Designs, Codes and Cryptography (2022) 90:1037–1058
https://doi.org/10.1007/s10623-022-01026-2

On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes

Dipak K. Bhunia[1] · **Cristina Fernández-Córdoba**[1] · **Mercè Villanueva**[1]

Received: 22 August 2021 / Revised: 17 February 2022 / Accepted: 22 February 2022 /
Published online: 14 March 2022

Abstract
$\mathbb{Z}_{p^s}$-additive codes of length n are subgroups of $\mathbb{Z}_{p^s}^n$, and can be seen as a generalization of linear codes over $\mathbb{Z}_2$, $\mathbb{Z}_4$, or $\mathbb{Z}_{2^s}$ in general. 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 by a generalized Gray map. In this paper, we generalize some known results for $\mathbb{Z}_{p^s}$-linear GH codes with $p = 2$ to any odd prime p. First, we show some results related to the generalized Carlet's Gray map. Then, by using an iterative construction of $\mathbb{Z}_{p^s}$-additive GH codes of type $(n; t_1, \ldots, t_s)$, we show for which types the corresponding $\mathbb{Z}_{p^s}$-linear GH codes of length p^t are nonlinear over $\mathbb{Z}_p$. For these codes, we compute the kernel and its dimension, which allow us to give a partial classification. The obtained results for $p \geq 3$ are different from the case with $p = 2$. Finally, the exact number of non-equivalent such codes is given for an infinite number of values of s, t, and any $p \geq 2$; by using also the rank as an invariant in some specific cases.

Keywords Hadamard code · Gray map · $\mathbb{Z}_{p^s}$-linear code · $\mathbb{Z}_{p^s}$-additive code · Kernel · Classification

Mathematics Subject Classification 94B25 · 94B60

Communicated by C. Carlet.

This work has been partially supported by the Spanish MINECO under Grant PID2019-104664GB-I00 (AEI/10.13039/501100011033) and by Catalan AGAUR scholarship 2020 FI SDUR 00475.
The material in this paper was presented in part at the 26th International Conference on Applications of Computer Algebra, CACT@ACA2021, 23–27 July 2021-Virtual.

✉ Mercè Villanueva
merce.villanueva@uab.cat

Dipak K. Bhunia
dipak.bhunia@uab.cat

Cristina Fernández-Córdoba
cristina.fernandez@uab.cat

[1] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Cerdanyola del Vallès, Spain

1 Introduction

Let $\mathbb{Z}_{p^s}$ be the ring of integers modulo p^s with p prime and $s \geq 1$. The set of n-tuples over $\mathbb{Z}_{p^s}$ is denoted by $\mathbb{Z}_{p^s}^n$. 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 $m\mathbf{u} = \mathbf{0}$.

A code over $\mathbb{Z}_p$ of length n is a nonempty subset of $\mathbb{Z}_p^n$, and it is 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 if it is a subgroup of $\mathbb{Z}_{p^s}^n$. Note that, 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 $\mathbb{Z}_4$.

Two codes C_1 and C_2 over $\mathbb{Z}_p$ of length n are said to be monomially equivalent (or just equivalent) provided there is a monomial matrix M such that $C_2 = \{\mathbf{c}M : \mathbf{c} \in C_1\}$. Recall that a monomial matrix is a square matrix with exactly one nonzero entry in each row and column. They are said to be permutation equivalent if there is a permutation matrix P such that $C_2 = \{\mathbf{c}P : \mathbf{c} \in C_1\}$. Recall that a permutation matrix is a square matrix with exactly one 1 in each row and column and 0s elsewhere. A permutation matrix represents a permutation of coordinates, so we can also say that they are permutation equivalent if there is a permutation of coordinates π such that $C_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in C_1\}$. Similarly, two $\mathbb{Z}_{p^s}$-additive codes, $\mathcal{C}_1$ and $\mathcal{C}_2$, are said to be permutation equivalent if they differ only by a permutation of coordinates, that is, if there is a permutation of coordinates π such that $\mathcal{C}_2 = \{\pi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_1\}$.

In [15], a Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined as $\phi(0) = (0, 0), \phi(1) = (0, 1), \phi(2) = (1, 1)$ and $\phi(3) = (1, 0)$. There exist different generalizations of this Gray map, which go from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ [5, 7, 9, 16, 19]. The one given in [16] can be defined in terms of the elements of a Hadamard code [19], and Carlet's Gray map [7] is a particular case of the one given in [19] satisfying $\sum \lambda_i \phi(2^i) = \phi(\sum \lambda_i 2^i)$ [11]. In this paper, we focus on a generalization of Carlet's Gray map, from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_p^{p^{s-1}}$, which is also a particular case of the one given in [25]. We define $\Phi : \mathbb{Z}_{p^s}^n \to \mathbb{Z}_p^{np^{s-1}}$ as the component-wise Gray map ϕ.

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code of length n. We say that its image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_{p^s}$-linear code of length $p^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{p^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \mathbb{Z}_p^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(n; t_1, \ldots, t_s)$. Note that $|\mathcal{C}| = p^{st_1} p^{(s-1)t_2} \cdots p^{t_s}$. Unlike linear codes over finite fields, linear codes over rings do not have a basis, but there exists a generator matrix for these codes having minimum number of rows, that is, $t_1 + \cdots + t_s$ rows.

The Hamming weight of a vector $\mathbf{u} \in \mathbb{Z}_p^n$, denoted by $\mathrm{wt}_H(\mathbf{u})$, is the number of nonzero coordinates of $\mathbf{u}$. The Hamming distance of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_p^n$, denoted by $d_H(\mathbf{u}, \mathbf{v})$, is the number of coordinates in which they differ. Note that $d_H(\mathbf{u}, \mathbf{v}) = \mathrm{wt}_H(\mathbf{v} - \mathbf{u})$. The minimum distance of a code C over $\mathbb{Z}_p$ is $d(C) = \min\{d_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$.

Two structural properties of codes over $\mathbb{Z}_p$ are the rank and dimension of the kernel. The rank of a code C over $\mathbb{Z}_p$ is simply the dimension of the linear span, $\langle C \rangle$, of C. The kernel of a code C over $\mathbb{Z}_p$ is defined as $\mathrm{K}(C) = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x} + C = C\}$ [3, 20]. If the all-zero vector belongs to C, then $\mathrm{K}(C)$ is a linear subcode of C. Note also that if C is linear, then $K(C) = C = \langle C \rangle$. We denote the rank of C as $\mathrm{rank}(C)$ and the dimension of the kernel as $\ker(C)$. These parameters can be used to distinguish between non-equivalent codes, 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 $i, j, 1 \leq i < j \leq p\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \leq s \leq p\lambda\}$ contains every element of $\mathbb{Z}_p$ exactly λ times

[17]. An ordinary Hadamard matrix of order 4μ corresponds to a GH matrix $H(2, \lambda)$ over $\mathbb{Z}_2$, where $\lambda = 2\mu$ [2]. 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. From a normalized Hadamard matrix H, we denote by F_H the code over $\mathbb{Z}_p$ consisting of the rows of H, and C_H the one defined as $C_H = \bigcup_{\alpha\in\mathbb{Z}_p}(F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$ and $\mathbf{1}$ denotes the all-one vector. The code C_H over $\mathbb{Z}_p$ is called a generalized Hadamard (GH) code [10]. Note that C_H is generally a nonlinear code over $\mathbb{Z}_p$.

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code such that $\Phi(\mathcal{C})$ is a GH code. Then, we say that $\mathcal{C}$ is a $\mathbb{Z}_{p^s}$-additive GH code and $\Phi(\mathcal{C})$ 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 $\frac{N(p-1)}{p}$. It is known that 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 as a complete invariant for determining the equivalence class [18, 21]. There are exactly $\lfloor\frac{t-1}{2}\rfloor$ such codes for all $t \geq 2$. Later, in [11], an iterative construction for $\mathbb{Z}_{2^s}$-linear Hadamard codes was described, and the linearity and kernel of these codes were established. A partial classification by using the kernel was obtained, and the exact amount of non-equivalent such codes was given up to $t = 11$ for any $s \geq 2$.

Linear codes over $\mathbb{Z}_{p^s}$ were studied by Blake [4] and Shankar [22] in 1975 and 1979, respectively. Nevertheless, the study of codes over rings increased significantly after the publication of some good properties of linear codes over $\mathbb{Z}_4$ and the definition of the Gray map [15]. After that, $\mathbb{Z}_{2^s}$-additive codes and their images under the Gray map have been deeply studied, for example, in [7], and later in [26] and [14]. In [19], Krotov studied $\mathbb{Z}_{2^s}$-linear Hadamard codes and their dual codes by using different generalizations of the Gray map. In [23, 24], considering Carlet's generalization of the Gray map, two-weight $\mathbb{Z}_{p^s}$-linear and $\mathbb{Z}_{2^s}$-linear codes are studied. Note that $\mathbb{Z}_{p^s}$-linear Hadamard codes are in fact a particular case of these two-weight codes. More recently, $\mathbb{Z}_{p^s}$-linear GH codes have been constructed in [1] as images under the Gray map of Butson Hadamard codes, defined from Butson Hadamard matrices.

This paper is focused on $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, for any $t \geq 3$, $s \geq 2$ and p an odd prime. We generalize some results related to the linearity, kernel and classification of such codes, that are given for $p = 2$ in [11]. This paper is organized as follows. In Sect. 2, we recall the definitions of different Gray maps for elements of $\mathbb{Z}_{p^s}$, and we establish some properties for the one considered in this paper, called Carlet's Gray map. In Sect. 3, we describe the construction of $\mathbb{Z}_{p^s}$-linear GH codes of type $(n; t_1, \ldots, t_s)$ when this Gray map is used. In Sects. 4 and 5, we establish for which types these codes are linear, and we give the kernel and its dimension whenever they are nonlinear. In Sect. 6, we show that, in general, the dimension of the kernel is not enough to classify completely $\mathbb{Z}_{p^s}$-linear GH codes. However, for an infinite number of values of t and s, we can obtain a full classification and give the exact amount of non-equivalent such codes. It is worth to mention that the obtained results for $p \geq 3$ are different from the binary case. Moreover, new classification results are given also for $p = 2$. Finally, in Sect. 7, we give some conclusions and further research on this topic.

2 Generalized gray map and some properties

In this section, first we give the definition of some Gray maps for elements of $\mathbb{Z}_{p^s}$, and then we establish some properties for the one considered in this paper.

The usual Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$, given in [15], has been generalized to a Gray map from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ in [7, 19]. Actually, Carlet's Gray map from [7] is a particular case of the Gray map given in [19] satisfying $\sum \lambda_i \phi(2^i) = \phi(\sum \lambda_i 2^i)$ [11]. Similarly, in [25], a generalized Gray map from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_p^{p^{s-1}}$, with p prime, is defined as follows. Let P be the linear code over $\mathbb{Z}_p$ generated by a matrix A of size $s \times p^{s-1}$ as follows:

$$A = \begin{pmatrix} \mathbf{1} \\ Y \end{pmatrix}, \tag{1}$$

where the columns of the matrix Y are all different vectors in $\mathbb{Z}_p^{s-1}$. It is easy to check that P is a linear two-weight code of size p^s with nonzero weights $(p-1)p^{s-2}$ and p^{s-1}. Indeed, it is a linear GH code over $\mathbb{Z}_p$, and the corresponding GH matrix $H(p, p^{s-2})$ is known as the Sylvester Hadamard matrix. Note that P is also known as the 1st order generalized Reed-Muller code [2]. Whether the results hold or not is independent of the choice of Y. We arrange the codewords in $P = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{p^s-1}\}$ in such a way that $\mathbf{c}_0 = \mathbf{0}$ and for all u, $0 \le u \le p^{s-1} - 1$, and $j, 0 \le j \le p-1$, we have that $\mathbf{c}_{u+jp^{s-1}} - \mathbf{c}_u = (j, j, \ldots, j)$. Then, the Gray map ϕ is defined as

$$\begin{aligned} \phi : \mathbb{Z}_{p^s} &\longrightarrow \mathbb{Z}_p^{p^{s-1}} \\ u &\longmapsto \mathbf{c}_u. \end{aligned} \tag{2}$$

Example 1 Let $p = 3$ and $s = 2$. For example, we can take $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$ and $P = \{\mathbf{c}_0 = (0,0,0), \mathbf{c}_1 = (0,1,2), \mathbf{c}_2 = (0,2,1), \mathbf{c}_3 = (1,1,1), \mathbf{c}_4 = (1,2,0), \mathbf{c}_5 = (1,0,2), \mathbf{c}_6 = (2,2,2), \mathbf{c}_7 = (2,0,1), \mathbf{c}_8 = (2,1,0)\}$. Then, the Gray map defined by (2) is $\phi(u) = \mathbf{c}_u$ for all $u \in \mathbb{Z}_{3^2}$.

