(1,4) = [H_2^{1,4}, H_2^{1,0,3}, H_2^{1,0,0,2}, H_2^{1,0,0,0,1}, H_2^{1,0,0,0,0,0}]$$

and it contains $t_2 + 1 = 5$ codes. From the other hand, the chain of equivalence of $H_2^{2,2}$ is

$$C_2(2,2) = [H_2^{2,2}, H_2^{1,1,1}, H_2^{1,0,1,0}]$$

and it contains exactly $t_2 + 1 = 3$ codes. Note that the values of (t_1, t_2) in both cases, (1, 4) and (2, 2), satisfy the first condition of Theorem 8, so these chains contain linear Hadamard codes. In fact, the sequences $C_2(1, 4)$ and $C_2(2, 2)$ contain all the linear Hadamard codes of length of $2^t = 2^5$ and dimension t + 1 = 6 as can be seen in Table 1. Therefore, all the codes in these chains are permutation equivalent to each other.

Recall that $\mathbf{w}_2^{(s)}$ is the second row of $A_p^{t_1,\dots,t_s}$. Let σ be the integer such that $o(\mathbf{w}_2^{(s)}) = p^{s+1-\sigma}$. For $\mathcal{H}_p^{1,0,\dots,0}$, we define $\sigma = s$. Note that $\sigma = 1$ if and only if $t_1 \geq 2$, and $\sigma = \min\{i: t_i > 0, i \in \{2,\dots,s\}\}$ if $t_1 = 1$. Then, $\sigma \in \{1,\dots,s\}$. We say that $o(\mathcal{H}_p^{t_1,\dots,t_s}) = \sigma$; or equivalently, $o(H_p^{t_1,\dots,t_s}) = \sigma$. Note that if $\sigma = s$, then $H_p^{t_1,\dots,t_s} = H_p^{1,0,\dots,0,t_s}$ with $s \geq 2$ and $t_s \geq 0$, so it is linear by Theorems 1, 2, and 3. Moreover, since σ_2 is the integer such that $o(\mathbf{w}_2^{(s)}) = p^{\sigma_2}$, we have that $\sigma = s + 1 - \sigma_2$.

If we focus on the chains of equivalences $C_p(t_1, \ldots, t_s)$ having nonlinear codes, then we can assume that $t_1 \ge 2$ by Theorem 8.

Proposition 3 Let $C_p(t_1, ..., t_s)$ be the chain of equivalences of $H_p^{t_1, ..., t_s}$, where $t_1 \ge 2$. If $H_p^{t_1, ..., t_s}$ is nonlinear, then for all $H \in C_p(t_1, ..., t_s)$,

$$ker(H) = \begin{cases} \sum_{i=1}^{s} t_i & \text{if } p \ge 3 \text{ prime,} \\ 1 + \sum_{i=1}^{s} t_i & \text{if } p = 2. \end{cases}$$

Proof Since $t_1 \ge 2$, then $\sigma = 1$. By [3, Theorem 4], for $p \ge 3$ prime, we have that $\ker(H_p^{t_1,\dots,t_s}) = (\sum_{i=1}^s t_i) + \sigma - 1 = \sum_{i=1}^s t_i$. Note that for p = 2 and s > 2, $H_2^{t_1,\dots,t_s}$ is nonlinear by Theorem 2. Thus, by [11, Theorem 3], we have that $\ker(H_2^{t_1,\dots,t_s}) = \sigma + (\sum_{i=1}^s t_i) = 1 + \sum_{i=1}^s t_i$. Therefore, the result follows from the definition of the chain of equivalences $C_p(t_1,\dots,t_s)$.

Example 8 The chain of equivalences of $H_3^{2,5}$ is the sequence $C_3(2,5) = [H_3^{2,5}, H_3^{1,1,4}, H_3^{1,0,1,3}, H_3^{1,0,0,1,2}, H_3^{1,0,0,0,1,1}, H_3^{1,0,0,0,0,1,0}]$ and contains exactly $t_2+1=6$ codes. Note that this sequence contains all the codes of length 3^8 having the pair (r,k)=(10,7) in Table 4. In the same table, note that there is only one code of length 3^9 having the pair (r,k)=(43,4), named $H_3^{2,2,0}$. Therefore, $C_3(2,2,0)=[H_3^{2,2,0}]$, which contains just this code, since $t_3+1=1$.

