On $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear generalized Hadamard codes⋆

Dipak Kumar Bhunia, Cristina Fernández-Córdoba, and Mercè Villanueva

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193 Cerdanyola del Vallès, Spain
{Dipak.Bhunia,Cristina.Fernandez,Merce.Villanueva}@uab.cat

Abstract. The $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive codes are subgroups of $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2}$, and can be seen as linear codes over $\mathbb{Z}_p$ when $\alpha_2 = 0$, $\mathbb{Z}_{p^2}$-additive codes when $\alpha_1 = 0$, or $\mathbb{Z}_2\mathbb{Z}_4$-additive codes when $p = 2$. A $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear generalized Hadamard (GH) code is a GH code over $\mathbb{Z}_p$ which is the Gray map image of a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code. In this paper, we generalize some known results for $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes with $p = 2$ to any $p \geq 3$ prime when $\alpha_1 \neq 0$. First, we give a recursive construction of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes of type $(\alpha_1, \alpha_2; t_1, t_2)$ with $t_1, t_2 \geq 1$. Then, we show for which types the corresponding $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes are non-linear over $\mathbb{Z}_p$. For these codes, we compute the kernel and its dimension, which allow us to give a complete classification of these codes.

Keywords: Hadamard code · Gray map · $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear code · kernel · classification

1 Introduction

Let $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ be the ring of integers modulo p and p^2, respectively, where p is a prime. Let $\mathbb{Z}_p^n$ and $\mathbb{Z}_{p^2}^n$ denote the set of all n-tuples over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$, respectively. In this paper, the elements of $\mathbb{Z}_p^n$ and $\mathbb{Z}_{p^2}^n$ will also be called vectors of length n. The order of a vector $\mathbf{u}$ over $\mathbb{Z}_{p^2}$, 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 $\mathbb{Z}_{p^2}^n$ is a $\mathbb{Z}_{p^2}$-additive if it is a subgroup of $\mathbb{Z}_{p^2}^n$. A $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code is a subgroup of $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2}$. Note that a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code is a linear code over $\mathbb{Z}_p$ when $\alpha_2 = 0$, a $\mathbb{Z}_{p^2}$-additive code when $\alpha_1 = 0$, or a $\mathbb{Z}_2\mathbb{Z}_4$-additive code when $p = 2$.

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 $d(C) = \min\{d_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}\}$.

⋆ 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.

In [9], 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 $\mathbb{Z}_2^{2^{s-1}}$ [4,5,6,10,13]. The one given in [10] can be defined in terms of the elements of a Hadamard code [13], and Carlet's Gray map [5] is a particular case of the one given in [13] satisfying $\sum \lambda_i \phi(2^i) = \phi(\sum \lambda_i 2^i)$ [8]. 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 [17]. Specifically,

$$\phi : \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p^p \tag{1}$$

$$u \mapsto (u_0, u_1)M, \tag{2}$$

where $u \in \mathbb{Z}_{p^2}$; $[u_0, u_1]_p$ is the p-ary expansion of u, that is $u = u_0 + u_1 p$ with $u_0, u_1 \in \mathbb{Z}_p$; and M is the following matrix of size $2 \times p$:

$$\begin{pmatrix} 0 \; 1 \; 2 \cdots & p-1 \\ 1 \; 1 \; 1 \cdots & 1 \end{pmatrix}.$$

Let $\Phi : \mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2} \to \mathbb{Z}_p^n$, where $n = \alpha_1 + p\alpha_2$, be an extension of the Gray map ϕ given by

$$\Phi(\mathbf{x} \mid \mathbf{y}) = (\mathbf{x} \mid \phi(y_1), \ldots, \phi(y_{\alpha_2})),$$

for any $\mathbf{x} \in \mathbb{Z}_p^{\alpha_1}$ and $\mathbf{y} = (y_1, \ldots, y_{\alpha_2}) \in \mathbb{Z}_{p^2}^{\alpha_2}$.