Carlet's Gray map from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_2^{2^{s-1}}$ [7] can be generalized to a map from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_p^{p^{s-1}}$ as follows [13]:

$$\phi(u) = (u_{s-1}, u_{s-1}, \ldots, u_{s-1}) + (u_0, \ldots, u_{s-2})Y, \tag{3}$$

where $u \in \mathbb{Z}_{p^s}$; $[u_0, u_1, \ldots, u_{s-1}]_p$ is the p-ary expansion of u, that is, $u = \sum_{i=0}^{s-1} u_i p^i$ with $u_i \in \mathbb{Z}_p$; and Y is the same matrix as in (1), that is, a matrix of size $(s-1) \times p^{s-1}$ whose columns are all the vectors in $\mathbb{Z}_p^{s-1}$.

The Gray map defined by (3) is a particular case of the one defined by (2), when we consider $P = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{p^s-1}\}$, with $\mathbf{c}_u = \phi(u)$ for all $1 \le u \le p^s - 1$. In fact, since the p-ary expansion of u, $1 \le u \le p^{s-1} - 1$, is $[u_0, u_1, \ldots, u_{s-2}, 0]_p$, the p-ary expansion of $u + jp^{s-1}$ is $[u_0, u_1, \ldots, u_{s-2}, j]_p$ and we have that $\mathbf{c}_{u+jp^{s-1}} - \mathbf{c}_u = (j, j, \ldots, j)$. From now on, throughout the paper, we only consider this particular generalization of the Gray map. We define $\Phi : \mathbb{Z}_{p^s}^n \to \mathbb{Z}_p^{np^{s-1}}$ as the component-wise extended map of ϕ.

Example 2 Let $p = 3$ and $s = 2$. Consider $Y = (0\ 1\ 2)$ as in Example 1. Table 1 shows the Gray map ϕ for the elements of $\mathbb{Z}_{3^2}$, defined by using (3). Note that this Gray map coincides with the one given in Example 1. However, if in Example 1 we consider another order of the elements of P such that $\mathbf{c}_1 \ne (0,1,2)$ or $\mathbf{c}_2 \ne (0,2,1)$, then both Gray maps would be different.

Lemma 1 *Let $u \in \mathbb{Z}_{p^s}$ and $\lambda \in \mathbb{Z}_p$. Then, $\phi(u + \lambda p^{s-1}) = \phi(u) + (\lambda, \lambda, \ldots, \lambda)$.*

Table 1 Gray map for $\mathbb{Z}_{3^2}$ by using (3)

$u \in \mathbb{Z}_{3^2}$	$[u_0, u_1]_3$	$\phi(u) = (u_1, u_1, u_1) + u_0 Y \in \mathbb{Z}_3^3$
0	$[0, 0]_3$	(0, 0, 0)
1	$[1, 0]_3$	(0, 1, 2)
2	$[2, 0]_3$	(0, 2, 1)
3	$[0, 1]_3$	(1, 1, 1)
4	$[1, 1]_3$	(1, 2, 0)
5	$[2, 1]_3$	(1, 0, 2)
6	$[0, 2]_3$	(2, 2, 2)
7	$[1, 2]_3$	(2, 0, 1)
8	$[2, 2]_3$	(2, 1, 0)

Proof Note that $u + \lambda p^{s-1} = u_1 + \lambda_0 p^{s-1} + \lambda p^{s-1} = u_1 + (\lambda_0 + \lambda) p^{s-1}$, where $u_1 \in \{0, \ldots, p^{s-1} - 1\}$ and $\lambda_0 \in \mathbb{Z}_p$. Then, by the definition of ϕ, $\phi(u + \lambda p^{s-1}) = \phi(u_1) + (\lambda_0 + \lambda, \ldots, \lambda_0 + \lambda) = \phi(u_1) + (\lambda_0, \ldots, \lambda_0) + (\lambda, \ldots, \lambda) = \phi(u) + (\lambda, \ldots, \lambda)$. □

Corollary 1 *Let $\lambda, \mu \in \mathbb{Z}_p$. Then, $\phi(\lambda\mu p^{s-1}) = \lambda\phi(\mu p^{s-1}) = \lambda\mu\phi(p^{s-1})$.*

Proof By the definition of ϕ, we have that $\phi(\mu p^{s-1}) = (\mu, \ldots, \mu)$. Then, $\phi(\lambda\mu p^{s-1}) = (\lambda\mu, \ldots, \lambda\mu) = \lambda(\mu, \ldots, \mu) = \lambda\phi(\mu p^{s-1}) = \lambda\mu\phi(p^{s-1})$. □

Let $u, v \in \mathbb{Z}_{p^s}$ and $[u_0, u_1, \ldots, u_{s-1}]_p$, $[v_0, v_1, \ldots, v_{s-1}]_p$ be the p-ary expansions of u and v, respectively, i.e. $u = \sum_{i=0}^{s-1} u_i p^i$ and $v = \sum_{i=0}^{s-1} v_i p^i$. We define two operations "$\oplus_p$" and "$\odot_p$" between elements in $\mathbb{Z}_{p^s}$ as $u \oplus_p v = \sum_{i=0}^{s-1} r_i p^i$, where $u_i + v_i = r_i$ in $\mathbb{Z}_p$, and $u \odot_p v = \sum_{i=0}^{s-1} t_i p^i$, where

$$t_i = \begin{cases} 1 \text{ if } \quad u_i + v_i \geq p, \\ 0 \text{ otherwise.} \end{cases}$$

Note that the p-ary expansion of $u \oplus_p v$ is $[r_0, r_1, \ldots, r_{s-1}]_p = [u_0 + v_0, \ldots, u_{s-1} + v_{s-1}]_p$ and the p-ary expansion of $u \odot_p v$ is $[t_0, t_1, \ldots, t_{s-1}]_p$, where $t_i \in \{0, 1\}$. We denote in the same way, "$\oplus_p$" and "$\odot_p$", the component-wise operation.

Proposition 1 *Let $u, v \in \mathbb{Z}_{p^s}$. Then, $\phi(u) + \phi(v) = \phi(u \oplus_p v)$.*

Proof Let $[u_0, u_1, \ldots, u_{s-1}]_p$, $[v_0, v_1, \ldots, v_{s-1}]_p$ be the p-ary expansions of u and v, respectively. Let $\mathbf{y}_i$ be the $(i+1)$-th row of Y, $0 \leq i \leq s-2$. Then, $\phi(u) = (u_{s-1}, u_{s-1}, \ldots, u_{s-1}) + \sum_{i=0}^{s-2} u_i \mathbf{y}_i$ and $\phi(v) = (v_{s-1}, v_{s-1}, \ldots, v_{s-1}) + \sum_{i=0}^{s-2} v_i \mathbf{y}_i$. Therefore, $\phi(u) + \phi(v) = (r_{s-1}, r_{s-1}, \ldots, r_{s-1}) + \sum_{i=0}^{s-2} r_i \mathbf{y}_i = \phi(u \oplus_p v)$, where $r_i = u_i + v_i$ in $\mathbb{Z}_p$ for $0 \leq i \leq s-1$. □

Proposition 2 *Let $u, v \in \mathbb{Z}_{p^s}$. Then, $u \oplus_p v = u + v - p(u \odot_p v)$.*

Proof Let $[u_0, u_1, \ldots, u_{s-1}]_p$, $[v_0, v_1, \ldots, v_{s-1}]_p$ be the p-ary expansions of u and v, respectively. Note that $0 \leq u_i + v_i \leq 2p - 2$. By the division algorithm for integers, we can write $u_i + v_i = pt_i + r_i$, where t_i is 1 if $u_i + v_i \geq p$ and it is 0 otherwise, and $0 \leq r_i \leq p - 1$. Then, we have $u + v = \sum_{i=0}^{s-1}(u_i + v_i)p^i = \sum_{i=0}^{s-1}(pt_i + r_i)p^i = p\sum_{i=0}^{s-1} t_i p^i + \sum_{i=0}^{s-1} r_i p^i = p(u \odot_p v) + u \oplus_p v$. Therefore, $u \oplus_p v = u + v - p(u \odot_p v)$. □

Corollary 2 *Let $u, v \in \mathbb{Z}_{p^s}$. Then, $\phi(u) + \phi(v) = \phi(u + v - p(u \odot_p v))$.*

Proof The result follows from Proposition 1 and Proposition 2. □

Corollary 3 *Let $u, v \in \mathbb{Z}_{p^s}$. Then, $p^{s-1}u \oplus_p v = p^{s-1}u + v$.*

Proof Let $[u_0, u_1, \ldots, u_{s-1}]_p$, $[v_0, v_1, \ldots, v_{s-1}]_p$ be the p-ary expansions of u and v, respectively. We have that $[0, \ldots, 0, u_0]_p$ is the p-ary expansion of $p^{s-1}u$, so $p^{s-1}u \odot_p v$ is p^{s-1} if $u_0 + v_{s-1} \geq p$ and it is 0 otherwise. In any case, $p(p^{s-1}u \odot_p v) = 0$. Hence, the result follows from Proposition 2. □

Corollary 4 *Let $u \in \mathbb{Z}_{p^s}$ and $[u_0, u_1, \ldots, u_{s-1}]_p$ its p-ary expansion. Then, for any $i \in \{0, \ldots, s-1\}$, $\phi(u) + \phi(p^i) = \phi(u + p^i - p^{i+1}t_i)$, where*

$$t_i = \begin{cases} 1 \text{ if } u_i = p-1, \\ 0 \text{ otherwise.} \end{cases}$$

Corollary 5 *Let $u, v \in \mathbb{Z}_{p^s}$. Then, $\phi(p^{s-1}u + v) = \phi(p^{s-1}u) + \phi(v)$.*

Proof The result follows from Proposition 1 and Corollary 3. □

Note that Lemma 1 and Corollary 1 are true for any Gray map ϕ defined by (2). However, Proposition 1 is only true if we consider the one defined by (3). For example, if $\phi(1) = (1, 0, 2)$ and $\phi(2) = (1, 2, 0)$, then $\phi(2) + \phi(4) = \phi(2) + \phi(1 + 3) = \phi(2) + \phi(1) + (1, 1, 1) = (0, 0, 0)$, but $\phi(2 \oplus_p 4) = \phi(3) = (1, 1, 1)$.

From [8], the homogeneous weight of an element $u \in \mathbb{Z}_{p^s}$ is defined by

$$\mathrm{wt}^*(u) = \begin{cases} 0 & \text{if } u = 0, \\ p^{s-1} & \text{if } u \in p^{s-1}\mathbb{Z}_{p^s} \setminus \{0\}, \\ (p-1)p^{s-2} & \text{otherwise,} \end{cases} \tag{4}$$

and the corresponding homogeneous distance of $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{Z}_{p^s}^n$ is defined as follows: $d^*(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^n \mathrm{wt}^*(u_i - v_i)$. Note that Carlet's Gray map is an isometry which transforms homogeneous distances defined in $\mathbb{Z}_{p^s}^n$ to Hamming distances defined in $\mathbb{Z}_p^{np^{s-1}}$.

Proposition 3 *Let $u, v \in \mathbb{Z}_{p^s}$ be two distinct elements. Then, $\phi(u) - \phi(v) = \phi(u - v) = (\lambda, \ldots, \lambda)$ if $u - v = \lambda p^{s-1} \in p^{s-1}\mathbb{Z}_{p^s} \setminus \{0\}$, and $\phi(u) - \phi(v)$ contains every element of $\mathbb{Z}_p$ exactly p^{s-2} times if $u - v \in \mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$.*

Proof First, if $u - v = \lambda p^{s-1} \in p^{s-1}\mathbb{Z}_{p^s} \setminus \{0\}$, then by Lemma 1, $\phi(u) = \phi(v) + (\lambda, \ldots, \lambda)$ with $\lambda \neq 0$. So, $\phi(u) - \phi(v) = (\lambda, \ldots, \lambda) = \phi(\lambda p^{s-1}) = \phi(u - v)$.