Example 9 Consider the chains of equivalences $C_3(4, 1) = [H_3^{4,1}, H_3^{1,3,0}]$ and $C_3(2, 0, 3) = [H_3^{2,0,3}, H_3^{1,1,0,2}, H_3^{1,0,1,0,1}, H_3^{1,0,0,1,0,0}]$. Note that, from Proposition 3, the codes in both chains have dimension of the kernel equals to 5. However, from Table 4, we have that the pair (r, k) is (22, 5) for codes in $C_3(4, 1)$, and (16, 5) for codes in $C_3(2, 0, 3)$. Therefore, codes in $C_3(4, 1)$ are not equivalent to codes in $C_3(2, 0, 3)$.

Proposition 4 Let $C_p(t_1,...,t_s)$ be the chain of equivalences of $H_p^{t_1,...,t_s}$. Then, the $\mathbb{Z}_{p^{s'}}$ linear GH code $H_p^{t_1',...,t_{s'}'} = C_p(t_1,...,t_s)[i]$, $1 \le i \le t_s + 1$, satisfies



- (i) s' = s + i 1,
- (ii) $\sigma' = i$.
- (iii) $t'_{s'} = t_s i + 1$,

(iv)
$$(t'_1, \dots, t'_{s'}) = \begin{cases} (t_1, \dots, t_s) & \text{if } i = 1, \\ (1, \mathbf{0}^{i-2}, t_1 - 1, t_2, \dots, t_{s-1}, t_s - i + 1) & \text{otherwise.} \end{cases}$$

Proof Straightforward from Theorem 7 and the definition of the chain of equivalences $C_p(t_1, \ldots, t_s)$.

Note that the value of s' is different for every code $H_p^{t_1', \dots, t_{s'}'}$ belonging to the same chain of equivalences $C_p(t_1, \dots, t_s)$ as pointed out in Remark 2.

Corollary 4 Let $C_p(t_1, ..., t_s)$ be the chain of equivalences of $H_p^{t_1, ..., t_s}$. Then,

- (i) if $t_1 \geq 2$, the $\mathbb{Z}_{p^{s'}}$ -linear GH code $H_p^{t'_1, \dots, t'_{s'}} = C_p(t_1, \dots, t_s)[1]$ is the only one in $C_p(t_1, \dots, t_s)$ with $t'_1 \geq 2$;
- (ii) the $\mathbb{Z}_{p^{s'}}$ -linear GH code $H_p^{t_1',\ldots,t_{s'}'}=C_p(t_1,\ldots,t_s)[t_s+1]$ is the only one in $C_p(t_1,\ldots,t_s)$ with $t_{s'}'=0$; and
- (iii) if $t_1 = 1$ and s = 2, every $H_p^{t_1', \dots, t_{s'}'} \in C_p(t_1, \dots, t_s)$ satisfies $t_1' = 1$.

Now, given any \mathbb{Z}_{p^s} -linear GH code $H_p^{t_1,\ldots,t_s}$, we determine the chain of equivalences containing this code, as well as its position in the sequence. Therefore, note that indeed we prove that any code $H_p^{t_1,\ldots,t_s}$ (with $t_1\geq 1$) belongs to a unique chain of equivalences $C_p(t_1',\ldots,t_{s'}')$ with $t_1'\geq 2$ or $t_1'=1$ and s'=2.

