

# Butson full propelinear codes

José Andrés Armario\*

Universidad de Sevilla, Sevilla, Spain

Ivan Bailera†

Universitat Autònoma de Barcelona, Bellaterra, Spain

Ronan Egan‡

National University of Ireland Galway, Galway, Ireland

November 30, 2020

## Abstract

In this paper we study Butson Hadamard matrices, and codes over finite rings coming from these matrices in logarithmic form, called BH-codes. We introduce a new morphism of Butson Hadamard matrices through a generalized Gray map on the matrices in logarithmic form, which is comparable to the morphism given in a recent note of Ó Catháin and Swartz. That is, we show how, if given a Butson Hadamard matrix over the  $k^{\text{th}}$  roots of unity, we can construct a larger Butson matrix over the  $\ell^{\text{th}}$  roots of unity for any  $\ell$  dividing  $k$ , provided that any prime  $p$  dividing  $k$  also divides  $\ell$ .

We prove that a  $\mathbb{Z}_{p^s}$ -additive code with  $p$  a prime number is isomorphic as a group to a BH-code over  $\mathbb{Z}_{p^s}$  and the image of this BH-code under the Gray map is a BH-code over  $\mathbb{Z}_p$  (binary Hadamard code for  $p = 2$ ). Further, we investigate the inherent propelinear structure of these codes (and their images) when the Butson matrix is cocyclic. Some structural properties of these codes are studied and examples are provided.

**Keywords:** Cocycles, Butson Hadamard matrices, Gray map, propelinear codes.

**Mathematics Subject Classification (2010):** 05B20, 05E18, 94B60.

---

\*E-mail: armario@us.es

†E-mail: ivan.bailera@uab.cat

‡E-mail: ronan.egan@nuigalway.ie

# 1 Introduction

Let  $n$  and  $k$  be positive integers, and  $\zeta_k = \exp(2\pi\sqrt{-1}/k)$  be the complex  $k^{\text{th}}$  root of unity. We write  $\langle \zeta_k \rangle = \{\zeta_k^j\}_{0 \leq j \leq k-1}$ . Let  $\mathbb{Z}_k$  be the ring of integers modulo  $k$  with  $k > 1$ , and denote by  $\mathbb{Z}_k^n$  the set of  $n$ -tuples over  $\mathbb{Z}_k$ . We use bold notation  $\mathbf{x} = [x_1, \dots, x_n] \in \mathbb{Z}_k^n$  to denote vectors (or codewords) in  $\mathbb{Z}_k^n$ . We denote the set of  $n \times n$  matrices with entries in a set  $X$  by  $\mathcal{M}_n(X)$ .

## 1.1 Butson Hadamard matrices

A *Butson Hadamard* (or simply *Butson*) matrix of order  $n$  and phase  $k$  is a matrix  $H \in \mathcal{M}_n(\langle \zeta_k \rangle)$  such that  $HH^* = nI_n$ , where  $I_n$  denotes the identity matrix of order  $n$  and  $H^*$  denotes the conjugate transpose of  $H$ . We write  $\text{BH}(n, k)$  for the set of such matrices. The simplest examples of Butson matrices are the Fourier matrices  $F_n = [\zeta_n^{(i-1)(j-1)}]_{i,j=1}^n \in \text{BH}(n, n)$ . Hadamard matrices of order  $n$ , as they are usually defined, are the elements of  $\text{BH}(n, 2)$ . The phase and orthogonality of a  $\text{BH}(n, k)$  is preserved by multiplication on the left or right by a  $n \times n$  monomial matrix with non-zero entries in the  $k^{\text{th}}$  roots of unity. For any pair of such monomial matrices  $(P, Q)$  the operation defined by  $H(P, Q) = PHQ^* = H'$  is an equivalence operation, and  $H$  and  $H'$  are said to be *equivalent*. If  $H = H'$ , then  $(P, Q)$  is an automorphism of  $H$ .

A Butson matrix  $H \in \text{BH}(n, k)$  is conveniently represented in logarithmic form, that is, the matrix  $H = [\zeta_k^{\varphi_{i,j}}]_{i,j=1}^n$  is represented by the matrix  $L(H) = [\varphi_{i,j} \bmod k]_{i,j=1}^n$  with the convention that  $L_{i,j} \in \mathbb{Z}_k$  for all  $i, j \in \{1, \dots, n\}$ .

**Example 1.1.** The following is a  $\text{BH}(4, 8)$  matrix  $H$ , display in logarithmic form

$$L(H) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 \\ 0 & 4 & 0 & 4 \\ 0 & 6 & 4 & 2 \end{bmatrix}$$

Observe that the matrix above is in dephased form, that is, its first row and column are all 0. Every matrix can be dephased by using equivalence operations. Throughout this paper all matrices are assumed to be dephased.

**Example 1.2.** Let  $p$  be a prime number. If  $L(D) = [xy^T]_{x,y \in \mathbb{Z}_p^n}$  then  $D$  is a  $\text{BH}(p^n, p)$ . In fact  $D$  is the  $n$ -fold Kronecker product of the Fourier matrix of order  $p$ . When  $p = 2$  this is the well known Sylvester Hadamard matrix of order  $2^n$ .