Assume now that $u - v \in \mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$. Then, without loss of generality, either $u \in p^{s-1}\mathbb{Z}_{p^s}$, $v \in \mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$ or $u, v \in \mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$. For the first case, $\phi(u) = (\lambda_1, \ldots, \lambda_1)$ and $\phi(v) = \phi(v_1) + (\lambda_2, \ldots, \lambda_2)$, where $v_1 \in \{1, 2, \ldots, p^{s-1} - 1\}$ and $\lambda_1, \lambda_2 \in \mathbb{Z}_p$. Note that $\phi(v_1)$ is a nonzero row of the GH matrix $H(p, p^{s-2})$ corresponding to the GH code $\phi(\mathbb{Z}_{p^s})$. Therefore, $\phi(v_1)$ contains every element of $\mathbb{Z}_p$ exactly p^{s-2} times and hence $\phi(u) - \phi(v)$ contains every element of $\mathbb{Z}_p$ exactly p^{s-2} times. For the second case, $\phi(u) = \phi(u_1) + (\lambda_1, \ldots, \lambda_1)$ and $\phi(v) = \phi(v_1) + (\lambda_2, \ldots, \lambda_2)$, where $u_1, v_1 \in \{1, 2, \ldots, p^{s-1} - 1\}$ and $\lambda_1, \lambda_2 \in \mathbb{Z}_p$. Again, note that both $\phi(u_1)$ and $\phi(v_1)$ are nonzero rows of $H(p, p^{s-2})$, so they contain every element of $\mathbb{Z}_p$ exactly p^{s-2} times. Thus, in this case, $\phi(u) - \phi(v)$ contains every element of $\mathbb{Z}_p$ exactly p^{s-2} times. □

Proposition 4 *Let $u, v \in \mathbb{Z}_{p^s}$. Then, $d_H(\phi(u), \phi(v)) = \mathrm{wt}_H(\phi(u - v))$.*

Proof If $u = 0$ or $v = 0$, the result is trivially true. We assume that $u \neq 0$ and $v \neq 0$, and we consider three cases. First, if $u = v$, the result is true trivially. Second, if $u - v \in p^{s-1}\mathbb{Z}_{p^s} \setminus \{0\}$, then by Proposition 3, $\phi(u) - \phi(v) = \phi(u - v)$, and hence $d_H(\phi(u), \phi(v)) = \mathrm{wt}_H(\phi(u - v))$. Finally, assume that $u - v \in \mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$. Again, by Proposition 3, $\phi(u) - \phi(v)$ contains every element of $\mathbb{Z}_p$ exactly p^{s-2} times, and hence $d_H(\phi(u), \phi(v)) = (p - 1)p^{s-2} = \mathrm{wt}_H(\phi(u - v))$. □

3 Construction of $\mathbb{Z}_{p^s}$-additive GH codes

The description of generator matrices having minimum number of rows for $\mathbb{Z}_4$-additive Hadamard codes, and an iterative construction of these matrices, are given in [18]. In [19], $\mathbb{Z}_{2^s}$-additive Hadamard codes are defined for $s > 2$, and an iterative construction is given in [11]. In this section, we generalize these results for $\mathbb{Z}_{p^s}$-additive GH codes with $s \geq 2$ and p an odd prime. Specifically, we define an iterative construction for the generator matrices and establish that they generate $\mathbb{Z}_{p^s}$-additive GH codes, as in [11] for $p = 2$. The generalization of the construction is quite straightforward, but the proof that the codes are GH is different from the binary case. This result has also been obtained independently in [1] by using another approach and considering Butson Hadamard matrices.

Let $T_i = \{j \cdot p^{i-1} : j \in \{0, 1, \ldots, p^{s-i+1} - 1\}\}$ for all $i \in \{1, \ldots, s\}$. Note that $T_1 = \{0, \ldots, p^s - 1\}$. Let $t_1, t_2, \ldots, t_s$ be non-negative integers with $t_1 \geq 1$. Consider the matrix $A_p^{t_1,\ldots,t_s}$ whose columns are exactly all the vectors of the form $\mathbf{z}^T$, $\mathbf{z} \in \{1\} \times T_1^{t_1-1} \times T_2^{t_2} \times \cdots \times T_s^{t_s}$. We write $A^{t_1,\ldots,t_s}$ instead of $A_p^{t_1,\ldots,t_s}$ when the value of p is clear by the context.

Let $\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \mathbf{p^s - 1}$ be the vectors having the elements $0, 1, 2, \ldots, p^s - 1$ from $\mathbb{Z}_{p^s}$ repeated in each coordinate, respectively.

Example 3 For $p = 3$ and $s = 3$, we have the following matrices:

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

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

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

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

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

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

$$A_i = \begin{pmatrix} A & A & \cdots & A \\ 0 \cdot \mathbf{p^{i-1}} & 1 \cdot \mathbf{p^{i-1}} & \cdots & (p^{s-i+1} - 1) \cdot \mathbf{p^{i-1}} \end{pmatrix}. \tag{5}$$

Finally, permuting the rows of A_i, we obtain a matrix $A^{t'_1,\ldots,t'_s}$, 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 $A^{t'_1,\ldots,t'_s}$.

Example 4 Let $p = 3$ and $s = 3$ as in Example 3. From the matrix $A^{1,0,0} = (1)$, we obtain the matrix $A^{2,0,0}$; and from $A^{2,0,0}$ we can construct $A^{2,0,1}$, where $A^{2,0,0}$ and $A^{2,0,1}$ are the matrices given in Example 3. Note that we can also generate another matrix $A^{2,0,1}$ as follows: from $A^{1,0,0} = (1)$, we obtain $A^{1,0,1} = \begin{pmatrix} \mathbf{1} \\ \mathbf{k} \end{pmatrix}$, where $\mathbf{k} = (0, 9, 18)$, given in Example 3; and from $A^{1,0,1}$, we can construct the matrix

$$A_1 = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \cdots & \mathbf{1} & \mathbf{1} \\ \mathbf{k} & \mathbf{k} & \mathbf{k} & \mathbf{k} & \cdots & \mathbf{k} & \mathbf{k} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \cdots & \mathbf{25} & \mathbf{26} \end{pmatrix}.$$

Then, after permuting the rows of A_1, we have a matrix

$$A^{2,0,1} = \begin{pmatrix} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \cdots & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \cdots & \mathbf{25} & \mathbf{26} \\ \mathbf{k} & \mathbf{k} & \mathbf{k} & \mathbf{k} & \cdots & \mathbf{k} & \mathbf{k} \end{pmatrix},$$

which is different to the matrix $A^{2,0,1}$ of Example 3. These two matrices $A^{2,0,1}$ generate permutation equivalent codes.

In this paper, we consider that the matrices $A^{t_1,t_2,\ldots,t_s}$ are constructed recursively starting from $A^{1,0,\ldots,0}$ in the following way. First, we add $t_1 - 1$ rows of order p^s, in order to obtain $A^{t_1,0,\ldots,0}$; then t_2 rows of order p^{s-1} to generate $A^{t_1,t_2,0,\ldots,0}$; and so on, until we add t_s rows of order p to achieve $A^{t_1,t_2,\ldots,t_s}$.

Let $\mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive code generated by the matrix $A^{t_1,\ldots,t_s}$, where $t_1, \ldots, t_s \geq 0$ with $t_1 \geq 1$. Let $n = p^{t-s+1}$, where $t = \left(\sum_{i=1}^{s}(s - i + 1) \cdot t_i\right) - 1$. It is easy to see that $\mathcal{H}^{t_1,\ldots,t_s}$ is of length n and has $|\mathcal{H}^{t_1,\ldots,t_s}| = p^s n = p^{t+1}$ codewords. Note that this code is of type $(n; t_1, t_2, \ldots, t_s)$. Let $H^{t_1,\ldots,t_s} = \Phi(\mathcal{H}^{t_1,\ldots,t_s})$ be the corresponding $\mathbb{Z}_{p^s}$-linear code.

Example 5 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, $F_H = \{(0, 0, 0), (0, 1, 2), (0, 2, 1)\}$ and $C_H = \bigcup_{\alpha \in \mathbb{Z}_3}(F_H + \alpha\mathbf{1})$, which coincides with the code P given in Example 1. Note that C_H is a linear GH code over $\mathbb{Z}_3$ of length 3, and $C_H = H^{1,0} = \Phi(\mathcal{H}^{1,0}) = \Phi(\mathbb{Z}_9)$, where $\mathcal{H}^{1,0}$ is generated by $A^{1,0} = (1)$. More generally, we can consider the normalized GH matrix $H(p, 1)$ given by the multiplicative table over $\mathbb{Z}_p$. Then, the corresponding GH code over $\mathbb{Z}_p$ is $C_H = H^{1,0} = \Phi(\mathcal{H}^{1,0}) = \Phi(\mathbb{Z}_{p^2})$, which is linear.

Example 6 The code $\mathcal{H}^{1,0,\ldots,0}$ is generated by $A^{1,0,\ldots,0} = (1)$, so $\mathcal{H}^{1,0,\ldots,0} = \mathbb{Z}_{p^s}$. This linear code over $\mathbb{Z}_{p^s}$ has length $n = 1$ and cardinality p^s. Thus, the code $H^{1,0,\ldots,0} = \Phi(\mathcal{H}^{1,0,\ldots,0})$ over $\mathbb{Z}_p$ has length $N = p^{s-1}$ and cardinality $p^s = Np$. Actually, $H^{1,0,\ldots,0} = \Phi(\mathbb{Z}_{p^s})$ is the linear GH code over $\mathbb{Z}_p$ of length p^{s-1} used to define the Gray map Φ, so it is generated by (1).

The result given by Theorem 1 is already proved in [19] and [11] for $p = 2$. In [19], it is shown that each $\mathbb{Z}_{2^s}$-linear Hadamard code is equivalent to $H^{t_1,\ldots,t_s}$ for some $t_1, \ldots, t_s \geq 0$

with $t_1 \geq 1$, considering a generalized Gray map that includes the one given by Carlet. In [11], another technique is used to obtain that the $\mathbb{Z}_{2^s}$-linear codes $H^{t_1,\ldots,t_s}$ are Hadamard. For $p \geq 3$ prime, the result is already proved in [1]. However, we include another proof which is different, and it is not a generalization of the ones given in [19] and [11] neither.

Let $\mathcal{G}$ be a generator matrix of a $\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ of length n. Then, $(\mathcal{G} \cdots \mathcal{G})$ is a generator matrix of the r-fold replication code of $\mathcal{C}$, $(\mathcal{C}, \ldots, \mathcal{C}) = \{(\mathbf{c}, \ldots, \mathbf{c}) : \mathbf{c} \in \mathcal{C}\}$, of length $r \cdot n$.

Theorem 1 *Let $t_1, \ldots, t_s$ be non-negative 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 $N = p^t$, with $t = (\sum_{i=1}^{s}(s-i+1)\cdot t_i)-1$ and $n = p^{t-s+1}$.*

Proof Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive code of length n generated by the matrix $A = A^{t_1,\ldots,t_s}$. We can write $\mathcal{H} = \cup_{\lambda\in\mathbb{Z}_p}(A_{\mathcal{H}} + \lambda \cdot \mathbf{p^{s-1}})$, where $A_{\mathcal{H}} = \{\mathbf{h} \pmod{p^{s-1}} : \mathbf{h} \in \mathcal{H}\}$ and $A_{\mathcal{H}} + \lambda \cdot \mathbf{p^{s-1}} = \{\mathbf{h} + \lambda \cdot \mathbf{p^{s-1}} : \mathbf{h} \in A_{\mathcal{H}}\}$ for any $\lambda \in \mathbb{Z}_p$. Then, by Lemma 1, $H = \Phi(\mathcal{H}) = \cup_{\lambda\in\mathbb{Z}_p}(\Phi(A_{\mathcal{H}}) + \lambda \cdot \mathbf{1})$. The code H has length $p^t = np^{s-1}$ and cardinality $p^{t+1} = np^s$. Then, it is enough to proof that $\Phi(A_{\mathcal{H}})$ corresponds to the rows of a GH matrix $H(p, p^{s-2}n)$. We take two distinct elements $\mathbf{u}, \mathbf{v}$ from $A_{\mathcal{H}}$. Now, we have to show that $\Phi(\mathbf{u}) - \Phi(\mathbf{v})$ contains every element of $\mathbb{Z}_p$ exactly $p^{s-2}n$ times.