Let $\mathcal{C}$ be a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code over $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2}$. We say that its Gray map image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear code of length $\alpha_1 + p\alpha_2$. Since $\mathcal{C}$ can be seen as a subgroup of $\mathbb{Z}_{p^2}^{\alpha_1+\alpha_2}$, it is isomorphic to an abelian structure $\mathbb{Z}_{p^2}^{t_1} \times \mathbb{Z}_p^{t_2}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(\alpha_1, \alpha_2; t_1, t_2)$. Note that $|\mathcal{C}| = p^{2t_1+t_2}$. 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, $t_1 + t_2$ rows.

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 $\mathrm{K}(C) = \{\mathbf{x} \in \mathbb{Z}_p^n : \mathbf{x} + C = C\}$ [2,14]. 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, $1 \le i < j \le p\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \le s \le p\lambda\}$ contains every element of $\mathbb{Z}_p$ exactly λ times [11]. An ordinary Hadamard matrix of order 4μ corresponds to 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. From a normalized GH matrix H, we denote by F_H the code consisting of the rows of H, and $C_H = \bigcup_{\alpha\in\mathbb{Z}_p}(F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$ and $\mathbf{1}$ denotes the all-one vector. The code C_H over $\mathbb{Z}_p$ is called generalized Hadamard (GH) code [7]. Note that C_H is generally a non-linear code over $\mathbb{Z}_p$. Moreover, if it is of length N, it has pN codewords and minimum distance $N(p-1)/p$.

The $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive codes such that after the Gray map Φ give GH codes are called $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes and the corresponding images are called $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes. It is known that $\mathbb{Z}_2\mathbb{Z}_4$-linear GH codes with $\alpha_1 = 0$ and $\alpha_1 \neq 0$ can be classified by using either the rank or the dimension of the kernel [12,15]. For $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes with $\alpha_1 = 0$ and $p \geq 3$ prime, it is also known that the kernel can be used to give a complete classification [3].

This paper is focused on $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes with $\alpha_1 \neq 0$ and $p \geq 3$ prime, generalizing some results given for $p = 2$ in [15,16] related to the construction, linearity, kernel and classification of such codes. This paper is organized as follows. In Section 2, we describe the construction of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes of type $(\alpha_1, \alpha_2; t_1, t_2)$ with $\alpha_1 \neq 0$. In Sections 3 and 4, we establish for which types these codes are linear, and we give the kernel and its dimension whenever they are non-linear. We also show that the dimension of the kernel is enough to classify completely the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes with $\alpha_1 \neq 0$ of a given length, providing the number of non-equivalent such codes, like it was proved for $\mathbb{Z}_2\mathbb{Z}_4$-linear GH codes in [15].

2 Construction of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes

The description of a generator matrix having minimum number of rows for $\mathbb{Z}_2\mathbb{Z}_4$-additive GH codes with $\alpha_1 \neq 0$, as long as an iterative construction of these matrices, are given in [15,16]. In this section, we generalize these results for $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes with $\alpha_1 \neq 0$ and any $p \geq 3$ prime. Specifically, we define an iterative construction for the generator matrices and establish that they generate $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes.

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

$$A_p^{1,1} = \left(\begin{array}{cccc|cccc} 1 & 1 & \cdots & 1 & p & p & \cdots & p \\ 0 & 1 & \cdots & p-1 & 1 & 2 & \cdots & p-1 \end{array}\right). \tag{3}$$

Any matrix $A_p^{t_1,t_2}$ with $t_1 \geq 1, t_2 \geq 2$ or $t_1 \geq 2, t_2 \geq 1$ can be obtained by applying the following iterative construction. First, if A is a generator matrix of a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code, that is, a subgroup of $\mathbb{Z}_p^{\alpha_1} \times \mathbb{Z}_{p^2}^{\alpha_2}$, then we denote by A_1 the submatrix of A with the first α_1 columns over $\mathbb{Z}_p$, and A_2 the submatrix with the last α_2 columns over $\mathbb{Z}_{p^2}$. We start with $A_p^{1,1}$. Then, if we have a matrix $A = A_p^{t_1,t_2}$, we may construct the matrices