Butson matrices have been subject to a considerable increase in interest recently for a variety of reasons. For one, a  $\text{BH}(n, k)$  exists for all  $n$ , (the Fourier matrix for example), but real Hadamard matrices, i.e.,  $\text{BH}(n, 2)$ , exist when  $n > 2$  only if  $n \equiv 0 \pmod{4}$ , and this condition is famously not yet known to be sufficient. A Butson morphism [8] is a map  $\text{BH}(n, k) \rightarrow \text{BH}(m, \ell)$ . This motivates the study of Butson matrices even if real Hadamard matrices are the primary interest. In Section 2.2 we construct a morphism  $\text{BH}(n, k) \rightarrow \text{BH}(nm, k/m)$  where  $k = p_1^{e_1} \cdots p_t^{e_t}$  and  $m = p_1^{e_1-1} \cdots p_t^{e_t-1}$ , matching the parameters of the morphism discovered by Ó Catháin and Swartz in [18]. But their applications in applied sciences most strongly motivate their study. A  $\text{BH}(n, k)$  scaled by a factor of  $1/\sqrt{n}$  is an orthonormal basis of  $\mathbb{C}^n$ . In any set of mutually unbiased bases (MUBs) which includes the standard basis, all other bases are necessarily of this form. MUBs have important applications in quantum physics, such as yielding optimal schemes of orthogonal quantum measurement (see e.g., [2]). Butson matrices also have applications in coding theory, as we discuss next.

## 1.2 BH-codes and propelinear codes

Interest in studying codes over finite rings increased significantly after it was proved in [11] that certain notorious non-linear binary codes (such as the Preparata codes or the Kerdock codes), which had some of the properties of linear codes were, in fact, the images of codes over  $\mathbb{Z}_4$  under a non-linear map (the Gray map). Codes constructed from Butson matrices [10, 17, 19, 21] are a particular type of codes over a finite ring. A code over  $\mathbb{Z}_k$  (or  $\mathbb{Z}_k$ -code) of length  $n$  is a nonempty subset  $C$  of  $\mathbb{Z}_k^n$ . The elements of  $C$  are called *codewords*. The Hamming weight of a vector  $\mathbf{x} \in \mathbb{Z}_k^n$ , denoted by  $\text{wt}_H(\mathbf{x})$ , is the number of nonzero coordinates of  $\mathbf{x}$ . The Hamming distance between two vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_k^n$ , denoted by  $d_H(\mathbf{x}, \mathbf{y}) = \text{wt}_H(\mathbf{x} - \mathbf{y})$ , is the number of coordinates in which they differ. Given a minimum Hamming distance  $d = \min_{\mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} d_H(\mathbf{x}, \mathbf{y})$  for a code  $C$  of length  $n$ , we say  $C$  is a  $(n, |C|, d)$  code. Other distances functions are used, for instance, the Lee distance between two vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_k^n$  is  $d_L(\mathbf{x}, \mathbf{y}) = \text{wt}_L(\mathbf{x} - \mathbf{y})$  where the Lee weight of a vector  $\mathbf{z} = [z_1, \dots, z_n] \in \mathbb{Z}_k^n$  is  $\text{wt}_L(\mathbf{z}) = \sum_{i=1}^n \text{wt}_L(z_i)$  with  $\text{wt}_L(z_i) = \min\{z_i, k - z_i\}$ .

Given  $H \in \text{BH}(n, k)$ , we denote by  $F_H$  the  $\mathbb{Z}_k$ -code of length  $n$  consisting of the rows of  $L(H)$ , and by  $C_H$  the  $\mathbb{Z}_k$ -code defined as  $C_H = \cup_{\alpha \in \mathbb{Z}_k} (F_H + \alpha \mathbf{1})$  where  $\mathbf{1}$  denotes the all-one vector (and  $\alpha \mathbf{1}$  the all- $\alpha$  vector). We will write  $\mathbf{1}_n$  to denote the all-one vector of length  $n$  when clarification is required. The code  $C_H$  over  $\mathbb{Z}_k$  is called a *Butson Hadamard code* (briefly, BH-code).

**Example 1.3.** Given  $H \in \text{BH}(4, 8)$  of Example 1.1. Then

$$F_H = \{[0, 0, 0, 0], [0, 2, 4, 6], [0, 4, 0, 4], [0, 6, 4, 2]\},$$

$$C_H = \left\{ \begin{array}{cccc} [0, 0, 0, 0], & [0, 2, 4, 6], & [0, 4, 0, 4], & [0, 6, 4, 2], \\ [1, 1, 1, 1], & [1, 3, 5, 7], & [1, 5, 1, 5], & [1, 7, 5, 3], \\ [2, 2, 2, 2], & [2, 4, 6, 0], & [2, 6, 2, 6], & [2, 0, 6, 4], \\ [3, 3, 3, 3], & [3, 5, 7, 1], & [3, 7, 3, 7], & [3, 1, 7, 5], \\ [4, 4, 4, 4], & [4, 6, 0, 2], & [4, 0, 4, 0], & [4, 2, 0, 6], \\ [5, 5, 5, 5], & [5, 7, 1, 3], & [5, 1, 5, 1], & [5, 3, 1, 7], \\ [6, 6, 6, 6], & [6, 0, 2, 4], & [6, 2, 6, 2], & [6, 4, 2, 0], \\ [7, 7, 7, 7], & [7, 1, 3, 5], & [7, 3, 7, 3], & [7, 5, 3, 1] \end{array} \right\}.$$