We consider two cases depending on the order of $\mathbf{u} - \mathbf{v}$. First, if $o(\mathbf{u} - \mathbf{v}) = p$, then, by construction, $\mathbf{u} - \mathbf{v}$ contains every element of $p^{s-1}\mathbb{Z}_{p^s}$ exactly n/p times. Thus, $\Phi(\mathbf{u} - \mathbf{v})$ contains every element of $\mathbb{Z}_p$ exactly $p^{s-1}n/p = p^{s-2}n$ times. By Proposition 3, $\Phi(\mathbf{u}-\mathbf{v}) = \Phi(\mathbf{u}) - \Phi(\mathbf{v})$ and hence $\Phi(\mathbf{u}) - \Phi(\mathbf{v})$ contains every element of $\mathbb{Z}_p$ exactly $p^{s-2}n$ times. Second, if $o(\mathbf{u} - \mathbf{v}) > p$, then by construction, $\mathbf{u} - \mathbf{v}$ contains every element of $p^{s-1}\mathbb{Z}_{p^s}$ exactly α times, $\alpha \geq 0$, and the remaining $n - p\alpha$ coordinates are from $\mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$. So, by Proposition 3, $\Phi(\mathbf{u}) - \Phi(\mathbf{v})$ contains every element of $\mathbb{Z}_p$ exactly $\alpha\, p^{s-1} + (n - p\alpha)\, p^{s-2} = p^{s-2}n$ times. □

Example 7 Let $\mathcal{H}^{2,0,0}$ be the $\mathbb{Z}_{27}$-additive code generated by $A^{2,0,0}$ given in Example 3. The $\mathbb{Z}_{27}$-linear code $H^{2,0,0} = \Phi(\mathcal{H}^{2,0,0})$ has length $N = 27 \cdot 9 = 3^5$, $pN = 3^6$ codewords and minimum (Hamming) distance $N(p-1)/p = 162$. Therefore, it is a $\mathbb{Z}_{27}$-linear GH code.

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

As shown in [18, 21], the codes H_2^{1,t_2} and H_2^{2,t_2}, $t_2 \geq 0$, are the only $\mathbb{Z}_4$-linear Hadamard codes which are linear. In [14], it is proved that the codes $H_2^{1,0,\ldots,0,t_s}$, $t_s \geq 0$, are linear. Indeed, in [11], it is shown that for $s > 2$ the codes $H_2^{1,0,\ldots,0,1,t_s}$ and $H_2^{1,0,\ldots,0,t_s}$, $t_s \geq 0$, are the only $\mathbb{Z}_{2^s}$-linear Hadamard codes which are linear. The next result shows that for any $p \geq 3$ prime, $s \geq 2$ and $t_s \geq 0$, $H_p^{1,0,\ldots,0,t_s}$ are the only $\mathbb{Z}_{p^s}$-linear GH codes which are linear. Note that this result for $p \geq 3$ does not coincide with the case $p = 2$.

Theorem 2 *The $\mathbb{Z}_{p^s}$-linear GH codes $H^{1,0,\ldots,0,t_s}$, with $p \geq 3$ prime, $s \geq 2$ and $t_s \geq 0$, are linear.*

Proof We prove that these codes are linear by induction on t_s. By Example 6, $H^{1,0,\ldots,0}$ is linear. Assume, $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{1,0,\ldots,0,t_s}$, $s \geq 2$ and $t_s \geq 0$, is linear. Now, we

have to show that $H_s = H^{1,0,\ldots,0,t_s+1}$ is linear. By the iterative construction,

$$H_s = \{\Phi((\mathbf{h}, \mathbf{h}, \ldots, \mathbf{h}) + \lambda(\mathbf{0}, \mathbf{p^{s-1}}, 2\mathbf{p^{s-1}}, \ldots, (p-1)\mathbf{p^{s-1}}) : \mathbf{h} \in \mathcal{H}, \lambda \in \mathbb{Z}_p\}$$
$$= \{(\Phi(\mathbf{h}), \Phi(\mathbf{h} + \lambda\mathbf{p}^{s-1}), \Phi(\mathbf{h} + \lambda 2\mathbf{p}^{s-1}), \ldots, \Phi(\mathbf{h} + \lambda(p-1)\mathbf{p}^{s-1})) :$$

$\mathbf{h} \in \mathcal{H}, \lambda \in \mathbb{Z}_p\}$,

and, by Corollaries 5 and 1, it is equal to

$$\{(\Phi(\mathbf{h}), \Phi(\mathbf{h}) + \lambda\Phi(\mathbf{p}^{s-1}), \Phi(\mathbf{h}) + \lambda\Phi(2\mathbf{p}^{s-1}), \ldots, \Phi(\mathbf{h}) + \lambda\Phi((p-1)\mathbf{p}^{s-1})) :$$
$$\mathbf{h} \in \mathcal{H}, \lambda \in \mathbb{Z}_p\} = \{(\mathbf{h}', \mathbf{h}' + \lambda \cdot \mathbf{1}, \mathbf{h}' + \lambda \cdot \mathbf{2}, \ldots, \mathbf{h}' + \lambda \cdot (\mathbf{p-1})) : \mathbf{h}' \in H, \lambda \in \mathbb{Z}_p\}.$$

Thus, we can partition H_s into p-blocks, $H_{s0}, H_{s1}, H_{s2}, \ldots, H_{s(p-1)}$, where

$$H_{s0} = \{(\mathbf{h}', \mathbf{h}', \ldots, \mathbf{h}') : \mathbf{h}' \in H\},$$
$$H_{s1} = \{(\mathbf{h}', \mathbf{h}' + \mathbf{1}, \mathbf{h}' + \mathbf{2}, \ldots, \mathbf{h}' + (\mathbf{p-1})) : \mathbf{h}' \in H\},$$
$$H_{s2} = \{(\mathbf{h}', \mathbf{h}' + \mathbf{2}, \mathbf{h}' + \mathbf{4}, \ldots, \mathbf{h}' + \mathbf{2}(\mathbf{p-1})) : \mathbf{h}' \in H\},$$
$$\ldots.$$
$$H_{s(p-1)} = \{(\mathbf{h}', \mathbf{h}' + (\mathbf{p-1}), \mathbf{h}' + \mathbf{2}(\mathbf{p-1}), \ldots, \mathbf{h}' + \mathbf{1})) : \mathbf{h}' \in H\}.$$

Since H is linear, it is clear that if we take any two vectors from H_s, then their addition belongs to any one of the blocks $H_{s0}, H_{s1}, H_{s2}, \cdots, H_{s(p-1)}$. Therefore, H_s is linear. □

Theorem 3 *The $\mathbb{Z}_{p^s}$-linear GH codes $H^{1,0,\ldots,0,t_s}$, 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.*

Proof By Theorem 2, we have that the codes $H^{1,0,\ldots,0,t_s}$ are linear.

Let $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$. For any $i \in \{1, \ldots, s\}$, we define $H_i = \Phi(\mathcal{H}_i)$, where $\mathcal{H}_i = \mathcal{H}^{t'_1,\ldots,t'_s}$, $t'_i = t_i + 1$ and $t'_j = t_j$ for $j \neq i$. We consider that $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{1,0,\ldots,0}$. Now, we prove that H_i is nonlinear for any $i \in \{1, \ldots, s-1\}$.

Note that the generator matrix of $\mathcal{H}_i$ has two rows: $\mathbf{w}_1 = \mathbf{1}$ and $\mathbf{w}_2 = p^{i-1}(0, 1, \ldots, p^{s+1-i} - 1)$. Let w_{2j} be the j-th coordinate of $\mathbf{w}_2$ and $[(w_{2j})_0, (w_{2j})_1, \ldots, (w_{2j})_{s-1}]_p$ its p-ary expansion. By Corollary 4, $\phi(w_{2j}) + \phi(p^{i-1}) = \phi(w_{2j} + p^{i-1} - z_j)$, where $z_j = p^i$ if $(w_{2j})_{i-1} = p - 1$, and 0 otherwise. Note that $w_{2j} = p^{i-1}(j-1)$, so $(w_{2j})_{i-1} = p - 1$ if and only if $j \in \{p, 2p, \ldots, p^{s+1-i}\}$. Then, $\Phi(\mathbf{w}_2) + \Phi(\mathbf{p^{i-1}}) = \Phi(\mathbf{w}_2 + \mathbf{p^{i-1}} - \mathbf{z})$, where $\mathbf{z} = (z_1, z_2, \ldots, z_{p^{s+1-i}}) \in \mathbb{Z}_{p^s}^{p^{s+1-i}}$, $z_j = p^i$ for $j \in \{p, 2p, \ldots, p^{s+1-i}\}$ and $z_j = 0$ otherwise. Therefore, we just need to show that $\mathbf{z} \notin \mathcal{H}_i$.

Note that $\mathrm{wt}_H(\Phi(\mathbf{z})) = p^{s-i} \cdot \mathrm{wt}_H(\phi(p^i))$. If $i = s-1$, then $\mathrm{wt}_H(\Phi(\mathbf{z})) = p \cdot p^{s-1} = p^s$. If $i \in \{1, \ldots, s-2\}$, then $\mathrm{wt}_H(\Phi(\mathbf{z})) = p^{s-i} \cdot (p-1)p^{s-2} = p^{2s-i-2}(p-1)$. However, the minimum distance of H_i is $p^{s-2}(p-1)p^{s+1-i} = p^{2s-i-1}(p-1)$. Therefore, $\Phi(\mathbf{z}) \notin H_i$, for $i \in \{1, \ldots, s-1\}$.

Finally, in general, for $H = \Phi(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$, we prove that if H is nonlinear, then H_i is nonlinear for any $i \in \{1, \ldots, s\}$. Assume that H_i is linear. Then, by the iterative construction (5), for any $\mathbf{u}, \mathbf{v} \in \mathcal{H}$, we have that $(\mathbf{u}, \ldots, \mathbf{u}), (\mathbf{v}, \ldots, \mathbf{v}) \in \mathcal{H}_i$. Moreover, since H_i is linear, $\Phi((\mathbf{u}, \ldots, \mathbf{u})) + \Phi((\mathbf{v}, \ldots, \mathbf{v})) = \Phi((\mathbf{a}, \ldots, \mathbf{a}) + \lambda \cdot p^{i-1}(0, 1, \ldots, p^{s-i+1} - 1)) \in H_i$, where $\mathbf{a} \in \mathcal{H}$ and $\lambda \in \mathbb{Z}_{p^s}$. Therefore, $\Phi(\mathbf{u}) + \Phi(\mathbf{v}) = \Phi(\mathbf{a}) \in H$, and we have that H is linear and the result follows. □

Example 8 Considering all non-negative integer solutions with $t_1 \geq 1$ of the equation $4 = 3t_1 + 2t_2 + t_3 - 1$, we have that the $\mathbb{Z}_{p^3}$-linear GH codes of length p^4 are the following: $H_p^{1,0,2}$ and $H_p^{1,1,0}$. By Theorem 3, we have that $H_p^{1,0,2}$ is linear, so $\ker(H_p^{1,0,2}) = 5$. By the same theorem, we also have that $H_p^{1,1,0}$ is nonlinear, so $\ker(H_p^{1,1,0}) = 3 < 5$.

Example 9 Considering all non-negative integer solutions with $t_1 \geq 1$ of the equation $5 = 3t_1+2t_2+t_3-1$, we have that the $\mathbb{Z}_{p^3}$-linear GH codes of length p^5 are the following: $H_p^{1,0,3}$, $H_p^{1,1,1}$ and $H_p^{2,0,0}$. By Theorem 3, we have that $H_p^{1,0,3}$ is linear, so $\ker(H_p^{1,0,3}) = 6$. By the same theorem, we also have that $H_p^{1,1,1}$ and $H_p^{2,0,0}$ are nonlinear, so $\ker(H_p^{1,1,1}) = 4 < 6$ and $\ker(H_p^{2,0,0}) = 2 < 6$.

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

For $\mathbb{Z}_4$-linear Hadamard codes and $\mathbb{Z}_{2^s}$-linear Hadamard codes with $s > 2$, the kernel and its dimension are given in [18, 21] and [11], respectively. In this section, we generalize these results for $\mathbb{Z}_{p^s}$-linear GH codes with $p \geq 3$ prime and $s \geq 2$. First, we establish a lower bound on the dimension of the kernel, and then we construct a basis of the kernel and give its exact dimension. We see that all the basis vectors of the kernel for $p \geq 3$ are the generalized forms of the nonlinear ones for $p = 2$ except $\Phi(\sum_{i=0}^{s-2} \mathbf{p^i})$, which does not belong to the kernel, and so the dimension of the kernel is decreased by one for $p \geq 3$ prime.

Let $A^{t_1,\ldots,t_s}$ be the generator matrix of $\mathcal{H}^{t_1,\ldots,t_s}$, and let $\mathbf{w}_i$ be the i-th row vector of $A^{t_1,\ldots,t_s}$. By construction, $\mathbf{w}_1 = \mathbf{1}$ and $o(\mathbf{w}_i) \leq o(\mathbf{w}_j)$ if $i > j$. We define $\sigma \in \{1, \ldots, s\}$ as the integer such that $o(\mathbf{w}_2) = p^{s+1-\sigma}$. For $\mathcal{H}^{1,0,\ldots,0}$, we define $\sigma = s$. Note that $\sigma = 1$ if $t_1 > 1$, and $\sigma = \min\{i : t_i > 0, i \in \{2, \ldots, s\}\}$ if $t_1 = 1$. In the case $\sigma = s$, the code is $\mathcal{H}^{1,0,\ldots,0,t_s}$, which is linear.

Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_{p^s}^n$ and $[u_{j,0}, u_{j,1}, \ldots, u_{j,s-1}]_p$ be the p-ary expansion of u_j, where $j \in \{1, \ldots, n\}$. Let i be an integer such that $i \in \{0, \ldots, s-1\}$. Then, we denote by $\mathbf{u}^{(i)}$ the vector having in the j-th coordinate the i-th element of the p-ary expansion of u_j, that is, $\mathbf{u}^{(i)} = (u_{1,i}, \ldots, u_{n,i}) \in \mathbb{Z}_p^n$.

Proposition 5 *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1, \ldots, t_s)$ with $p \geq 3$ prime. Let $\mathcal{H}_p$ be the subcode of $\mathcal{H}$ which contains all the codewords of order p. Let $M = \{\mathbf{p^m}\}_{m=0}^{\sigma-2}$ if $\sigma \geq 2$, and $M = \emptyset$ if $\sigma = 1$. Then,*

$$\langle \Phi(\mathcal{H}_p), \Phi(M) \rangle \subseteq K(\Phi(\mathcal{H}))$$

and $ker(\Phi(\mathcal{H})) \geq (\sum_{i=1}^{s} t_i) + \sigma - 1$.

Proof Let $H = \Phi(\mathcal{H})$ and $\tau = \sum_{i=1}^{s} t_i$. Let $Q = \{(o(\mathbf{w}_k)/p)\mathbf{w}_k\}_{k=1}^{\tau}$. Since $\mathcal{H}_p$ contains all the elements of $\mathcal{H}$ of order p, we have that the set $\Phi(Q)$ is a basis for the linear subcode $H_p = \Phi(\mathcal{H}_p)$ of H over $\mathbb{Z}_p$. By Corollary 5, for all $\mathbf{b} \in \mathcal{H}_p$ and $\mathbf{u} \in \mathcal{H}$, we have that $\Phi(\mathbf{b}) + \Phi(\mathbf{u}) = \Phi(\mathbf{b} + \mathbf{u}) \in H$ and, therefore, $H_p \subseteq K(H)$.

Assume $\sigma \geq 2$. Now, we prove that $\Phi(\mathbf{p^m}) \in K(H)$ for all $m \in \{0, \ldots, \sigma-2\}$. Equivalently, we show that $\Phi(\mathbf{p^m}) + \Phi(\mathbf{u}) \in H$ for all $\mathbf{u} \in \mathcal{H}$. If $\mathbf{u} \in \mathcal{H}$, then $\mathbf{u} = \lambda \cdot \mathbf{1} + \mathbf{u}'$, where $\lambda \in \mathbb{Z}_{p^s}$ and $o(\mathbf{u}') \leq o(\mathbf{w}_2) = p^{s+1-\sigma}$. Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}_{p^s}^n$ and $[u_{j,0}, u_{j,1}, \ldots, u_{j,s-1}]_p$ be the p-ary expansion of u_j, $j \in \{1, \ldots, n\}$. Let $[\lambda_0, \lambda_1, \ldots, \lambda_{s-1}]_p$ be the p-ary expansion of $\lambda \in \mathbb{Z}_{p^s}$. Note that if $v \in \mathbb{Z}_{p^s}$ is of order p^i, then its p-ary expansion is of the form $[0, \ldots, 0, v_{s-i}, v_{s-i+1}, \ldots, v_{s-1}]_p$. Since $m \in \{0, \ldots, \sigma-2\}$ and $o(\mathbf{u}') \leq p^{s+1-\sigma}$, we have that $\mathbf{u}^{(m)} = (u_{1,m}, \ldots, u_{n,m}) = (\lambda_m, \ldots, \lambda_m)$. By Corollary 4, we have that $\Phi(\mathbf{p^m}) + \Phi(\mathbf{u}) = \Phi(\mathbf{p^m} + \mathbf{u} - p^{m+1}\mathbf{t_m})$, where $\mathbf{t_m} = \mathbf{1}$ or $\mathbf{t_m} = \mathbf{0}$ depending on whether $\lambda_m = p-1$ or not, respectively. Therefore, $p^{m+1}\mathbf{t_m}$ is $\mathbf{0}$ or $\mathbf{p^{m+1}}$. In both cases, $p^{m+1}\mathbf{t_m} \in \mathcal{H}$, so $\Phi(\mathbf{p^m}) + \Phi(\mathbf{u}) = \Phi(\mathbf{p^m} + \mathbf{u} - p^{m+1}\mathbf{t_m}) \in H$.

Finally, we have to see that the elements of the set $\{\Phi(Q), \Phi(M)\}$ are linearly independent. Clearly, the elements of $\Phi(Q)$, and also the elements of $\Phi(M)$, are linearly independent. By

construction, the generator matrix $A^{t_1,\ldots,t_s}$ is a block upper triangular matrix, so it is easy to see that the codewords of $\Phi(Q)$ are linearly independent of the ones of $\Phi(M)$. Therefore, we have that the dimension of the linear span of this set is $\tau+\sigma-1$, so $\ker(H) \geq \tau+\sigma-1$. □

Lemma 2 *Let $v, \lambda \in \mathbb{Z}_{p^s}$. Then, $v \odot_p \lambda = \sum_{i=0}^{s-1}(v \odot_p \lambda_i p^i)$, where $[\lambda_0, \lambda_1, \ldots, \lambda_{s-1}]_p$ is the p-ary expansion of λ.*

Proof Let $v \in \mathbb{Z}_{p^s}$ and let $[v_0, v_1, \ldots, v_{s-1}]_p$ be its p-ary expansion. By definition, we have that $v \odot_p \lambda = v \odot_p \sum_{i=0}^{s-1} \lambda_i p^i = \sum_{i=0}^{s-1} t_i p^i$, where t_i is 1 if $v_i + \lambda_i \geq p$, and 0 otherwise. Note that $t_i p^i = v \odot_p \lambda_i p^i$, so $v \odot_p \sum_{i=0}^{s-1} \lambda_i p^i = \sum_{i=0}^{s-1}(v \odot_p \lambda_i p^i)$. □

Lemma 3 *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1, \ldots, t_s)$ with $p \geq 3$ prime. Let $\mathcal{N} = \{\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{p^i} : \lambda_i \in \mathbb{Z}_p\}$ if $\sigma \leq s-1$, and $\mathcal{N} = \{\mathbf{0}\}$, otherwise. Then, $\Phi(\mathcal{N}) \cap K(\Phi(\mathcal{H})) = \{\mathbf{0}\}$.*

Proof Let $H = \Phi(\mathcal{H})$. Assume $\sigma \leq s-1$ and let $\mathbf{u} = \sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{p^i} \in \mathcal{N}$ such that $\Phi(\mathbf{u}) \in K(H)$. We want to prove that $\mathbf{u} = \mathbf{0}$. Assume that there exists $\mathbf{u} \neq \mathbf{0}$, so there exists $i_0 \in \{\sigma-1, \ldots, s-2\}$ such that $\lambda_{i_0} \neq 0$.

By construction, the second row $\mathbf{w}_2$ of $A^{t_1,\ldots,t_s}$ is a $p^{t-2s+\sigma}$-fold replication of $\mathbf{v} = p^{\sigma-1}(0, 1, \ldots, p^{s+1-\sigma}-1)$, and $o(\mathbf{w}_2) = p^{s+1-\sigma}$. By Corollary 2, we have that $\Phi(\mathbf{w}_2) + \Phi(\mathbf{u}) = \Phi(\mathbf{w}_2 + \mathbf{u} - p(\mathbf{w}_2 \odot_p \mathbf{u}))$. Since $\Phi(\mathbf{u}) \in K(H)$, $p(\mathbf{w}_2 \odot_p \mathbf{u}) \in \mathcal{H}$. Let $\mathbf{w}_2 = (w_1, w_2, \ldots, w_n)$ and $[w_{j,0}, w_{j,1}, \ldots, w_{j,s-1}]_p$ be the p-ary expansion of w_j, $j \in \{1, \ldots, n\}$. Note that, by Lemma 2, we have that $p(\mathbf{w}_2 \odot_p \mathbf{u}) = p\sum_{i=\sigma-1}^{s-2}(\mathbf{w}_2 \odot_p \lambda_i \mathbf{p^i}) = p\sum_{i=\sigma-1}^{s-2} \mathbf{T}_i p^i \in \mathcal{H}$, where $\mathbf{T}_i = (t_{1,i}, t_{2,i}, \ldots, t_{n,i})$, and $t_{j,i} = 1$ if $w_{j,i} + \lambda_i \geq p$ and $t_{j,i} = 0$ otherwise.

Let $\tau = \sum_{i=1}^{s} t_i$. Since $\sigma \leq s-1$, $\tau \geq 2$. If $\tau = 2$, then $\mathcal{H}$ has length $m = p^{s+1-\sigma}$ and the only rows in $A^{t_1,\ldots,t_s}$ are $\mathbf{1}$ and $\mathbf{w}_2$. Note that, in this case, $\mathbf{w}_2 = \mathbf{v}$. If $\tau \geq 3$, for $k \in \{3, \ldots, \tau\}$, the k-th row $\mathbf{w}_k$ of $A^{t_1,\ldots,t_s}$ contains zeros in the first $p^{s+1-\sigma}$ coordinates by construction. Hence, for $\tau \geq 2$, any element of $\mathcal{H}$ restricted to the first $p^{s+1-\sigma}$ coordinates is of the form $\mu_1\mathbf{1} + \mu_2\mathbf{v}$ for some $\mu_1, \mu_2 \in \mathbb{Z}_{p^s}$. We have that $p\sum_{i=\sigma-1}^{s-2} \mathbf{T}_i p^i$ restricted to the first $m = p^{s+1-\sigma}$ coordinates is $p\sum_{i=\sigma-1}^{s-2} \mathbf{T}'_i p^i$, where $\mathbf{T}'_i = (t_{1,i}, t_{2,i}, \ldots, t_{m,i})$. Therefore, we have to find $\mu_1, \mu_2 \in \mathbb{Z}_{p^s}$ such that $p\sum_{i=\sigma-1}^{s-2} \mathbf{T}'_i p^i = \mu_1\mathbf{1} + \mu_2\mathbf{v}$.

Since the first coordinate of $\mathbf{v}$ is 0, the first coordinate of $\mathbf{v}^{(i)}$ is 0 for all $i \in \{0, \ldots, s-1\}$. Then, we have that $\mu_1 = 0$, so

$$p\sum_{i=\sigma-1}^{s-2} \mathbf{T}'_i p^i = \mu_2\mathbf{v}. \tag{6}$$

Note that $\mathbf{v} = \sum_{i=0}^{s-1} \mathbf{v}^{(i)} p^i = \sum_{i=\sigma-1}^{s-1} \mathbf{v}^{(i)} p^i$. Let $\mathbf{x} = p\sum_{i=\sigma-1}^{s-2} \mathbf{T}'_i p^i$ and $\mathbf{y} = \mu_2\mathbf{v}$. On the one hand, we assume that $\mu_2 \in A = \{0, p^{s-\sigma+1}, \ldots, (p-1)p^{s-\sigma+1}\}$, and then $\mathbf{y} = \mathbf{0}$. Moreover, since there exists $\lambda_{i_0} \neq 0$, we have that $\mathbf{T}'_{i_0}$ has at least a nonzero coordinate, so $\mathbf{x} \neq \mathbf{0}$ and we get a contradiction. On the other hand, we assume that $\mu_2 \in \mathbb{Z}_{p^s} \setminus A$. Let $\mathbf{x}^{(i)} = (x_{1,i}, x_{2,i}, \ldots, x_{m,i})$, $\sigma \leq i \leq s-1$. Note that $x_{j,i} \in \{0, 1\}$ for all $j \in \{1, 2, \ldots, m\}$ and $i \in \{\sigma, \ldots, s-1\}$. However, since $\mathbf{v} = p^{\sigma-1}(0, 1, \ldots, p^{s+1-\sigma}-1)$, there exists $i_1 \in \{\sigma, \ldots, s-1\}$ such that the coordinates of $\mathbf{y}^{(i_1)}$ are not in $\{0, 1\}$, and hence we obtain a contradiction. Therefore, if $\mathbf{u} \neq \mathbf{0}$, then $p(\mathbf{w}_2 \odot_p \mathbf{u}) \neq \mu_1\mathbf{1} + \mu_2\mathbf{v}$ and hence $\mathbf{u} = \mathbf{0}$. □

Lemma 4 *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1, \ldots, t_s)$ with $p \geq 3$ prime. Let $\mathbf{w}_k$ be the k-th row of $A^{t_1,\ldots,t_s}$ and $\tau = \sum_{i=1}^{s} t_i$. Let $\mathcal{M} = \{\mathbf{v} = \sum_{k=2}^{\tau-t_s} \lambda_k \mathbf{w}_k : \lambda_k \in \mathbb{Z}_{p^s},\ o(\mathbf{v}) > p\}$, $\mathcal{N} = \{\sum_{i=\sigma-1}^{s-2} \lambda_i \mathbf{p}^{\mathbf{i}} : \lambda_i \in \mathbb{Z}_p\}$ if $\sigma \leq s-1$, and $\mathcal{N} = \{\mathbf{0}\}$, otherwise. Let $\mathcal{M}+\mathcal{N} = \{\mathbf{v}_\mathcal{M}+\mathbf{v}_\mathcal{N} : \mathbf{v}_\mathcal{M} \in \mathcal{M}\cup\{\mathbf{0}\}, \mathbf{v}_\mathcal{N} \in \mathcal{N}\}$. Then, $\Phi(\mathcal{M}+\mathcal{N})\cap K(\Phi(\mathcal{H})) = \{\mathbf{0}\}$.*

Proof Let $H = \Phi(\mathcal{H})$, which has length $N = n \cdot p^{s-1}$. By Lemma 3, we already know that $\Phi(\mathcal{N}) \cap K(H) = \{\mathbf{0}\}$.