$$A_p^{t_1,t_2+1} = \left(\begin{array}{cccc|cccc} A_1 & A_1 & \cdots & A_1 & A_2 & A_2 & \cdots & A_2 \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p-1} & p\cdot\mathbf{0} & p\cdot\mathbf{1} & \cdots & p\cdot(\mathbf{p-1}) \end{array}\right) \tag{4}$$

and

$$A_p^{t_1+1,t_2} = \left(\begin{array}{cccc|cccccccc} A_1 & A_1 & \cdots & A_1 & pA_1 & \cdots & pA_1 & A_2 & A_2 & \cdots & A_2 \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p-1} & \mathbf{1} & \cdots & \mathbf{p-1} & \mathbf{0} & \mathbf{1} & \cdots & \mathbf{p^2-1} \end{array}\right). \quad (5)$$

Example 1. Let

$$A_3^{1,1} = \left(\begin{array}{ccc|cc} 1 & 1 & 1 & 3 & 3 \\ 0 & 1 & 2 & 1 & 2 \end{array}\right)$$

be the matrix described in (3) for $p = 3$. By using the constructions described in (4) and (5), we obtain $A_3^{1,2}$ and $A_3^{2,1}$, respectively, as follows:

$$A_3^{1,2} = \left(\begin{array}{ccccccccc|cccccc} 1&1&1&1&1&1&1&1&1&3&3&3&3&3&3 \\ 0&1&2&0&1&2&0&1&2&1&2&1&2&1&2 \\ 0&0&0&1&1&1&2&2&2&0&0&3&3&6&6 \end{array}\right)$$

$$A_3^{2,1} = \left(\begin{array}{ccccccccc|ccccccccccccc} 1&1&1&1&1&1&1&1&1&3&3&3&3&3&3&3&3&3&3&\cdots&3&3 \\ 0&1&2&0&1&2&0&1&2&0&3&6&0&3&6&1&2&1&2&\cdots&1&2 \\ 0&0&0&1&1&1&2&2&2&1&1&1&2&2&2&0&0&1&1&\cdots&8&8 \end{array}\right).$$

Throughout this paper, we consider that the matrices $A_p^{t_1,t_2}$ are constructed recursively starting from $A_p^{1,1}$ in the following way. First, we add $t_1 - 1$ rows of order p^2, up to obtain $A_p^{t_1,1}$; and then t_2 rows of order p up to achieve $A_p^{t_1,t_2}$.

The $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code generated by $A_p^{t_1,t_2}$ is denoted by $\mathcal{H}_p^{t_1,t_2}$, and the corresponding $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear code $\Phi(\mathcal{H}_p^{t_1,t_2})$ by $H_p^{t_1,t_2}$. We also write A^{t_1,t_2}, $\mathcal{H}^{t_1,t_2}$, and H^{t_1,t_2} instead of $A_p^{t_1,t_2}$, $\mathcal{H}_p^{t_1,t_2}$, and $H_p^{t_1,t_2}$, respectively, when the value of p is clear by the context.

Theorem 1. *The $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive code $\mathcal{H}_p^{1,1}$ generated by the matrix*

$$A_p^{1,1} = \left(\begin{array}{cccc|cccc} 1 & 1 & \cdots & 1 & p & p & \cdots & p \\ 0 & 1 & \cdots & p-1 & 1 & 2 & \cdots & p-1 \end{array}\right)$$

is a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code of type $(p, p-1; 1, 1)$.

Example 2. The $\mathbb{Z}_3\mathbb{Z}_9$-additive code $\mathcal{H}_3^{1,1}$ generated by the matrix $A_3^{1,1}$, given in Example 1, is a $\mathbb{Z}_3\mathbb{Z}_9$-additive GH code of type $(3, 2; 1, 1)$. Indeed, we have that $H_3^{1,1} = \Phi(\mathcal{H}_3^{1,1}) = \bigcup_{\lambda \in \mathbb{Z}_3} (\Phi(A_0) + \lambda \mathbf{1})$, where $A_0 = \{\lambda(0, 1, 2 \mid 1, 2) : \lambda \in \mathbb{Z}_9\}$, and then $\Phi(A_0)$ consists of all the rows of the GH matrix