Theorem 9 Let $H = H_p^{t_1, \dots, t_s}$, p prime, and $\sigma = o(H)$. Let $\ell \in \{1, \dots, s-1\}$ such that $H = H_p^{t_1, 0^{\ell-1}, t_{\ell+1}, \dots, t_s}$, where $t_{\ell+1} \neq 0$ if $\ell < s-1$. Then, H belongs to an unique chain of equivalences, and it satisfies one of the following conditions:

- (i) if $t_1 \ge 2$, then $\sigma = 1$ and $H = C_p(t_1, ..., t_s)[1]$.
- (ii) if $t_1 = 1$ and $\ell = s 1$, then $\sigma = s$ and $H = C_p(1, t_s + \ell 1)[\sigma 1]$.
- (iii) if $t_1 = 1$ and $\ell < s-1$, then $\sigma = \ell+1$ and $H = C_p(t'_1, \ldots, t'_{s'})[\sigma]$, where $(t'_1, \ldots, t'_{s'}) = (t_{\sigma} + 1, t_{\sigma+1}, \ldots, t_{s-1}, t_s + \sigma 1)$ and $s' = s \sigma + 1$.

Proof Item (i) follows from Corollary 4 (i). For Item (ii), we have that $H_p^{t_1,\dots,t_s} = H_p^{1,0^{s-2},t_s}$ and hence $\sigma = s$. We have that $H_p^{1,0^{s-2},t_s}$ is a linear \mathbb{Z}_{p^s} -linear GH code by Theorems 1, 2 and 3. Since $H_p^{1,0^{s-2},t_s}$ is linear, then by Theorem 8, $H_p^{1,0^{s-2},t_s} \in C_p(t_1',t_2')$, where $t_1' \in \{1,2\}$ if p=2 and $t_1'=1$ if $p\geq 3$ prime. By Theorem 7, we have that $H_p^{1,0^{s-2},t_s} = C_p(1,t_s+\ell-1)[\ell]$ for p prime. Moreover, since no code in the chain $C_2(2,t_2')$ has $(t_1,\dots,t_s)=(1,0^{s-2},t_s)$, $H_2^{1,0^{s-2},t_s} \notin C_2(2,t_2')$.

For Item (iii), since $t_1 = 1$ and $\ell < s - 1$, we have that $t_{\ell+1} \neq 0$ and hence $\sigma = \ell + 1$. By Theorem 7, we have that $H_p^{t_1, \dots, t_s} = C_p(t_1', \dots, t_{s'}')[\ell + 1]$. Since $\ell = \sigma - 1$, by Proposition 4 we have that $(t_1, \dots, t_s) = (1, \mathbf{0}^{\sigma - 2}, t_1' - 1, t_2', \dots, t_{s'-1}', t_{s'}' - \sigma + 1)$. Therefore, $t_{\sigma} = t_1' - 1$, $t_{\sigma+1} = t_2', \dots, t_{s-1} = t_{s'-1}', t_s = t_{s'}' - \sigma + 1$, and the result follows.

Note that, in Theorem 9, the values of (t_1, \ldots, t_s) satisfying Item (ii) for p prime correspond to linear \mathbb{Z}_{p^s} -linear GH codes.



Table 6 Type of all \mathbb{Z}_{p^s} -linear
GH codes of length p^{t} with
$t_1 \ge 2$ (equivalently, $\sigma = 1$) and
$t_s = 0 \text{ for } t \le 10 \text{ and } p \in \{2, 3\}$

t = 5	(3,0), (2,0,0)
t = 7	(4,0), (2,1,0), (2,0,0,0)
t = 8	(3,0,0)
t = 9	(5,0), (2,2,0), (2,0,1,0), (2,0,0,0,0)
t = 10	(3,1,0), (2,1,0,0)

Corollary 5 Let $H = H_p^{t_1,0^{\ell-1},t_{\ell+1},\dots,t_s}$, where p prime, $\ell \in \{1,\dots,s-1\}$, $t_{\ell+1} \neq 0$ if $\ell < s-1$, and $\sigma = o(H)$. Let $C_p(t_1',\dots,t_{s'}')$ be the chain of equivalences such that $H \in C_p(t_1',\dots,t_{s'}')$. Then, if $t_1 = 1$ and $\ell = s-1$, $H = C_p(1,t_s+\ell-1)[\sigma-1]$ and $|C_p(1,t_s+\ell-1)| = t_s+\sigma-1$; otherwise, $H = C_p(t_1',\dots,t_{s'}')[\sigma]$ and $|C_p(t_1',\dots,t_{s'}')| = t_s+\sigma$.