Now, we prove that $\Phi(\mathcal{M}) \cap K(H) = \emptyset$. Let $\mathbf{v} = \sum_{k=2}^{\tau-t_s} \lambda_k \mathbf{w}_k = (v_1, v_2, \ldots, v_n) \in \mathcal{M}$. Since $o(\mathbf{v}) > p$ and $o(\mathbf{w}_k) \leq p^{s+1-\sigma}$, $o(\mathbf{v}) = p^q$ for some $2 \leq q \leq s+1-\sigma$. By the iterative construction (5) of $A^{t_1,\ldots,t_s}$, we know that all the elements of $\mathbb{Z}_{p^s}$ of order equal to or less than p^q appear as a coordinate of $\mathbf{v}$. Let $[v_{j,0}, v_{j,1}, \ldots, v_{j,s-1}]_p$ be the p-ary expansion of v_j, $j \in \{1, \ldots, n\}$. By Corollary 4, we have that $\Phi(\mathbf{v})+\Phi(\mathbf{p^{s-q}}) = \Phi(\mathbf{v}+\mathbf{p^{s-q}}-p^{s-q+1}\mathbf{T}_{s-q})$, where $\mathbf{T}_{s-q} = (t_{1,(s-q)}, t_{2,(s-q)}, \ldots, t_{n,(s-q)})$, and for $j \in \{1, \ldots, n\}$, $t_{j,(s-q)} = 1$ if $v_{j,(s-q)} = p-1$ and 0 otherwise. Again, it is enough to see that $p^{s-q+1}\mathbf{T}_{s-q} \notin \mathcal{H}$ to prove that $\Phi(\mathbf{v}) \notin K(H)$. Since, $\mathbf{v} = \sum_{k=2}^{\tau-t_s} \lambda_k \mathbf{w}_k = (v_1, v_2, \ldots, v_n)$ and $o(\mathbf{v}) = p^q$ for some $2 \leq q \leq s+1-\sigma$, we have that, by construction, $\mathbf{v}$ contains every element of $p^{s-1}\mathbb{Z}_{p^s}$ exactly α times, $\alpha > 0$, and the remaining $n - p\alpha$ coordinates are from $\mathbb{Z}_{p^s} \setminus p^{s-1}\mathbb{Z}_{p^s}$. So, $\mathrm{wt}_H(\Phi(p^{s-q+1}\mathbf{T}_{s-q})) \leq (n-p\alpha)\cdot(p-1)p^{s-2} < n\cdot(p-1)p^{s-2} = N(p-1)/p = d(H)$. Therefore, $\Phi(\mathbf{v}) \notin K(H)$ and $\Phi(\mathcal{M}) \cap K(H) = \emptyset$.

Now, we prove that $\Phi(\mathcal{M}+\mathcal{N}) \cap K(H) = \{\mathbf{0}\}$. Let $\mathbf{v} = \mathbf{v}_\mathcal{M} + \mathbf{v}_\mathcal{N} \in (\mathcal{M}+\mathcal{N})\setminus\{\mathbf{0}\}$, where $\mathbf{v}_\mathcal{M} \in \mathcal{M}$ and $\mathbf{v}_\mathcal{N} \in \mathcal{N}$. We just proved that $\Phi(\mathbf{v}) \notin K(H)$ if $\mathbf{v}_\mathcal{M} = \mathbf{0}$ or $\mathbf{v}_\mathcal{N} = \mathbf{0}$. Therefore, we can assume that $\mathbf{v}_\mathcal{M} \neq \mathbf{0}$ and $\mathbf{v}_\mathcal{N} \neq \mathbf{0}$. We know that $\mathbf{v}_\mathcal{N} = (v, \ldots, v)$. Let $[v_0, v_1, \ldots, v_{s-1}]_p$ be the p-ary expansion of v. Let $v_{\mathcal{N}_1}$ and $v_{\mathcal{N}_2}$ be the elements of $\mathbb{Z}_{p^s}$ having p-ary expansion $[0, \ldots, 0, v_{s-q}, \ldots, v_{s-1}]_p$ and $[v_0, \ldots, v_{s-q-1}, 0, \ldots, 0]_p$, respectively. Then, $\mathbf{v}_\mathcal{N} = \mathbf{v}_{\mathcal{N}_1} + \mathbf{v}_{\mathcal{N}_2}$, where $\mathbf{v}_{\mathcal{N}_i} = (v_{\mathcal{N}_i}, \ldots, v_{\mathcal{N}_i})$ for $i \in \{1, 2\}$. Since $o(\mathbf{v}_\mathcal{M}) = p^q$ with $2 \leq q \leq s+1-\sigma$, the p-ary expansion of each one of its coordinates is of the form $[0, \ldots, 0, (v_\mathcal{M})_{s-q}, \ldots, (v_\mathcal{M})_{s-1}]_p$. Note that we also have that $o(\mathbf{v}_{\mathcal{N}_1}) \leq o(\mathbf{v}_\mathcal{M})$ by construction.

It is easy to see that $p(\mathbf{v}_{\mathcal{N}_2} \odot_p \mathbf{p^{s-q}}) = \mathbf{0}$. Therefore, $\mathrm{wt}_H(\Phi(p(\mathbf{v} \odot_p \mathbf{p^{s-q}}))) = \mathrm{wt}_H(\Phi(p((\mathbf{v}_\mathcal{M} + \mathbf{v}_{\mathcal{N}_1}) \odot_p \mathbf{p^{s-q}})))$. Since $o(\mathbf{v}_{\mathcal{N}_1}) \leq o(\mathbf{v}_\mathcal{M})$, it is easy to see that there exists a permutation of coordinates π such that $\pi(\mathbf{v}_\mathcal{M} + \mathbf{v}_{\mathcal{N}_1}) = \mathbf{v}_\mathcal{M}$. Thus, $\mathrm{wt}_H(\Phi(p((\mathbf{v}_\mathcal{M} + \mathbf{v}_{\mathcal{N}_1}) \odot_p \mathbf{p^{s-q}}))) = \mathrm{wt}_H(\Phi(p(\mathbf{v}_\mathcal{M} \odot_p \mathbf{p^{s-q}})))$, and since $o(\mathbf{v}_\mathcal{M}) = p^q$ with $2 \leq q \leq s+1-\sigma$, we get a contradiction as above. Therefore, $\Phi(\mathbf{v}) \notin K(H)$ and $\Phi(\mathcal{M}+\mathcal{N}) \cap K(H) = \{\mathbf{0}\}$. □

Theorem 4 *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1, \ldots, t_s)$ with $p \geq 3$ prime. Let $\mathcal{H}_p$ be the subcode of $\mathcal{H}$ which contains all the codewords of order p. Let $M = \{\mathbf{p^m}\}_{m=0}^{\sigma-2}$ if $\sigma \geq 2$, and $M = \emptyset$ if $\sigma = 1$. Then,*

$$\langle \Phi(\mathcal{H}_p), \Phi(M) \rangle = K(\Phi(\mathcal{H}))$$

and $ker(\Phi(\mathcal{H})) = (\sum_{i=1}^{s} t_i) + \sigma - 1$.

Proof The result follows by Proposition 5 and Lemma 4. □

Corollary 6 *Let $\mathcal{H} = \mathcal{H}^{t_1,\ldots,t_s}$ be the $\mathbb{Z}_{p^s}$-additive GH code of type $(n; t_1, \ldots, t_s)$ with $p \geq 3$ prime. Let $\mathbf{w}_k$ be the k-th row of $A^{t_1,\ldots,t_s}$ and $\tau = \sum_{i=1}^{s} t_i$. Let $Q = \{(o(\mathbf{w}_k)/p)\mathbf{w}_k\}_{k=1}^{\tau}$ 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 $K(\Phi(\mathcal{H}))$.*

Example 10 Let $H_3^{1,1,0}$ be the $\mathbb{Z}_{27}$-linear GH code. By Theorem 4, we have that $\ker(H_3^{1,1,0}) = 3$ since $\sigma = 2$. Moreover, we can construct $K(H_3^{1,1,0})$ from a basis by Corollary 6. We have that $Q = \{\mathbf{9}, (0, 9, 18, 0, 9, 18, 0, 9, 18)\}$ and $M = \{\mathbf{1}\}$. Thus,

$$K(H_3^{1,1,0}) = \langle \Phi(\mathbf{9}), \Phi((0, 9, 18, 0, 9, 18, 0, 9, 18)), \Phi(\mathbf{1})\rangle.$$

More generally, if $H_p^{1,1,0}$ is a $\mathbb{Z}_{p^3}$-linear GH code with p an odd prime, then we have that

$$K(H_p^{1,1,0}) = \langle \Phi(\mathbf{p^2}), \Phi(\mathbf{u}), \Phi(\mathbf{1})\rangle,$$

where $\mathbf{u}$ is the p-fold replication of $(0, p^2, 2p^2, \ldots, (p-1)p^2)$, so $\ker(H_p^{1,1,0}) = 3$. Note that $\ker(H_2^{1,1,0}) = 5$ since $H_2^{1,1,0}$ is linear [11].

Example 11 Let $H_3^{2,0,0}$ be the $\mathbb{Z}_{27}$-linear GH code considered in Example 7. By Theorem 4, we have that $\ker(H_3^{2,0,0}) = 2$ since $\sigma = 1$. Moreover, we can construct $K(H_3^{2,0,0})$ from a basis by Corollary 6. We have that $Q = \{\mathbf{9}, \mathbf{u} = (0, 9, 18, 0, 9, 18, 0, 9, 18, 0, 9, 18, 0, 9, 18, 0, 9, 18, 0, 9, 18, 0, 9, 18, 0, 9, 18)\}$ and $M = \emptyset$. Thus,

$$K(H_3^{2,0,0}) = \langle \Phi(\mathbf{9}), \Phi(\mathbf{u})\rangle.$$

In the general case of the $\mathbb{Z}_{p^3}$-linear GH codes $H_p^{2,0,0}$ with p an odd prime, we have that

$$K(H_p^{2,0,0}) = \langle \Phi(\mathbf{p^2}), \Phi(\mathbf{u})\rangle,$$

where $\mathbf{u}$ is the p^2-fold replication of $(0, p^2, 2p^2, \ldots, (p-1)p^2)$, so $\ker(H_p^{2,0,0}) = 2$. Note that $\ker(H_2^{2,0,0}) = 3$ [11].

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

The classification of the $\mathbb{Z}_4$-linear Hadamard codes of length 2^t, for any $t \geq 3$, using the rank or the dimension of the kernel is shown in [18, 21]. In [11], it is shown that the dimension of the kernel can not be used to establish a complete classification of the $\mathbb{Z}_{2^s}$-linear Hadamard codes of length 2^t, in general, for any $t \geq 3$ and $s > 2$. However, it is also shown that this invariant allows us to obtain some partial results on the classification of these codes, through some examples. In this section, we obtain these results for $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, with $t \geq 1$, $s \geq 2$ and p an odd prime, which do not coincide exactly with the case $p = 2$. Moreover, we also establish for which parameters t and s the dimension of the kernel gives a full classification, and give the exact number of non-equivalent codes in these cases.