Assuming the Hamming metric, any isometry of  $\mathbb{Z}_k^n$  is given by a coordinate permutation  $\pi$  and  $n$  permutations  $\sigma_1, \dots, \sigma_n$  of  $\mathbb{Z}_k$ . We denote by  $\text{Aut}(\mathbb{Z}_k^n)$  the group of all isometries of  $\mathbb{Z}_k^n$ :

$$\text{Aut}(\mathbb{Z}_k^n) = \{(\sigma, \pi) : \sigma = (\sigma_1, \dots, \sigma_n) \text{ with } \sigma_i \in \text{Sym } \mathbb{Z}_k, \pi \in \mathcal{S}_n\}$$

where  $\text{Sym } \mathbb{Z}_k$  and  $\mathcal{S}_n$  denote, respectively, the symmetric group of permutations on  $\mathbb{Z}_k$  and on the set  $\{1, \dots, n\}$ . The action of  $(\sigma, \pi)$  is defined as

$$(\sigma, \pi)(\mathbf{v}) = \sigma(\pi(\mathbf{v})) \quad \text{for any } \mathbf{v} \in \mathbb{Z}_k^n,$$

and the group operation in  $\text{Aut}(\mathbb{Z}_k^n)$  is the composition

$$(\sigma, \pi) \circ (\sigma', \pi') = ((\sigma_1 \circ \sigma'_{\pi^{-1}(1)}, \dots, \sigma_n \circ \sigma'_{\pi^{-1}(n)}), \pi \circ \pi')$$

for all  $(\sigma, \pi), (\sigma', \pi') \in \text{Aut}(\mathbb{Z}_k^n)$ .

**Definition 1.4.** A code  $C$  of length  $n$  over  $\mathbb{Z}_k$  has a propelinear structure if for any codeword  $\mathbf{x} \in C$  there exist  $\pi_{\mathbf{x}} \in \mathcal{S}_n$  and  $\sigma_{\mathbf{x}} = (\sigma_{\mathbf{x},1}, \dots, \sigma_{\mathbf{x},n})$  with  $\sigma_{\mathbf{x},i} \in \text{Sym } \mathbb{Z}_k$  satisfying:

$$(i) \quad (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(C) = C \text{ and } (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{0}) = \mathbf{x},$$

$$(ii) \quad \text{if } \mathbf{y} \in C \text{ and } \mathbf{z} = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{y}), \text{ then } (\sigma_{\mathbf{z}}, \pi_{\mathbf{z}}) = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}}) \circ (\sigma_{\mathbf{y}}, \pi_{\mathbf{y}}).$$

The propelinear structure was introduced in [22] for binary codes, and it was generalized in [3] for  $q$ -ary codes.

For a code  $C \subseteq \mathbb{Z}_k^n$ , we denote by  $\text{Aut}(C)$  the group of all isometries of  $\mathbb{Z}_k^n$  fixing the code  $C$  and we call it the *automorphism group* of the code  $C$ . A code  $C$  over  $\mathbb{Z}_k$  is called *transitive* if  $\text{Aut}(C)$  acts transitively on its codewords, i.e., the code satisfies the property (i) of the above definition.

Assuming that  $C$  has a propelinear structure then a binary operation  $\star$  can be defined as

$$\mathbf{x} \star \mathbf{y} = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{y}) \quad \text{for any } \mathbf{x}, \mathbf{y} \in C.$$

Therefore,  $(C, \star)$  is a group, which is not abelian in general. This group structure is compatible with the Hamming distance, that is,  $d_H(\mathbf{x} \star \mathbf{u}, \mathbf{x} \star \mathbf{v}) = d_H(\mathbf{u}, \mathbf{v})$  where  $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_k^n$ . The vector  $\mathbf{0}$  is always a codeword where  $\pi_{\mathbf{0}} = Id_n$  is the identity coordinate permutation and  $\sigma_{\mathbf{0},i} = Id_k$  is the identity permutation on  $\mathbb{Z}_k$  for all  $i \in \{1, \dots, n\}$ . Hence,  $\mathbf{0}$  is the identity element in  $C$  and  $\pi_{\mathbf{x}^{-1}} = \pi_{\mathbf{x}}^{-1}$  and  $\sigma_{\mathbf{x}^{-1},i} = \sigma_{\mathbf{x},\pi_{\mathbf{x}}(i)}^{-1}$  for all  $\mathbf{x} \in C$  and for all  $i \in \{1, \dots, n\}$ . We call  $(C, \star)$  a *propelinear code*. Henceforth we use  $C$  instead of  $(C, \star)$  if there is no confusion.