Proof By Theorem 9, we have three cases. If $t_1 = 1$ and $\ell = s - 1$, we have that $\sigma = s$ and $H = H_p^{t_1,0^{\ell-1},t_s} = C_p(t_1,t_s+\ell-1)[\sigma-1]$. Then, by Corollary 2, $|C_p(t_1,t_s+\ell-1)| = t_s + \ell - 1 + 1 = t_s + s - 1 = t_s + \sigma - 1$. If $t_1 \geq 2$, then $\sigma = 1$ and $H = H_p^{t_1,\dots,t_s} = C_p(t_1,\dots,t_s)[1]$, so by Corollary 2, $|C_p(t_1,\dots,t_s)| = t_s + 1 = t_s + \sigma$.

If $t_1 = 1$ and $\ell < s-1$, we have that $H = H_p^{t_1, \dots, t_s} = C_p(t_\sigma + 1, t_{\sigma+1}, \dots, t_{s-1}, t_s + \sigma - 1)[\sigma]$. By Corollary 2, $|C_p(t_\sigma + 1, t_{\sigma+1}, \dots, t_{s-1}, t_s + \sigma - 1)| = t_s + \sigma - 1 + 1 = t_s + \sigma$. \square

Example 10 The \mathbb{Z}_{35} -linear GH code $H_3^{1,0,0,1,2}$ has $t_1=1, \ell=3, \sigma=4$, and s=5. By Theorem 9, since $3=\ell < s-1=4, \sigma=4$, and $s'=s-\sigma+1=2$, this code is placed in the fourth position of the chain of equivalences $C_3(t_1',t_2')$, where $t_1'=t_4+1=1+1=2$ and $t_2'=t_5+\sigma-1=2+4-1=5$. Therefore, $H_3^{1,0,0,1,2}=C_3(2,5)[4]$. By Corollary 5, $C_3(2,5)$ contains exactly $t_5+\sigma=2+4=6$ codes, which are the ones described in Example 8.

If $H_p^{t_1,\dots,t_s}$ is a \mathbb{Z}_{p^s} -linear GH code of length p^t with $t_1 \geq 2$ and $t_s = 0$, then $H_p^{t_1,\dots,t_s} = C_p(t_1,\dots,t_s)[1]$ and $|C_p(t_1,\dots,t_s)| = 1$ since $\sigma = 1$, by Corollary 5. From Tables 1 and 3 given in [11], and Tables 3, 4 and 5, we can see that $H_p^{t_1,\dots,t_s}$ is not equivalent to any other code $H_p^{t_1',\dots,t_s'}$ of the same length p^t , for $t \leq 11$ if p = 2, for $t \leq 10$ if p = 3, and for $t \leq 8$ if p = 5. We conjecture that this is true in general, for any $t \geq 3$ and p prime. The values of (t_1,\dots,t_s) for which the code $H_p^{t_1,\dots,t_s}$ is not equivalent to any other such code of the same length p^t , for $t \leq 10$ and $p \in \{2,3\}$, can be found in Table 6. These values are also the same at least for $t \leq 8$ if p = 5 by Table 5.

From Tables 3 and 4, we can also see that the \mathbb{Z}_{3^s} -linear GH codes of length 3^t with $t \le 10$ having the same values (r, k) are the ones which are equivalent by Theorem 7. The same happens for \mathbb{Z}_{5^s} -linear GH codes of length 5^t with $t \le 8$ by Table 5, and the same was known for \mathbb{Z}_{2^s} -linear GH codes of length 2^t with $t \le 11$ [12]. We conjecture that this is true in general, for any $t \ge 3$ and p prime.