By Theorem 3, for any $t \geq 1$, $s \geq 2$, and $p \geq 3$ prime, there is exactly one $\mathbb{Z}_{p^s}$-linear GH code of length p^t, $H^{1,0,\ldots,0,t_s}$, that is linear. Moreover, the following result implies that we can focus on $t \geq 5$ and $2 \leq s \leq t-2$ to classify the nonlinear ones.

Theorem 5 *Let $\mathcal{A}_{t,s,p}$ be the number of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, and $p \geq 3$ prime. Then,*

$$\mathcal{A}_{t,s,p} = \begin{cases} 0 \text{ if } t \geq 3 \text{ and } s \geq t+2, \\ 1 \text{ if } t \geq 3 \text{ and } s \in \{t, t+1\}, \\ 2 \text{ if } t \geq 3 \text{ and } s = t-1, \\ 2 \text{ if } t = 4 \text{ and } s = 2, \end{cases}$$

and the $\mathbb{Z}_{p^s}$-linear GH code is linear when $\mathcal{A}_{t,s,p} = 1$. Moreover, if $t \geq 5$ and $2 \leq s \leq t-2$, then $\mathcal{A}_{t,s,p} \geq 2$, and there is one which is linear and at least one which is nonlinear.

Proof First, if $t \geq 3$ and $s \geq t+2$, then the equation

$$t = \Big(\sum_{i=1}^{s}(s-i+1)\cdot t_i\Big) - 1, \tag{7}$$

with $t_1 \geq 1$, does not have any non-negative integer solution, so $\mathcal{A}_{t,s,p} = 0$. If $t \geq 3$ and $s = t+1$, then (7) has only one solution $(t_1, \ldots, t_s) = (1, 0, \ldots, 0)$. If $t \geq 3$ and $s = t$, (7) has only the solution $(1, 0, \ldots, 0, 1)$. By Theorem 3, for all the above solutions, we obtain exactly one linear code $H^{t_1,\ldots,t_s}$. Note that, when $t = 3$ and $s = 2$, the solutions are $(1, 2)$ and $(2, 0)$; when $t \geq 4$ and $s = t-1$, the only two solutions are $(1, 0, \ldots, 0, 2)$ and $(1,0,\ldots,0,1,0)$; and when $t = 4$ and $s = 2$, the solutions are $(1, 3)$ and $(2, 1)$. By Theorem 3, for these cases, we obtain exactly one linear code and one nonlinear code, so $\mathcal{A}_{t,s,p} = 2$.

Finally, when $t \geq 5$ and $s = 2$, (7) always has at least the solutions $(t_1, t_2) = (1, t+1-2)$ and $(2, t+1-4)$; and when $t \geq 5$ and $2 < s \leq t-2$, at least the solutions $(1, 0, \ldots, 0, t-s+1)$ and $(1, 0, \ldots, 0, 1, t-s-1)$. By Theorem 3, there is exactly one linear code and at least one nonlinear code, so $\mathcal{A}_{t,s,p} \geq 2$. □

The following example shows that the dimension of the kernel can not be used, in general, to classify completely all nonlinear $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, once $t \geq 5$ and $2 \leq s \leq t-2$ are fixed.

Example 12 The $\mathbb{Z}_{p^3}$-linear GH codes of length p^8 ($t = 8$ and $s = 3$) are the following: $H_p^{1,0,6}$, $H_p^{1,1,4}$, $H_p^{1,2,2}$, $H_p^{1,3,0}$, $H_p^{2,0,3}$, $H_p^{2,1,1}$ and $H_p^{3,0,0}$. When p is an odd prime, their kernels are of dimension 9, 7, 6, 5, 5, 4 and 3, respectively, by Theorem 4. Therefore, by using this invariant, we can say that all of them are non-equivalent except $H_p^{1,3,0}$ and $H_p^{2,0,3}$, which have the same dimension of the kernel. Note that, as shown in [11], for $p = 2$, the codes $H_2^{1,1,4}$ and $H_2^{1,0,6}$ are linear, and hence equivalent, whereas $H_p^{1,1,4}$ is nonlinear when $p \geq 3$.

By using the computer algebra system Magma [6], when $p = 3$, we have that $\operatorname{rank}(H_3^{1,3,0}) = 22$ and $\operatorname{rank}(H_3^{2,0,3}) = 16$, so they are non-equivalent. Actually, all these $\mathbb{Z}_{3^3}$-linear GH codes have ranks 9, 14, 22, 16, 26, 48 and 10, respectively, so we can use the rank instead of the dimension of the kernel to classify completely the $\mathbb{Z}_{3^3}$-linear GH codes of length $3^8 = 6561$.

As shown in the next example, for some values of $t \geq 5$ and $2 \leq s \leq t-2$, it is indeed possible to establish a complete classification by using just the dimension of the kernel. Actually, in Theorem 6, we show some infinite families of parameters for which this is also true.

Example 13 By Theorem 4, it is possible to check that, for any $5 \leq t \leq 7$, $2 \leq s \leq t-2$ and p an odd prime, all nonlinear $\mathbb{Z}_{p^s}$-linear GH codes of length p^t have a different dimension of the kernel, so this invariant allows us to classify them. For $t = 8$, $t = 9$ and $t = 10$, it also works, except when $s \in \{3\}$, $s \in \{3, 4\}$ and $s \in \{3, 4, 5\}$, respectively. For these given values of t and s, we can just obtain a partial classification by using the kernel.

By using Magma, we have also computed the rank of the nonlinear $\mathbb{Z}_{3^s}$-linear GH codes of length 3^t, for any $4 \leq t \leq 10$ and $2 \leq s \leq t-1$. Indeed, Tables 4 and 5 show the values of $(t_1, \ldots, t_s)$ and the pair (r, k), where r is the rank and k the dimension of the kernel, for all these codes. Note that the values of $(t_1, \ldots, t_s)$ and k do not depend on p, so they are the same for any $p \geq 3$ prime. Therefore, the results given in Examples 12 and 13 can also be checked

Table 2 Number $\mathcal{A}_{t,s,3}$ of non-equivalent $\mathbb{Z}_{3^s}$-linear GH codes of length 3^t

t	3	4	5	6	7	8	9	10
$\mathbb{Z}_{3^2}$	2	2	3	3	4	4	5	5
$\mathbb{Z}_{3^3}$	1	2	3	4	5	**7**	**8**	**10**
$\mathbb{Z}_{3^4}$	1	1	2	3	5	6	**9**	**11**
$\mathbb{Z}_{3^5}$	0	1	1	2	3	5	7	**10**
$\mathbb{Z}_{3^6}$	0	0	1	1	2	3	5	7
$\mathbb{Z}_{3^7}$	0	0	0	1	1	2	3	5
$\mathbb{Z}_{3^8}$	0	0	0	0	1	1	2	3
$\mathbb{Z}_{3^9}$	0	0	0	0	0	1	1	2

by looking at these tables. They also show that all nonlinear $\mathbb{Z}_{3^s}$-linear GH codes of length 3^t have different values of the rank, once $5 \le t \le 10$ and $2 \le s \le t-2$ are fixed. Therefore, for these cases, as in Example 12, we have that the codes are pairwise non-equivalent. This gives us a complete classification, by using the rank, and the number $\mathcal{A}_{s,t,3}$ of non-equivalent $\mathbb{Z}_{3^s}$-linear GH codes of length 3^t, as shown in Table 2 for any $3 \le t \le 10$ and $2 \le s \le t+1$. The cases where the dimension of the kernel is not enough to classify them are shown in bold type.

Theorem 6 *Let $\mathcal{A}_{t,s,p}$ be the number of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t. Then, for any $t \ge 3$, $2 \le s \le t-1$ and $p \ge 3$ prime,*

$$\mathcal{A}_{t,s,p} \le |\{(t_1, \ldots, t_s) \in \mathbb{N}^s : t = \Big(\sum_{i=1}^{s}(s-i+1)\cdot t_i\Big) - 1,\ t_1 \ge 1\}|.$$

Moreover, this bound is tight in the following cases:

1. *for any $t \ge 3$ and $s = 2$,*
2. *for any $3 \le t \le 7$ and $2 \le s \le t+1$,*
3. *for any $t \ge 7$ and $s = t-2$,*
4. *for any $t \ge 7$ and $s = t-3$,*
5. *for any $t \ge 9$ and $s = t-4$,*
6. *for $t = 8$ and $s = 4$,*
7. *for $p = 3$, any $3 \le t \le 10$ and $2 \le s \le t+1$.*

Proof Item 2 is given by Example 13. Item 7 is true by Tables 4 and 5, since given any possible t and s, all the codes have a different value of the rank.

For Item 1, since $t \ge 3$ and $s = 2$, the solutions of (7) are $(t_1, t-2t_1+1)$, where $t_1 \ge 1$ and $t+1 \ge 2t_1$. If $t_1 = 1$, the solution is $(1, t-1)$, and then the dimension of the kernel of the corresponding code is $1+t-1+2-1 = t+1$. If $t_1 \ge 2$, then the dimension of the kernel is $t-t_1+1+1-1 = t+1-t_1$ by Theorem 4, which gives different values for distinct values of t_1. Therefore, in this case, we see that there are exactly $\lfloor \frac{t+1}{2} \rfloor$ non-equivalent codes.

For Item 3, since $t \ge 7$ and $s = t-2$, then $s \ge 5$. Therefore, we have at least five terms in the addition part of equation $t+1 = (t-2)t_1 + (t-3)t_2 + \cdots + 2t_{t-3} + t_{t-2}$, with $t_1 \ge 1$, and hence we have exactly three solutions, which are $(1, 0, \ldots, 0, 3)$, $(1, 0, \ldots, 0, 1, 1)$, and $(1, 0, \ldots, 0, 1, 0, 0)$. The dimensions of the kernel for the corresponding codes are $4+t-2-1 = t+1$, $3+t-3-1 = t-1$ and $2+t-4-1 = t-3$, respectively. Since all these values are different, in this case, we have exactly three non-equivalent codes.

For Item 4, if $t = 7$ and $s = 4$, then we already know that there are exactly five non-equivalent codes by Item 2. If $t \geq 8$ and $s = t - 3$, then by applying the same argument as in Item 3, we have exactly five solutions: $(1, 0, \ldots, 0, 1, 0, 0, 0)$, $(1, 0, \ldots, 0, 1, 0, 1)$, $(1, 0, \ldots, 0, 2, 0)$, $(1, 0, \ldots, 0, 4)$ and $(1, 0, \ldots, 0, 1, 2)$. The dimensions of the kernel for the corresponding codes are $t-5$, $t-3$, $t-2$, $t+1$ and $t-1$, respectively. Again, since these values are different for a given t, in this case, we have exactly five non-equivalent codes.

For Item 5, if $t = 9$ and $s = 5$, we have exactly seven solutions: $(1, 0, 0, 0, 5)$, $(1, 0, 0, 2, 1)$, $(1, 0, 1, 0, 2)$, $(1, 0, 1, 1, 0)$, $(1, 1, 0, 0, 1)$, $(2, 0, 0, 0, 0)$ and $(1, 0, 0, 1, 3)$, and the dimensions of the kernel for the corresponding codes are 10, 7, 6, 5, 4, 2 and 8, respectively. If $t \geq 9$ and $s = t - 4$, then by applying the same argument as in Item 3, we have exactly seven solutions: $(1, 0, \ldots, 0, 5)$, $(1, 0, \ldots, 0, 2, 1)$, $(1, 0, \ldots, 0, 1, 0, 2)$, $(1, 0, \ldots, 0, 1, 1, 0)$, $(1, 0, \ldots, 0, 1, 0, 0, 1)$, $(1, 0, \ldots, 0, 1, 0, 0, 0, 0)$ and $(1, 0, \ldots, 0, 0, 1, 3)$, and the dimensions of the kernel for the corresponding codes are $t+1$, $t-2$, $t-3$, $t-4$, $t-5$, $t-7$ and $t-1$, respectively. Finally, since these values are different, we have exactly seven non-equivalent codes.