$$H(3,3) = \begin{pmatrix} 0&0&0&0&0&0&0&0&0 \\ 0&1&2&0&1&2&0&2&1 \\ 0&2&1&0&2&1&1&2&0 \\ 0&0&0&1&1&1&2&2&2 \\ 0&1&2&1&2&0&2&1&0 \\ 0&2&1&1&0&2&0&1&2 \\ 0&0&0&2&2&2&1&1&1 \\ 0&1&2&2&0&1&1&0&2 \\ 0&2&1&2&1&0&2&0&1 \end{pmatrix}. \quad (6)$$

The $\mathbb{Z}_3\mathbb{Z}_9$-linear code $H_3^{1,1}$ has length $N = 9$, $pN = 3 \cdot 9 = 27$ codewords and minimum distance $N(p-1)/p = 9(3-1)/3 = 6$.

Theorem 2. *Let $\mathcal{H}_p^{t_1,t_2}$ be a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code of type $(\alpha_1,\alpha_2;t_1,t_2)$ with $t_1,t_2 \geq 1$ and p prime. Then, with the above constructions, $\mathcal{H}_p^{t_1,t_2+1}$ and $\mathcal{H}_p^{t_1+1,t_2}$ are $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH codes of types $(p\alpha_1,p\alpha_2;t_1,t_2+1)$ and $(p\alpha_1,(p-1)\alpha_1+p^2\alpha_2;t_1+1,t_2)$, respectively.*

Example 3. Let $\mathcal{H}_3^{1,2}$ be the $\mathbb{Z}_3\mathbb{Z}_9$-additive code generated by the matrix $A_3^{1,2}$ given in Example 1. By Theorem 2, $H_3^{1,2} = \Phi(\mathcal{H}_3^{1,2})$ is a $\mathbb{Z}_3\mathbb{Z}_9$-linear GH code of type $(9,6;1,2)$. Actually, we can write $H_3^{1,2} = \bigcup_{\lambda\in\mathbb{Z}_3}(F_H + \lambda\mathbf{1})$, where F_H consists of all the rows of a GH matrix $H(3,9)$. Also, note that $H_3^{1,2}$ has length $N = 27$, $pN = 3\cdot 27 = 81$ codewords and minimum distance $N(p-1)/p = 27(3-1)/3 = 18$.

Remark 1. The above constructions (4) and (5) give always $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes with $\alpha_2 \neq 0$ since the starting matrix $A_p^{1,1}$ has $\alpha_2 \neq 0$. If $\alpha_2 = 0$, the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes coincide with the codes obtained from a Sylvester GH matrix, so they are always linear and of type $(p^{t_2-1},0;0,t_2)$ [7]. Therefore, we only focus on the ones with $\alpha_2 \neq 0$ to study whether they are linear or not.

Remark 2. Let $\mathcal{H} = \mathcal{H}_p^{t_1,t_2}$ be a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code of type $(\alpha_1,\alpha_2;t_1,t_2)$ with $t_1,t_2 \geq 1$ and p prime. Let $H = \Phi(\mathcal{H}_p^{t_1,t_2})$ be the corresponding $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH code of length $\alpha_1 + p\alpha_2$. Then, since H is a GH code, its minimum distance is

$$\frac{(p-1)(\alpha_1+p\alpha_2)}{p}.$$

Let $\mathcal{H}_1$ (respectively, $\mathcal{H}_2$) be the punctured code of $\mathcal{H}$ by deleting the last α_2 coordinates over $\mathbb{Z}_{p^2}$ (respectively, the first α_1 coordinates over $\mathbb{Z}_p$). Note that, by construction, $\mathcal{H}_1$ is a GH code over $\mathbb{Z}_p$ of length α_1 and minimum distance $(p-1)\alpha_1/p$. Therefore, $H_2 = \Phi(\mathcal{H}_2)$ has minimum distance $(p-1)\alpha_2$.

Remark 3. Since the length of the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH code $\Phi(\mathcal{H}_p^{1,1})$ is p^2, its minimum distance is $(p-1)p^2/p = p(p-1)$ by Remark 2.