4 Improvement of the partial classification

In this section, we improve some results on the classification of the \mathbb{Z}_{p^s} -linear GH codes of length p^t with $p \geq 3$ prime, once t is fixed. More precisely, we improve the upper bounds



of $A_{t,p}$ given by Theorem 6 and determine the exact value of $A_{t,3}$ for $t \le 10$ and $A_{t,5}$ for $t \le 8$, by using the equivalence results established in Sect. 3. This represents a generalization of the results given by Theorem 5 for p = 2.

Next, we prove two corollaries of Theorem 7, which allow us to improve the known upper bounds on $A_{t,p}$ with $t \ge 3$ and $p \ge 3$ prime.

Corollary 6 Let $H_p^{t_1,...,t_s}$ be a nonlinear \mathbb{Z}_{p^s} -linear GH code with p prime, and $\sigma = o(H_p^{t_1,...,t_s})$. Then, $H_p^{t_1,...,t_s}$ 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 $H_p^{t_1',\ldots,t_{s'}'}$ with $t_1' \geq 2$, and there is exactly one $H_p^{t_1',\ldots,t_{s'}'}$ with $t_2' = 0$.

Proof The code $H_p^{t_1,\ldots,t_s}$ belongs to a chain of equivalences C, which can be determined by Theorem 9. We have that $H_p^{t_1,\ldots,t_s}$ is equivalent to any code in C by Theorem 7, and the number of codes in C is $t_s+\sigma$ by Corollary 5. By Theorem 9, the first code in C has $s'=s-\sigma+1$. By Proposition 4, the i-th code $H_p^{t_1',\ldots,t_{s'}'}=C[i]$ has $s'=s-\sigma+i$ for $i\in\{1,\ldots,t_s+\sigma\}$. Therefore, $s'\in\{s-\sigma+1,\ldots,s+t_s\}$. Finally, by Corollary 4, C[1] is the only code in C with $t_1'\geq 2$ and $C[t_s+\sigma]$ is the only code in C with $t_{s'}'=0$.

From Corollary 6, in order to determine the number of nonequivalent nonlinear \mathbb{Z}_{p^s} -linear GH codes of length p^t with $p \geq 3$ prime, named $\mathcal{A}_{t,p}$, we just have to consider one code out of the $t_s + \sigma$ codes that are permutation equivalent. For example, we can consider the one with $t_1 \geq 2$.

Corollary 7 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 $s' \in \{2, \ldots, \lfloor (t+1)/2 \rfloor \}$.

Proof Let $H_p^{t_1,\dots,t_s}$ be a \mathbb{Z}_{p^s} -linear GH code with $s \in \{\lfloor (t+1)/2 \rfloor + 1,\dots,t+1\}$. Since $\sum_{i=1}^s (s+1-i)t_i = t+1$ and $t_1 \geq 1$, then $t_1 = 1$ and we have that $\sigma > 1$. Therefore, by Theorem 9, $H_p^{t_1,\dots,t_s}$ is permutation equivalent to the $\mathbb{Z}_{p^{s-\sigma+1}}$ -linear GH code $H = H_p^{t_\sigma+1,t_{\sigma+1},\dots,t_{s-1},t_s+\sigma-1}$.

Now, we just need to see that $s-\sigma+1<\lfloor (t+1)/2\rfloor$. Since the length of H is p^t , we have that $t+1=(s-\sigma+1)(t_\sigma+1)+\sum_{i=2}^{s-\sigma+1}(s-\sigma+2-i)t_{\sigma-1+i}+\sigma-1$. Therefore, $(s-\sigma+1)(t_\sigma+1)\leq t+1$ and $s-\sigma+1\leq (t+1)/(t_\sigma+1)$. By the definition of t_σ , we know that $t_\sigma\geq 1$, so $s-\sigma+1\leq \lfloor (t+1)/2\rfloor$.