**Definition 1.5.** A full propelinear code is a propelinear code  $C$  such that for every  $\mathbf{a} \in C$ ,  $\sigma_{\mathbf{a}}(\mathbf{x}) = \mathbf{a} + \mathbf{x}$  and  $\pi_{\mathbf{a}}$  has not any fixed coordinate when  $\mathbf{a} \neq \alpha \mathbf{1}$  for  $\alpha \in \mathbb{Z}_k$ . Otherwise,  $\pi_{\mathbf{a}} = Id_n$ .

**Remark 1.6.** Every linear code is propelinear but not necessarily full.

A Butson Hadamard code, which is also full propelinear, is called a *Butson Hadamard full propelinear code* (briefly, BHFP-code). In the binary case, we have the Hadamard full propelinear codes, they were introduced in [23] and their equivalence with Hadamard groups was proven. In the  $q$ -ary case, i.e., codes over the finite field  $\mathbb{F}_q$  where  $q$  is a prime power, the generalized Hadamard full propelinear codes were introduced in [1]. Their existence is shown to be equivalent to the existence of central relative  $(n, q, n, n/q)$ .

Propelinear codes are a topic of increasing interest in algebraic coding theory. The primary reason for this is that they offer one of the main benefits of linear codes, which is that they can be entirely described by a few generating codewords and group relations. However as the codes are not necessarily linear, they are not subject to all of the same minimum distance constraints as linear codes with the same number of codewords. Some propelinear codes may outperform comparable linear codes by having a larger minimum distance than any linear code of the same size, or by having more codewords than any linear code with a given minimum distance [1, 11]. In this paper we extend the work of the authors in [1] and describe the connection between cocyclic Butson Hadamard matrices and BHFP-codes.

## 2 Constructing Butson Hadamard matrices and related codes

Throughout this paper we study BH-codes over  $\mathbb{Z}_k$ . We have already introduced the Lee and Hamming distance between vectors  $\mathbf{x}$  and  $\mathbf{y}$ . We define other useful distance functions here. Initially, let  $k = p^s$  for a prime  $p$ . The weight function  $\text{wt}^*(x)$  with  $x \in \mathbb{Z}_{p^s}$  is defined by

$$\text{wt}^*(x) = \begin{cases} (p-1)p^{s-2} & x \neq kp^{s-1} \pmod{p^s}, k \in \mathbb{Z}_p \\ p^{s-1} & x = kp^{s-1} \pmod{p^s}, k \in \mathbb{Z}_p \setminus \{0\} \\ 0 & x = 0 \pmod{p^s} \end{cases}$$

For  $p = s = 2$ , this is the Lee weight. The corresponding distance  $d^*$  on  $\mathbb{Z}_{p^s}^n$  is defined as follows:

$$d^*(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \text{wt}^*(y_i - x_i), \quad (1)$$

where  $\mathbf{x} = [x_1, \dots, x_n]$  and  $\mathbf{y} = [y_1, \dots, y_n]$  in  $\mathbb{Z}_{p^s}^n$ . More generally, let  $k = mp^s$  for  $m$  coprime to  $p$ . Any  $x \in \mathbb{Z}_k$  may be written uniquely in the form  $x = ap^s + bm \pmod{k}$  where  $0 \leq a \leq m-1$  and  $0 \leq b \leq p^s-1$ . Define the weight function  $\text{wt}^\dagger(x)$  on  $\mathbb{Z}_k$  by

$$\text{wt}^\dagger(x) = \begin{cases} \text{wt}^*(b) & a = 0 \\ p^{s-1} & a \neq 0. \end{cases}$$

The definition of the weight function here is consistent with the homogeneous metric introduced in [5]. The corresponding distance  $d^\dagger$  on  $\mathbb{Z}_{mp^s}^n$  is defined as follows:

$$d^\dagger(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \text{wt}^\dagger(y_i - x_i), \quad (2)$$

where  $\mathbf{x} = [x_1, \dots, x_n]$  and  $\mathbf{y} = [y_1, \dots, y_n]$  in  $\mathbb{Z}_{mp^s}^n$ .

Given  $H \in \text{BH}(n, k)$ , recall that  $F_H$  is the  $\mathbb{Z}_k$ -code of length  $n$  consisting of the rows of  $L(H)$ , and  $C_H = \cup_{\alpha \in \mathbb{Z}_k} (F_H + \alpha \mathbf{1})$ . Let  $r_H^i(l)$  be the number of repetitions of  $l \in \mathbb{Z}_k$  in the  $i$ -th row of  $L(H)$  and  $r_H(l) = \max_{2 \leq i \leq n} r_H^i(l)$ .