3 Linearity of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes

In [15], it is shown that the $\mathbb{Z}_2\mathbb{Z}_4$-linear GH codes of type $(\alpha_1,\alpha_2;1,t_2)$ are the only ones which are linear, when $\alpha_1 \neq 0$ and $\alpha_2 \neq 0$. The next result shows that there are no $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes of type $(\alpha_1,\alpha_2;t_1,t_2)$, with $\alpha_1 \neq 0$, $t_1,t_2 \geq 1$ and $p \geq 3$ prime, which are linear. Note that this result for $p \geq 3$ does not coincide with the known result for $p = 2$ if $t_1 = 1$.

Theorem 3. *Let $\mathcal{H}_p^{t_1,t_2}$ be the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code of type $(\alpha_1,\alpha_2;t_1,t_2)$ with $\alpha_1 \neq 0$, $t_1,t_2 \geq 1$ and $p \geq 3$ prime. Then, $H_p^{t_1,t_2} = \Phi(\mathcal{H}_p^{t_1,t_2})$ is non-linear.*

Proof. First, we prove that $H_p^{1,1}$ is non-linear. Since $\mathbf{u} = (0,1,\dots,p-1 \mid 1,2,\dots,p-1) \in \mathcal{H}_p^{1,1}$, then $(p-1)\mathbf{u} = (0,(p-1)\cdot 1,\dots,(p-1)\cdot(p-1) \mid (p-1)\cdot 1,(p-1)\cdot 2,\dots,(p-1)\cdot(p-1)) \in \mathcal{H}_p^{1,1}$. Since $\phi(1)+\phi(p-1) = 0$, then the first $2p$ coordinates of the vector $\Phi(\mathbf{u})+\Phi((p-1)\mathbf{u})$ of length p^2 are zero. Therefore, $\mathrm{wt}_H(\Phi(\mathbf{u})+\Phi((p-1)\mathbf{u})) \leq p^2-2p = p(p-2) < p(p-1)$, and hence, $\Phi(\mathbf{u})+\Phi((p-1)\mathbf{u}) \notin H_p^{1,1}$, since the minimum distance of $H_p^{1,1}$ is $p(p-1)$ by Remark 3. Therefore, $H_p^{1,1}$ is non-linear.

Second, we prove that if $H_p^{t_1-1,t_2}$ is non-linear, then $H_p^{t_1,t_2}$ is also non-linear. Assume that $H_p^{t_1,t_2}$ is linear. Then, by the iterative construction defined in (5), for any $\mathbf{u}=(u \mid u')$, $\mathbf{v}=(v \mid v') \in \mathcal{H}_p^{t_1-1,t_2}$, we have that $\bar{\mathbf{u}}, \bar{\mathbf{v}} \in \mathcal{H}_p^{t_1,t_2}$, where

$$\bar{\mathbf{u}} = (u, \overset{p}{\ldots}, u \mid pu, \overset{p-1}{\ldots}, pu, u', \overset{p^2}{\ldots}, u')$$
$$\bar{\mathbf{v}} = (v, \overset{p}{\ldots}, v \mid pv, \overset{p-1}{\ldots}, pv, v', \overset{p^2}{\ldots}, v').$$

Moreover, since $H_p^{t_1,t_2}$ is linear, $\Phi(\bar{\mathbf{u}})+\Phi(\bar{\mathbf{v}}) = \Phi((a, \overset{p}{\ldots}, a \mid pa, \overset{p-1}{\ldots}, pa, a', \overset{p^2}{\ldots}, a') + \lambda(\mathbf{0},\mathbf{1},\ldots,\mathbf{p-1} \mid \mathbf{1},\mathbf{2},\ldots,\mathbf{p-1},\mathbf{0},\mathbf{1},\ldots,\mathbf{p^2-1})) \in H_p^{t_1,t_2}$, for some $\mathbf{a}=(a \mid a') \in \mathcal{H}_p^{t_1-1,t_2}$ and $\lambda \in \mathbb{Z}_{p^2}$. Considering the coordinates in positions 1 and $2p$ of $\bar{\mathbf{u}}$ and $\bar{\mathbf{v}}$, we have that $\Phi(\mathbf{u})+\Phi(\mathbf{v})=\Phi(\mathbf{a}) \in H_p^{t_1-1,t_2}$, and then $H_p^{t_1-1,t_2}$ is linear, which is a contradiction.