Note that we can focus on the \mathbb{Z}_{p^s} -linear GH codes of length p^t with p prime and $s \in \{2, \ldots, \lfloor (t+1)/2 \rfloor\}$ by Corollary 7, and we can restrict ourselves to the codes having $t_1 \geq 2$ by Corollary 6. With this on mind, in order to classify all such codes for a given $t \geq 3$, we define $\tilde{X}_{t,s,p} = |\{(t_1, \ldots, t_s) \in \mathbb{N}^s : t+1 = \sum_{i=1}^s (s-i+1)t_i, \ t_1 \geq 2\}|$ for $s \in \{2, \ldots, \lfloor (t+1)/2 \rfloor\}$ if $p \geq 3$ prime. Recall that for p = 2, $\tilde{X}_{t,s,2} = |\{(t_1, \ldots, t_s) \in \mathbb{N}^s : t+1 = \sum_{i=1}^s (s-i+1)t_i, \ t_1 \geq 2\}|$ for $s \in \{3, \ldots, \lfloor (t+1)/2 \rfloor\}$ and $\tilde{X}_{t,2,2} = |\{(t_1, t_2) \in \mathbb{N}^s : t+1 = 2t_1 + t_2, \ t_1 \geq 3\}|$.

Theorem 10 *For all* t > 3 *and p prime,*

$$\mathcal{A}_{t,p} \le 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} \tilde{X}_{t,s,p} \tag{13}$$



,							
3	4	5	6	7	8	9	10
2	2	4	4	7	8	12	14
2	2	4	4	7	8	12	14
2	2	5	6	11	15	26	33
(8) 2	2	6	9	15	22	33	46
	3 2 2 2 2 (8) 2	2 2 2 2 2 2	2 2 4 2 2 4 2 2 5	2 2 4 4 2 2 4 4 2 2 5 6	2 2 4 4 7 2 2 4 4 7 2 2 5 6 11	2 2 4 4 7 8 2 2 4 4 7 8 2 2 5 6 11 15	2 2 4 4 7 8 12 2 2 4 4 7 8 12 2 2 5 6 11 15 26

Table 7 Bounds for the number $A_{t,3}$ of nonequivalent \mathbb{Z}_{3^s} -linear GH codes of length 3^t for $3 \le t \le 10$

Table 8 Bounds for the number $A_{t,5}$ of nonequivalent \mathbb{Z}_{5^s} -linear GH codes of length 5^t for $3 \le t \le 8$

t	3	4	5	6	7	8
Previous lower bound (r, k)	2	2	4	4	7	8
New upper bound (13)	2	2	4	4	7	8
New upper bound (14)	2	2	5	6	11	15
Previous upper bounds (7) and (8)		2	6	9	15	22

and

$$\mathcal{A}_{t,p} \le 1 + \sum_{s=2}^{\lfloor \frac{t+1}{2} \rfloor} (\mathcal{A}_{t,s,p} - 1). \tag{14}$$

Moreover, for any $3 \le t \le 11$ if p = 2, any $3 \le t \le 10$ if p = 3, and any $3 \le t \le 8$ if p = 5, the upper bound (13) is tight.

Proof If p = 2, the result is given by Theorem 5.

For $p \ge 3$ prime, it is proven that the codes $H_p^{1,0,\ldots,0,t_s}$ with $s \ge 2$ and $t_s \ge 0$, are the only \mathbb{Z}_{p^s} -linear GH codes which are linear. Note that they are not included in the definition of $\tilde{X}_{t,s,p}$ for $s \in \{2,\ldots,\lfloor (t+1)/2\rfloor\}$. Therefore, the new upper bounds (13) and (14) follow by Corollaries 6 and 7, after adding 1 to take into account the linear code.

In Table 7, for p = 3 and $3 \le t \le 10$, these new upper bounds together with previous bounds are shown. Note that the lower bound based on the rank and dimension of the kernel coincides with the upper bound (13) for $t \le 10$, so this upper bound is tight for $t \le 10$. Similarly, for p = 5 and $3 \le t \le 8$, the upper bound (13) is tight considering Table 8.