For  $k = p^s$ , Lemma 3.1 of [16] gives a pattern that any row of  $L(H)$  has to follow. That is, any row  $\mathbf{x}$  has to be a permutation of the vector  $(\mathbf{u}, r_1 \mathbf{1} + \mathbf{u}, \dots, r_{t-1} \mathbf{1} + \mathbf{u})$  where  $\mathbf{u} = [0, p^{s-1}, 2p^{s-1}, \dots, (p-1)p^{s-1}]$ ,  $r_i \in \mathbb{Z}_{p^{s-1}}$ , for  $1 \leq i \leq t-1$  with  $t = \frac{n}{p}$ . Therefore,

$$r_H(l) \leq \begin{cases} \frac{n}{p} & l = hp^{s-1} \text{ where } h \in \mathbb{Z}_p \\ \frac{n}{p} - 1 & \text{Otherwise.} \end{cases}$$

As a consequence,  $n - \frac{n}{p}$  is an upper bound for the minimum Hamming distance of  $F_H$  when  $k = p^s$ . Furthermore, the minimum Hamming distance of both codes,  $F_H$  and  $C_H$ , is the same in this case.

In [19, 21], the authors prove that if  $n = p^{sm}$  and  $k = p^s$  then the minimum Hamming distance of  $F_H$  is  $n - \frac{n}{p}$  and the minimum Lee distance is given by

$$d_L = \begin{cases} 2^{m+s-2}, & p = 2 \\ \frac{p^{s(m+1)-2}}{4}(p^2 - 1), & p > 2 \text{ prime;} \end{cases}$$

where  $H$  is the Butson matrix of Theorem 2.3 and  $m = t_1 - 1$  for  $t_1 > 0$  and  $t_2 = \dots = t_s = 0$ .

Finally, Theorem 5.4 of [10] claims that for any pair  $(n, k)$  such that  $\text{BH}(n, k) \neq \emptyset$ , if  $H \in \text{BH}(n, k)$  then the code obtained by deleting the first coordinate in  $F_H$  has parameters  $(n - 1, n, \gamma n)$  meeting the Plotkin bound over Frobenius rings where  $\gamma$  is the average homogeneous weight over  $\mathbb{Z}_k$ .

## 2.1 A Fourier type construction and simplex codes

In what follows, we describe a method to construct Butson matrices of order  $n = p^{st_1+(s-1)t_2+\dots+t_s-s}$  and phase  $k = p^s$ , where  $p$  is a prime. Let  $s$  be a positive integer,  $t_1, t_2, \dots, t_s$  be nonnegative integers with  $t_1 \geq 1$ , and  $A^{1,0,\dots,0} = [0]$ . The matrix  $A^{t_1,t_2,\dots,t_s}$ , where  $\mathbf{p}^{i-1}$  denotes the all- $p^{i-1}$  vector, is defined recursively according to the following algorithm, where initially,  $(t'_1, t'_2, \dots, t'_s) = (1, 0, \dots, 0)$ .

```

for i=1 until s do
  while  $t'_i < t_i$  do
     $A \leftarrow A^{t'_1,\dots,t'_s}$ 
     $t'_i \leftarrow t'_i + 1$ 
     $A^{t'_1,\dots,t'_s} \leftarrow A_i = \begin{bmatrix} A & A & \dots & A \\ 0 \cdot \mathbf{p}^{i-1} & 1 \cdot \mathbf{p}^{i-1} & \dots & (p^{s-i+1} - 1) \cdot \mathbf{p}^{i-1} \end{bmatrix}$ 
  end while
end for

```

By construction, it is clear that  $A^{t_1,t_2,\dots,t_s}$  is a  $(t_1 + t_2 + \dots + t_s) \times (p^{st_1+(s-1)t_2+\dots+t_s-s})$  matrix. This is a generalization of the construction of [19] as we will point out in Corollary 2.8.

**Example 2.1.** For  $p = 2$  and  $s = 3$ . We have  $A^{1,1,0} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 \end{bmatrix}$  and

$$A^{1,1,1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 \end{bmatrix}.$$

Given  $\mathbf{x} \in \mathbb{Z}_k^n$ , the *order* of  $\mathbf{x}$  is the smallest positive integer  $m$  such that  $m\mathbf{x} = \mathbf{0}$  over  $\mathbb{Z}_k$ .

**Lemma 2.2.** *Let  $k = p^s$  and  $\mathbf{u}_i = [0 \cdot \mathbf{p}^{i-1}, 1 \cdot \mathbf{p}^{i-1}, \dots, (p^{s-i+1} - 1) \cdot \mathbf{p}^{i-1}] \in \mathbb{Z}_{p^s}^{p^{s-i+1}}$  where  $1 \leq i \leq s$ . Then*

- $\sum_{j=0}^{p^{s-i+1}-1} \zeta_k^{jp^{i-1}} = 0$ , for all  $1 \leq i \leq s$ .
- The order of  $\mathbf{u}_i$  is  $p^{s-i+1}$ .
- If  $\gcd(m, p^{s-i+1}) = 1$  then  $[m\mathbf{u}_i]_j = [\mathbf{u}_i]_{\pi(j)}$  where  $\pi \in \mathcal{S}_{p^{s-i+1}}$ .
- If  $\gcd(m, p^{s-i+1}) = p^l$  then  $[m\mathbf{u}_i]_j = [\frac{m}{p^l}\mathbf{u}_i]_{\pi(j \bmod p^{s-(i+l)+1})}$  where  $\pi \in \mathcal{S}_{p^{s-(i+l)+1}}$ .