Finally, if $H_p^{t_1,t_2-1}$ is non-linear, then as above we can show that $H_p^{t_1,t_2}$ is also non-linear, and hence the result follows.

Example 4. Let $\mathcal{H}_3^{1,1}$ be the $\mathbb{Z}_3\mathbb{Z}_9$-additive GH code of type $(3,2;1,1)$ considered in Example 2. Note that $(0,1,2,0,1,2,0,2,1)+(0,2,1,0,2,1,1,2,0) = (0,0,0,0,0,0,1,1,1) \notin \Phi(\mathcal{H}_3^{1,1})$, so $H_3^{1,1}=\Phi(\mathcal{H}_3^{1,1})$ is a non-linear code.

4 Kernel and classification of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes

The kernel of $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes with $\alpha_1 \neq 0$ and its dimension are given in [15]. In this section, we generalize these results for $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes with $\alpha_1 \neq 0$ and $p \geq 3$ prime. First, we found the kernel for these codes, and then we establish a basis of the kernel, which give us its dimension. Specifically, the dimension of the kernel of a $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH code of type $(\alpha_1,\alpha_2;t_1,t_2)$, with $\alpha_1 \neq 0$, $t_1,t_2 \geq 1$ and $p \geq 3$ prime, is t_1+t_2. Again, note that this result for $p \geq 3$ does not coincide with the known result for $p=2$ if $t_1=1$.

Theorem 4. *Let $\mathcal{H}=\mathcal{H}_p^{t_1,t_2}$ be the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code of type $(\alpha_1,\alpha_2;t_1,t_2)$ with $\alpha_1 \neq 0$, $t_1,t_2 \geq 1$ and $p \geq 3$ prime. Let $\mathcal{H}_p$ be the subcode of $\mathcal{H}$ which contains all the codewords of order p. Then, $K(\Phi(\mathcal{H}))=\Phi(\mathcal{H}_p)$.*

Corollary 1. *Let $\mathcal{H}=\mathcal{H}_p^{t_1,t_2}$ be the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code of type $(\alpha_1,\alpha_2;t_1,t_2)$ with $\alpha_1 \neq 0$, $t_1,t_2 \geq 1$ and $p \geq 3$ prime. Let $\mathbf{w}_k$ be the kth row of A^{t_1,t_2} and $Q=\{(o(\mathbf{w}_k)/p)\mathbf{w}_k\}_{k=1}^{t_1+t_2}$. Then, $\Phi(Q)$ is a basis of $K(\Phi(\mathcal{H}))$ and $ker(\Phi(\mathcal{H}))=t_1+t_2$.*

Example 5. Let $\mathcal{H}_3^{1,2}$ be the $\mathbb{Z}_3\mathbb{Z}_9$-additive GH code generated by $A_3^{1,2}$ given in Example 1. By Corollary 1, we have that $\ker(H_3^{1,2})=1+2=3$. Also by Corollary 1, we can construct $K(H_3^{1,2})$ from a basis. We have that $Q=\{(\mathbf{1} \mid \mathbf{3}),(\mathbf{0} \mid 3,6,3,6,3,6),(\mathbf{0} \mid 0,0,3,3,6,6)\}$. Thus,

$$K(H_3^{1,2}) = \langle \Phi(\mathbf{1} \mid \mathbf{3}), \Phi(\mathbf{0} \mid 3,6,3,6,3,6), \Phi(\mathbf{0} \mid 0,0,3,3,6,6) \rangle.$$

More generally, if $\mathcal{H}_p^{1,2}$ is the $\mathbb{Z}_p\mathbb{Z}_{p^2}$-additive GH code generated by $A_p^{1,2}$ with $p \geq 3$ prime, then we have that

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

where $\mathbf{u}$ is the p-fold replication of $(p, 2p, \ldots, (p-1)p)$ and $\mathbf{v} = (\mathbf{0}, p \cdot \mathbf{1}, \ldots, p \cdot (\mathbf{p}-\mathbf{1}))$ with $\mathbf{i} = (i, \overset{p-1}{\ldots}, i), i \in \{0, 1, \ldots, p-1)\}$. Therefore, $\ker(H_p^{1,2}) = 3$. Note that $\ker(H_2^{1,2}) = 4$, since $H_2^{1,2}$ is linear [15].