For Item 6, since $t = 8$ and $s = 4$, we have exactly six solutions: $(1, 0, 0, 5)$, $(1, 0, 2, 1)$, $(1, 1, 0, 2)$, $(1, 1, 1, 0)$, $(2, 0, 0, 1)$ and $(1, 0, 1, 3)$ and the dimensions of the kernel for the corresponding codes are 9, 6, 5, 4, 3 and 7, respectively. Again, since these values are different, we have exactly six non-equivalent codes. □

Corollary 7 *Let $\mathcal{A}_{t,s,p}$ be the number of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, and $p \geq 3$ prime. Then,*

1. $\mathcal{A}_{t,s,p} = \lfloor \frac{t+1}{2} \rfloor$ *if* $t \geq 3$ *and* $s = 2$,
2. $\mathcal{A}_{t,s,p}$ *as in Table 2 if* $3 \leq t \leq 7$ *and* $2 \leq s \leq t+1$,
3. $\mathcal{A}_{t,s,p} = 3$ *if* $t \geq 7$ *and* $s = t-2$,
4. $\mathcal{A}_{t,s,p} = 5$ *if* $t \geq 7$ *and* $s = t-3$,
5. $\mathcal{A}_{t,s,p} = 7$ *if* $t \geq 9$ *and* $s = t-4$,
6. $\mathcal{A}_{t,s,p} = 6$ *if* $t = 8$ *and* $s = 4$,
7. $\mathcal{A}_{t,s,p}$ *as in Table 2 if* $p = 3$, $3 \leq t \leq 10$ *and* $2 \leq s \leq t+1$.

Proof It follows by the proof of Theorem 6. □

Corollary 8 *Let $\mathcal{A}_{t,s,2}$ be the number of non-equivalent $\mathbb{Z}_{2^s}$-linear GH codes of length 2^t. Then,*

1. $\mathcal{A}_{t,s,2} = \lfloor \frac{t+1}{2} \rfloor - 1$ *if* $t \geq 3$ *and* $s = 2$,
2. $\mathcal{A}_{t,s,2}$ *as in Table 2 given in [11] if* $3 \leq t \leq 11$ *and* $2 \leq s \leq t+1$,
3. $\mathcal{A}_{t,s,2} = 2$ *if* $t \geq 7$ *and* $s = t-2$,
4. $\mathcal{A}_{t,s,2} = 4$ *if* $t \geq 7$ *and* $s = t-3$,
5. $\mathcal{A}_{t,s,2} = 6$ *if* $t \geq 9$ *and* $s = t-4$,
6. $\mathcal{A}_{t,s,2} = 5$ *if* $t = 8$ *and* $s = 4$.

Proof Recall that Item 1 is proved in [18, 21]. The proof of the other items follows by the same arguments as in the proof of Theorem 6, but using previous results given in Theorems 2, 3, 4 and 5, and Table 2 from [11]. □

Note that Theorem 5 gives $\mathcal{A}_{s,t,p}$ for the extreme cases when there are only one or two non-equivalent codes, and together with the results given by Corollary 7, we conjecture that they cover all cases when the kernel allows us to classify $\mathbb{Z}_{p^s}$-linear GH codes of length p^t with $p \geq 3$ prime. Indeed, they do cover all cases that are not in bold type in Table 2. We

Table 3 Bounds for the number $\mathcal{A}_{t,p}$ of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t

t	3	4	5	6	7	8	9	10
lower bound K	2	2	4	4	6	6	8	8
lower bound RK ($p = 3$)	2	2	4	4	7	8	12	14
upper bound	2	3	6	9	15	22	33	46

also give $\mathcal{A}_{s,t,2}$ for the same cases in Corollary 8, since they were not included in [11]. Note that the values of $\mathcal{A}_{s,t,2}$ are different from $\mathcal{A}_{s,t,p}$ with $p \geq 3$ prime, but they just differ by one unit, because two of the codes are linear, instead of just one.

Next, we focus on $\mathbb{Z}_{p^s}$-linear GH codes, once only the length p^t is fixed. First, Example 14 shows that there are $\mathbb{Z}_{p^s}$-linear GH codes with $s > 2$, which are not equivalent to any $\mathbb{Z}_{p^2}$-linear GH code of the same length p^t. Then, Example 15 also shows that there are $\mathbb{Z}_{p^2}$-linear GH codes which are not equivalent to any $\mathbb{Z}_{p^s}$-linear GH codes with $s > 2$.

Example 14 Let $H_p^{2,0,0}$ be the $\mathbb{Z}_{p^3}$-linear GH code of length p^5 with p an odd prime. Recall that $\ker(H_p^{2,0,0}) = 2$ by Theorem 4, and hence $H_p^{2,0,0}$ is nonlinear. By Corollary 7, there are three $\mathbb{Z}_{p^2}$-linear GH codes of length p^5, $H_p^{1,4}$, $H_p^{2,2}$ and $H_p^{3,0}$. The first one is linear, and the last two have $\ker(H_p^{2,2}) = 4$ and $\ker(H_p^{3,0}) = 3$ by Theorem 4. Hence, there is no $\mathbb{Z}_{p^2}$-linear GH code equivalent to the $\mathbb{Z}_{p^3}$-linear GH code $H^{2,0,0}$ of length p^5.

Example 15 By Theorem 3 or Table 4, we have that there are five nonlinear $\mathbb{Z}_{p^s}$-linear GH codes of length p^5 ($t = 5$): $H_p^{2,2}$, $H_p^{3,0}$, $H_p^{2,0,0}$, $H_p^{1,1,1}$ and $H_p^{1,0,1,0}$. Recall that the values of $(t_1, \ldots, t_s)$ and k do not depend on the value of p. It is easy to see that $H_p^{3,0}$ is not equivalent to any $\mathbb{Z}_{p^s}$-linear GH codes with $s > 2$, by considering just the dimension of the kernel. Other examples like this one can be found when t is odd, and at least for $p = 3$. For example, by Tables 4 and 5, for $t = 7$ and $t = 9$ there are $\mathbb{Z}_{3^2}$-linear GH codes, $H_3^{4,0}$ and $H_3^{5,0}$, respectively, which are not equivalent to any $\mathbb{Z}_{3^s}$-linear GH codes with $s > 2$ of the same length, by using both invariants: the rank and dimension of the kernel.

Finally, we establish some lower and upper bounds on the number of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, when only the length p^t is fixed, for some values of t. By Theorem 4, we can determine a lower bound (K) taking into account just the dimension of the kernel. This lower bound can be improved (RK) if we consider both invariants, the rank and the dimension of the kernel, at least for $p = 3$ and $t \leq 10$. Note that there are codes having the same dimension of the kernel with different ranks (for $p = 3$ and $t = 7, 8, 9, 10$), and codes having the same rank with different dimensions of the kernel (for $p = 3$ and $t = 9, 10$). An upper bound can be given easily by considering all non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, once t and s are fixed, as it is shown in the next theorem.

Theorem 7 *Let $\mathcal{A}_{t,s,p}$ be the number of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, and $p \geq 3$ prime. Let $\mathcal{A}_{t,p}$ be the number of non-equivalent $\mathbb{Z}_{p^s}$-linear GH codes of length p^t, for any $s \geq 2$. Then, $\mathcal{A}_{t,p} \leq \sum_{s=2}^{t-1}(\mathcal{A}_{t,s,p} - 1) + 1$.*

The results related to the upper and lower bound of the value $\mathcal{A}_{t,p}$ are summarized in Table 3, where we give these bounds for all $3 \leq t \leq 10$.

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

	$t=4$		$t=5$		$t=6$		$t=7$	
	$(t_1,\ldots,t_s)$	(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)

7 Conclusions and further research

In this paper, we establish the classification of the $\mathbb{Z}_{p^s}$-linear GH codes of length p^t once t, s, and p are fixed, giving the exact number $\mathcal{A}_{t,s,p}$ of non-equivalent such codes for all possible parameters, except for $t \geq 8$ and $3 \leq s \leq t-5$. For these values, at least if $p = 3$ and $t = 8, 9, 10$ (and $p = 2$ and $t = 8, 9, 10, 11$ [11]), there are codes with the same dimension of the kernel, so this invariant can not be used to fully classify. However, in these cases, we have checked that the rank classifies. We conjecture that, even though there are some cases when the dimension of the kernel does not classify, the rank always does, and thus $\mathcal{A}_{t,s,p}$ coincides with the upper bound given in Theorem 6 if p is an odd prime, and the one given in [11,Theorem 5] if $p = 2$.

On the other hand, when only t and p are fixed, at least if $p = 2$ and $p = 3$, we have $\mathbb{Z}_{p^s}$-linear GH codes of length p^t (with different values of s) which have the same values for the rank and dimension of the kernel. For $p = 2$, these codes are equivalent as shown in [12]. Another further research on this topic would be to determine whether they are also equivalent for any odd prime p.

The $\mathbb{Z}_{p^s}$-linear GH codes studied in this paper are the ones obtained by using Carlet's Gray map. As mentioned in the introduction, there are other Gray maps, which could be used to generate GH codes from the $\mathbb{Z}_{p^s}$-additive codes $\mathcal{H}_p^{t_1,\ldots,t_s}$ constructed in Sect. 3 for $p > 2$ prime or in [11] for $p = 2$. However, the results about the linearity, kernel, rank, and classification would be different. For example, the $\mathbb{Z}_{16}$-linear Hadamard code $\Phi(\mathcal{H}_2^{1,1,0,0})$ has rank $r = 9$ and kernel of dimension $k = 4$ [11]. By using other Gray maps ϕ' such that $\sum \lambda_i \phi'(2^i) \neq \phi'(\sum \lambda_i 2^i)$, the parameters (r, k) become (9, 2), (11, 3), (11, 2), and (13, 2), so we could obtain new non-equivalent GH codes.

Table 5 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)
$\mathbb{Z}_{3^2}$	(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)
$\mathbb{Z}_{3^6}$	(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)
			(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)

Table 5 continued

	$t=8$		$t=9$		$t=10$	
	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)	$(t_1,\ldots,t_s)$	(r,k)
$\mathbb{Z}_{37}$	(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)

Acknowledgements The authors thank Adrián Torres for reviewing the latest version of the paper. They also 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.

References

1. Armario, J.A., Bailera, I., Egan, R.: Butson full propelinear codes. preprint arXiv:2010.06206 (2020)
2. Assmus E.F., Key J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992).
3. Bauer H., Ganter B., Hergert F.: Algebraic techniques for nonlinear codes. Combinatorica **3**(1), 21–33 (1983).
4. Blake I.F.: Codes over integer residue rings. Information and Control **29**(4), 295–300 (1975).
5. Borges J., Fernández-Córdoba C., Rifà J.: Every $\mathbb{Z}_{2^k}$-code is a binary propelinear code. Electron Notes Discret Math **10**, 100–102 (2001).
6. Bosma, W., Cannon, J.J., Fieker, C., Steel, A.: Handbook of Magma functions. Edition **2.25** (2020). http://magma.maths.usyd.edu.au/magma/
7. Carlet C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inf. Theory **44**(4), 1543–1547 (1998).
8. Constantinescu I., Heise W.: A metric for codes over residue class rings. Problemy Peredachi Informatsii **33**(3), 22–28 (1997).
9. Dougherty S.T., Fernández-Córdoba C.: Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes. Adv. Math. Commun. **5**(4), 571–588 (2011).
10. 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).
11. Fernández-Córdoba C., Vela C., Villanueva M.: On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification. Des. Codes Cryptogr. **87**(2–3), 417–435 (2019).
12. Fernández-Córdoba C., Vela C., Villanueva M.: Equivalences among $\mathbb{Z}_{2^s}$-linear Hadamard codes. Discret Math. **343**(3), 111721 (2020).
13. 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).
14. Gupta M.K., Bhandari M.C., Lal A.K.: On linear codes over $\mathbb{Z}_{2^s}$. Des. Codes Cryptogr. **36**(3), 227–244 (2005).

15. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J., Solé P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Theory **40**(2), 301–319 (1994).
16. Honold T., Nechaev A.A.: Weighted modules and representations of codes. Probl. Inf. Transm. **35**(3), 205–223 (1999).
17. Jungnickel D.: On difference matrices, resolvable transversal designs and generalized Hadamard matrices. Math. Z. **167**(1), 49–60 (1979).
18. Krotov D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. Electron. Notes Discret Math. **6**, 107–112 (2001).
19. Krotov D.S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Trans. Inf. Theory **53**(4), 1532–1537 (2007).
20. 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).
21. Phelps K.T., Rifà J., Villanueva M.: On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: Rank and kernel. IEEE Trans. Inf. Theory **52**(1), 316–319 (2006).
22. Shankar P.: On BCH codes over arbitrary integer rings. IEEE Trans. Inf. Theory **25**(4), 480–483 (1979).
23. 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).
24. Shi M., Sepasdar Z., Alahmadi A., Solé P.: On two-weight $\mathbb{Z}_{2^k}$-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. Tapia-Recillas H., Vega G.: On $\mathbb{Z}_{2^k}$-linear and quaternary codes. SIAM J. Discret Math. **17**(1), 103–113 (2003).