*Proof.* It is a straightforward comprobation. □

**Theorem 2.3.** *Let  $n = p^{st_1+(s-1)t_2+\dots+t_s-s}$  and  $L(H)$  be the  $n \times n$  matrix whose rows are the  $n$  possible linear combinations (with coefficients in  $\mathbb{Z}_{p^s}$ ) of the rows of  $A^{t_1, t_2, \dots, t_s}$ . Then,  $H \in \text{BH}(n, p^s)$ .*

*Proof.* By construction, the difference between two distinct rows of  $L(H)$  is a linear combination (with coefficients in  $\mathbb{Z}_{p^s}$ ) of the rows of  $A^{t_1, t_2, \dots, t_s}$ . Hence, it is a row of  $L(H)$ .

Therefore, proving  $HH^* = nI_n$  reduces to proving that every row sum of  $H$  is 0. For the rows of  $H$  corresponding to multiples of the rows of  $A^{t_1, t_2, \dots, t_s}$ , this holds as a consequence of Lemma 2.2. Finally, the proof for the rows of  $H$  corresponding to a linear combination of the rows of  $A^{t_1, t_2, \dots, t_s}$  is by a simple induction. □

We provide some examples of Butson matrices coming from Theorem 2.3.

**Example 2.4.** Let  $p = 2$  and  $s = 3$ . For  $t_1 = 1, t_2 = 1, t_3 = 0$  then  $L(H)$  is the matrix given in Example 1.1. For  $t_1 = 1, t_2 = 1, t_3 = 1$  then



$H \in \text{BH}(8, 8)$  where

$$L(H) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\ 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\ 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\ 0 & 0 & 0 & 0 & 4 & 4 & 4 & 4 \\ 0 & 2 & 4 & 6 & 4 & 6 & 0 & 2 \\ 0 & 4 & 0 & 4 & 4 & 0 & 4 & 0 \\ 0 & 6 & 4 & 2 & 4 & 2 & 0 & 6 \end{bmatrix}$$

**Remark 2.5.** Let  $L(H)$  be the matrix of Example 2.4 for  $t_1 = 1, t_2 = 1, t_3 = 1$ . Then  $L(H) = L(F_2 \otimes F_4)$  where we have used that  $F_2 \otimes F_4 \in \text{BH}(8, 8)$  by means of  $\zeta_2 = \zeta_8^4$  and  $\zeta_4 = \zeta_8^2$ .

In general we have the following.

**Proposition 2.6.** Let  $n = p^{st_1+(s-1)t_2+\dots+t_s-s}$  and  $L(H)$  be the  $n \times n$  matrix of Theorem 2.3. Then,  $H$  is equivalent to

$$(F_p)^{t_s} \otimes (F_{p^2})^{t_{s-1}} \otimes \dots \otimes (F_{p^{s-1}})^{t_2} \otimes (F_{p^s})^{t_1-1}$$

where  $F_{p^{s-j}}$  denotes the Fourier matrix of order  $p^{s-j}$  embedded in  $\text{BH}(p^{s-j}, p^s)$  using that  $\zeta_{p^{s-j}} = \zeta_{p^s}^{p^j}$ , and  $(M)^r$  denotes the  $r$ -fold Kronecker product of the matrix  $M$ .

*Proof.* The proof is by induction. The case  $t_1, t_2, \dots, t_s = 1, 0, \dots, 0$  is trivial, so consider the case  $t_1 = 2$  and  $t_2 = \dots = t_s = 0$ . It is clear that  $L(H) = L(F_{p^s})$  since  $A^{2,0,\dots,0} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & p^s - 1 \end{bmatrix}$ . For the next step of the induction, we assume that  $t_{i+1} = \dots = t_s = 0$  and  $L(H) = L((F_{p^{s-(i-1)}})^{t'_i} \otimes (F_{p^{s-(i-1)}})^{t_{i-1}} \otimes \dots \otimes (F_{p^{s-1}})^{t_2} \otimes (F_{p^s})^{t_1-1})$ . Now, we have to distinguish two possibilities:

- $t'_i < t_i$ ; then let  $t'_i \leftarrow t'_i + 1$  and  $t_{i+1} = \dots = t_s = 0$ . All the possible linear combinations of the rows of  $A^{t_1, \dots, t_{i-1}, t'_i+1, 0, \dots, 0}$  are the rows of  $B = L(F_{p^{s-(i-1)}} \otimes H)$ .
- $t'_i = t_i$ ; then take  $t_{i+1} = 1$  with  $t_{i+2} = \dots = t_s = 0$ . Proceeding in a similar way, the result holds.

□

It is clear now that this construction is not new, in the sense that it does not produce any Butson matrices not already known. However this perspective gives us new insights into the related BH-codes.

**Remark 2.7.** For  $t_1 \neq 0, t_2 = \dots = t_s = 0$  and  $p = 2$ , the code generated with the rows of  $A^{t_1, 0, \dots, 0}$  is a  $\mathbb{Z}_{p^s}$ -simplex code of type  $\alpha$  (see [19, Definition 4.1]). Furthermore, this code is self-orthogonal if  $s = 2$ .