Corollary 2. *For any $t \geq 2$ and $p \geq 3$ prime, there are at least $\lfloor t/2 \rfloor + 1$ non-equivalent $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes of length p^t.*

Proof. Considering all the non-negative integer solutions (t_1, t_2) with $t_1, t_2 \geq 1$ of the equation $t + 1 = 2t_1 + t_2$, we have that all the non-linear $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes of length p^t are $H_p^{t_1, t-2t_1+1}$, where $1 \leq t_1 \leq \lfloor t/2 \rfloor$, by Theorem 3. Then, by Corollary 1, the dimensions of the kernels of the these codes are $t - t_1 + 1$, which gives different values for distinct values of t_1. Therefore, they are all non-equivalent codes. We have at least one $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH code of type $(p^t, 0; 0, t+1)$, which is linear. Therefore, there are at least $\lfloor t/2 \rfloor + 1$ non-equivalent $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear GH codes of length p^t.

References

1. Assmus, E.F., Key, J.D.: Designs and Their Codes. Cambridge University Press (1994)
2. Bauer, H., Ganter, B., Hergert, F.: Algebraic techniques for nonlinear codes. Combinatorica **3**(1), 21–33 (1983)
3. Bhunia, D.K., Fernández-Córdoba, C., Villanueva, M.: On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes. submitted to Designs, Codes and Cryptography (2021)
4. Borges, J., Fernández-Córdoba, C., Rifà, J.: Every $\mathbb{Z}_{2^k}$-code is a binary propelinear code. Electronic Notes in Discrete Mathematics **10**, 100–102 (2001)
5. Carlet, C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Transactions on Information Theory **44**(4), 1543–1547 (1998)
6. Dougherty, S.T., Fernández-Córdoba, C.: Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes. Advances in Mathematics of Communications **5**(4), 571–588 (2011)
7. Dougherty, S.T., Rifà, J., Villanueva, M.: Ranks and kernels of codes from generalized Hadamard matrices. IEEE Transactions on Information Theory **62**(2), 687–694 (2016)
8. Fernández-Córdoba, C., Vela, C., Villanueva, M.: On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification. Designs, Codes and Cryptography **87**(2-3), 417–435 (2019)
9. 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 Transactions on Information Theory **40**(2), 301–319 (1994)
10. Honold, T., Nechaev, A.A.: Weighted modules and representations of codes. Probl. Inf. Transm. **35**(3), 205–223 (1999)
11. Jungnickel, D.: On difference matrices, resolvable transversal designs and generalized Hadamard matrices. Mathematische Zeitschrift **167**(1), 49–60 (1979)

12. Krotov, D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. Electronic Notes in Discrete Mathematics **6**, 107–112 (2001)
13. Krotov, D.S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Transactions on Information Theory **53**(4), 1532–1537 (2007)
14. Phelps, K.T., Rifà, J., Villanueva, M.: Kernels and p-kernels of p^r-ary 1-perfect codes. Designs, Codes and Cryptography **37**(2), 243–261 (2005)
15. 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 transactions on information theory **52**(1), 316–319 (2006)
16. Rifà, J., Solov'eva, F.I., Villanueva, M.: On the intersection of $\mathbb{Z}_2\mathbb{Z}_4$-additive perfect codes. IEEE transactions on information theory **54**(3), 1346–1356 (2008)
17. Shi, M., Wu, R., Krotov, D.S.: On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality. IEEE Transactions on Information Theory **65**(6), 3841–3847 (2019)