This last result improves the partial classification given in [3] or Theorem 6. Actually, by definition, we have that $\tilde{X}_{t,s,p} \leq X_{t,s,p} - 1$, so the upper bound (13) is clearly better than (7). It is also clear that the upper bound (14) is better than (8) since there are fewer addends. Therefore, both new upper bounds improve the previous known upper bounds given by Theorem 6. Recall that $A_{t,s,3} = X_{t,s,3}$ for any $3 \leq t \leq 10$ and $2 \leq s \leq t - 1$, and $A_{t,s,5} = X_{t,s,5}$ for any $3 \leq t \leq 8$ and $2 \leq s \leq t - 1$. If this equation is also true for any $t \geq 3$ and $p \geq 3$ prime, then upper bounds (7) and (8) coincide. Moreover, upper bound (13) would always be better than (14) since $\tilde{X}_{t,s,p} \leq X_{t,s,p} - 1 = A_{t,s,p} - 1$.

5 Conclusions and further research

The aim of this paper is to improve the classification of \mathbb{Z}_{p^s} -linear GH codes of length p^t with p prime, fixing the value of t. This approach complements the classification given in [3,



11] in which the authors fix the values of t and s. Specifically, we prove that there are some families of \mathbb{Z}_{p^s} -linear GH codes of length p^t , with codes having different values of s, such that all the codes belonging to the same family are equivalent to each other. This result is a generalization of a similar result given in [12] for p = 2. It allows us to improve the known upper bounds for $\mathcal{A}_{t,p}$. Moreover, it can be used to see that we only need to focus on finding the rank of \mathbb{Z}_{p^s} -linear GH codes $H_p^{t_1,\dots,t_s}$ with $t_1 \geq 2$ and $s \in \{2,\dots,\lfloor (t+1)/2\rfloor\}$ in order to establish a full classification, that is, to prove that the upper bound (13) is tight.

Taking into account the results about equivalences presented along this paper, we conjecture that \mathbb{Z}_{p^s} -linear GH codes $H_p^{t_1,\dots,t_s}$ with $t_1 \geq 2$ and $t_s = 0$ are not equivalent to any other $\mathbb{Z}_{p^{s'}}$ -linear GH code of the same length. We know that this statement is true at least for the codes of length p^t with t up to 11, 10, 8 when p is equal to 2, 3, 5, respectively.

Acknowledgements The authors would like to thank the anonymous referees for their valuable comments, which enabled them to improve the quality of the paper.

Funding Open Access Funding provided by Universitat Autonoma de Barcelona.

Data availability No data was used for the research described in the article.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

- 1. Assmus E.F., Key J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992).
- Bauer H., Ganter B., Hergert F.: Algebraic techniques for nonlinear codes. Combinatorica 3(1), 21–33 (1983).
- Bhunia D.K., Fernández-Córdoba C., Villanueva M.: On the linearity and classification of Z_p^s-linear generalized Hadamard codes. Des. Codes Cryptogr. 90, 1037–1058 (2022).
- Borges J., Fernández-Córdoba C., Rifà J.: Every Z_{2k}-code is a binary propelinear code. Electron. Notes Discret. Math. 10, 100−102 (2001).
- 5. Butson A.T.: Generalized Hadamard matrices. Proc. Am. Math. Soc. 13, 894-898 (1962).
- Bose R.C., Bush K.A.: Orthogonal arrays of strength two and three. Ann. Math. Stat. 23(4), 508–524 (1952).
- Bosma W., Cannon J.J., Fieker C., Steel A.: Handbook of Magma functions. Edition 2.25 (2020). http://magma.maths.usyd.edu.au/magma/.
- 8. Carlet C.: \mathbb{Z}_{2k} -linear codes. IEEE Trans. Inf. Theory **44**(4), 1543–1547 (1998).
- Dougherty Š.T., Fernández-Córdoba C.: Codes over Z_{2k}, Gray map and self-dual codes. Adv. Math. Commun. 5(4), 571−588 (2011).
- Dougherty S.T., Rifà J., Villanueva M.: Ranks and kernels of codes from generalized Hadamard matrices. IEEE Trans. Inf. Theory 62(2), 687–694 (2016).
- Fernández-Córdoba C., Vela C., Villanueva M.: On Z₂s-linear Hadamard codes: kernel and partial classification. Des. Codes Cryptogr. 87(2–3), 417–435 (2019).
- Fernández-Córdoba C., Vela C., Villanueva M.: Equivalences among Z₂s -linear Hadamard codes. Discret. Math. 343(3), 111721 (2020).
- Greferath M., Schmidt S.E.: Gray isometries for finite chain rings and a nonlinear ternary (36, 3¹², 15) code. IEEE Trans. Inf. Theory 45(7), 2522–2524 (1999).
- Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J., Solé P.: The Z₄-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Theory 40(2), 301–319 (1994).