**Corollary 2.8.** *A simplex code of type  $\alpha$  over  $\mathbb{Z}_{2^s}$  of length  $2^{sm}$  (see [19]) and the code whose codewords are the rows of  $L((F_{2^s})^m)$  are the same. Therefore  $M_\psi$ , the cocyclic BH( $2^{sm}, 2^s$ ) of [19, Theorem 5.1, ii)] is equivalent to  $(F_{2^s})^m$ . Similarly, when  $p > 2$  prime, the analogous classifying result for the cocyclic BH( $p^{sm}, p^s$ ) of [21, Proposition 3.1, ii)] holds.*

*Proof.* Attending to the Remark above, a simplex code of type  $\alpha$  over  $\mathbb{Z}_{2^s}$  of length  $n = 2^{st_1}$  is exactly the code  $F_H$  where  $H$  is the  $n \times n$  matrix of Theorem 2.3. Applying Proposition 2.6, the results follows.  $\square$

The classifying result above follows also as a consequence of [17, Theorem 13].

A nonempty subset  $\mathcal{C}$  of  $\mathbb{Z}_{p^s}^n$  is a  $\mathbb{Z}_{p^s}$ -additive code if it is a subgroup of  $\mathbb{Z}_{p^s}^n$  (i.e., a  $\mathbb{Z}_{p^s}$ -module). Clearly, given a  $\mathbb{Z}_{p^s}$ -additive code,  $\mathcal{C}$ , of length  $n$  there exist some non negative integers  $t_1, \dots, t_s$  such that  $\mathcal{C}$  is isomorphic (as an abelian group) to  $\mathbb{Z}_{p^{t_1}} \times \mathbb{Z}_{p^{t_2}} \times \dots \times \mathbb{Z}_{p^{t_s}}$ . Thus,  $\mathcal{C}$  is said to be of type  $(n; t_1, \dots, t_s)$ . Note that  $|\mathcal{C}| = p^{st_1} p^{(s-1)t_2} \dots p^{t_s}$  since there are  $t_1$  (generators) codewords of order  $p^s$ ,  $t_2$  of order  $p^{s-1}$  and so on.

**Remark 2.9.** Let  $t_1, \dots, t_s$  be non negative integers and taking  $A^{1, 0, \dots, 0} = [1]$  instead of  $[0]$ , the method described at the beginning of this section provides  $A^{t_1, t_2, \dots, t_s}$  as a generator matrix for a  $\mathbb{Z}_{p^s}$ -additive code of type  $(n; t_1, \dots, t_s)$  where  $n = p^{st_1 + (s-1)t_2 + \dots + t_s - s}$ . The description of recursive constructions of these matrices are in [9, 13, 14] for  $p = 2$ . The case  $p \neq 2$  has been studied in [24]. We will denote the codes associated to these matrices by  $\mathcal{H}^{t_1, \dots, t_s}$ . Let us point out that  $\mathcal{H}^{0, t_2, \dots, t_s} \subset \mathcal{H}^{1, t_2, \dots, t_s}$ .

Now, we establish the following result.

**Proposition 2.10.** *For  $t_1 > 0$ , every  $\mathcal{H}^{t_1, \dots, t_s}$  is a BH-code where the Butson Hadamard matrix is a Kronecker product of Fourier matrices.*

*Proof.* Let  $C_H$  be the BH-code associated to  $H$  of Theorem 2.3. It is clear that  $C_H$  is equivalent to  $\mathcal{H}^{t_1, \dots, t_s}$ . Now, the result follows from Proposition 2.6.  $\square$

The following is an example of a BH-code which is not additive.

**Example 2.11.** Let  $H \in \text{BH}(8, 4)$  with

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

$C_H$  is not  $\mathbb{Z}_{2^2}$ -additive since the double of the second row is not a codeword.

Now, we can state that, in a certain sense, the class of BH-codes encompasses strictly the class of  $\mathbb{Z}_{p^s}$ -additive codes. Since any  $\mathbb{Z}_{p^s}$ -additive code is always of type  $(n; t_1, \dots, t_s)$  for some non negatives integers  $t_1, \dots, t_s$  and  $\mathcal{H}^{t_1, \dots, t_s} \in \text{BH}(p^{st_1 + (s-1)t_2 + \dots + t_s - s}, p^s)$ , assuming that  $t_1 > 0$ .