- Jungnickel D.: On difference matrices, resolvable transversal designs and generalized Hadamard matrices. Math. Z. 167(1), 49–60 (1979).
- Krotov D.S.: Z₄-linear Hadamard and extended perfect codes. Electron. Notes Discret. Math. 6, 107–112 (2001).
- 17. Krotov D.S.: On \mathbb{Z}_{2^k} -dual binary codes. IEEE Trans. Inf. Theory **53**(4), 1532–1537 (2007).
- Li X., Shi M., Wang S., Lu H., Zheng Y.: Rank and pairs of rank and dimension of kernel of Z_pZ_{p2}-linear codes. IEEE Trans. Inf. Theory (2023). https://doi.org/10.1109/TIT.2023.3317064.
- Nechaev A.A., Khonol'd T.: Weighted modules and representations of codes. Problemy Peredachi Informatsii 35(3), 18–39 (1999).
- Phelps K.T., Rifà J., Villanueva M.: Kernels and p-kernels of p^r-ary 1-perfect codes. Des. Codes Cryptogr. 37(2), 243–261 (2005).
- Phelps K.T., Rifà J., Villanueva M.: On the additive (Z4-linear and non-Z4-linear) Hadamard codes: rank and kernel. IEEE Trans. Inf. Theory 52(1), 316–319 (2006).
- 22. Pujol J., Villanueva M.: *q*-ary codes. A MAGMA package, version 1.0. Universitat Autònoma de Barcelona, Barcelona (2017). https://ccsg.uab.cat/.
- Semakov N.V., Zinoviev V.A., Zaitsev V.G.: Class of maximal equidistant codes. Probl. Inf. Transm. 4(2), 84–87 (1968).
- Shi M., Sepasdar Z., Alahmadi A., Solé P.: On two-weight Z_{2k}-codes. Des. Codes Cryptogr. 86(6), 1201−1209 (2018).
- 25. Shi M., Wu R., Krotov D.S.: On $\mathbb{Z}_p\mathbb{Z}_{p^k}$ -additive codes and their duality. IEEE Trans. Inf. Theory **65**(6), 3841–3847 (2019).
- 26. Shi M., Honold T., Solé P., Qiu Y., Wu R., Sepasdar Z.: The geometry of two-weight codes over \mathbb{Z}_{p^m} . IEEE Trans. Inf. Theory **67**(12), 7769–7781 (2021).
- Villanueva N., Zinoviev V.A., Zinoviev D.V.: On one construction method for Hadamard matrices. Probl. Inf. Transm. 58(4), 13–37 (2022).
- Zinoviev V.A., Zinoviev D.V.: On the generalized concatenated construction for codes in l₁ and lee metrics. Probl. Inf. Transm. 57(1), 81–95 (2021).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Dipak K. Bhunia¹ • Cristina Fernández-Córdoba¹ • Carlos Vela² • Mercè Villanueva¹

Cristina Fernández-Córdoba cristina.fernandez@uab.cat Carlos Vela carlos.vela@ua.pt

Mercè Villanueva merce.villanueva@uab.cat

- Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Cerdanyola del Vallès, Spain
- Department of Mathematics, University of Aveiro, 3810-197 Aveiro, Portugal