## 2.2 Generalized Gray map

The Gray map is a function from  $\mathbb{Z}_4$  to  $\mathbb{Z}_2^2$  which is typically used to form binary codes from  $\mathbb{Z}_4$ -codes. In what follows, we introduce a generalized Gray map  $\Phi_p$  from  $\mathbb{Z}_{p^s}$  to  $\mathbb{Z}_p^{p^{s-1}}$ , and extend this to a yet more general function  $\Psi_p$  from  $\mathbb{Z}_{mp^s}$  to  $\mathbb{Z}_{mp}^{p^{s-1}}$ . For  $k = p_1^{e_1} \cdots p_t^{e_t}$ , and  $\ell = p_1 \cdots p_t$  the composition  $\Psi_{p_t} \cdots \Psi_{p_1}$  is a function from  $\mathbb{Z}_k$  to  $\mathbb{Z}_\ell^{k/\ell}$ . From this function we construct a morphism  $\text{BH}(n, k) \rightarrow \text{BH}(nk/\ell, \ell)$ . Where  $\mathbf{x} = [x_1, \dots, x_n] \in \mathbb{Z}_k^n$  and  $\varphi$  is any function with domain  $\mathbb{Z}_k$ , we will write  $\varphi(\mathbf{x}) = [\varphi(x_1), \dots, \varphi(x_n)]$ . Further, we write  $\varphi(\mathcal{C}) = \{\varphi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}\}$  where  $\mathcal{C} \subseteq \mathbb{Z}_k^n$ .

We consider the elements of  $\mathbb{Z}_p^{s-1}$  to be ordered in increasing lexicographic order. We denote by  $D$  the  $\text{BH}(p^{s-1}, p)$  matrix defined in Example 1.2 and label the rows of  $L(D)$  in the order  $0, 1, \dots, p^{s-1} - 1$ . Let  $[L(D)]_i$  denotes the row of  $L(D)$  labeled by  $i$ . Then we let  $\Phi_p : \mathbb{Z}_{p^s} \rightarrow \mathbb{Z}_p^{p^{s-1}}$  be the map defined by

$$\Phi_p(x) = [L(D)]_b + a\mathbf{1}, \quad x = ap^{s-1} + b.$$

Let us observe that for  $p = 2$ ,  $\Phi_p$  is the well-known Carlet's map [4] and for  $p > 2$ ,  $\Phi_p$  is of type  $\varphi$  given in [24]. For what remains of this section we write  $\Phi = \Phi_p$  for brevity unless there is some confusion.

**Proposition 2.12** ([24]). *The entrywise application of  $\Phi$  is an isometric embedding of  $(\mathbb{Z}_{p^s}^n, d^*)$  into  $(\mathbb{Z}_p^{p^{s-1}n}, d_H)$ . Furthermore, if  $\mathcal{C}$  is a code with parameters  $(n, M, d^*)$  over  $\mathbb{Z}_{p^s}$ , then the image code  $C = \Phi(\mathcal{C})$  is a code with parameters  $(p^{s-1}n, M, d_H)$  over  $\mathbb{Z}_p$ .*

**Lemma 2.13.** *Let  $x, y \in \mathbb{Z}_{p^s}$ . Then  $\Phi(x - y) = \Phi(x) - \Phi(y) + \alpha \mathbf{1}$  where  $\alpha \in \{0, p - 1\}$ .*

*Proof.* Let  $x = a_1 p^{s-1} + b_1$  and  $y = a_2 p^{s-1} + b_2$ . Then

$$x - y = \begin{cases} (a_1 - a_2)p^{s-1} + (b_1 - b_2), & \text{if } b_1 \geq b_2 \\ (a_1 - a_2 - 1)p^{s-1} + (b_1 - b_2), & \text{if } b_1 < b_2. \end{cases}$$

Further, by the linearity of the inner product  $vw^T$  and the definition  $L(D) = [vw^T]_{v,w \in \mathbb{Z}_p^n}$  it follows that  $\Phi(b_1 - b_2 \bmod p^{s-1}) = [L(D)]_{b_1 - b_2} = [L(D)]_{b_1} - [L(D)]_{b_2} = \Phi(b_1) - \Phi(b_2)$ . Thus  $\Phi(x - y) = \Phi(x) - \Phi(y) + \alpha \mathbf{1}$  where  $\alpha = 0$  if  $b_1 \geq b_2$ , and  $\alpha = p - 1$  otherwise.  $\square$

Given  $H \in \mathcal{M}_n(\langle \zeta_{p^s} \rangle)$ , we write  $L(H^\Phi)$  for the entrywise application of  $\Phi$  to

$$\begin{bmatrix} L(H) \\ L(H) + J \\ L(H) + 2J \\ \vdots \\ L(H) + (p^{s-1} - 1)J \end{bmatrix}.$$

Then  $H^\Phi$  is the corresponding matrix in  $\mathcal{M}_{np^{s-1}}(\langle \zeta_p \rangle)$ .

**Theorem 2.14.** *If  $H \in \text{BH}(n, p^s)$ , then  $H^\Phi \in \text{BH}(np^{s-1}, p)$ .*

*Proof.* Observe that  $H^\Phi$  is Butson Hadamard over  $\langle \zeta_p \rangle$  if, for all  $i \neq j$ , the sequence of differences  $[L(H^\Phi)]_{i,l} - [L(H^\Phi)]_{j,l}$ ,  $0 \leq l \leq n \cdot p^{s-1} - 1$  contains each element of  $\mathbb{Z}_p$  equally often. First note that for all  $i \neq j$ , the sequence of differences  $[L(H)]_{i,l} - [L(H)]_{j,l}$ ,  $0 \leq l \leq n - 1$  contains each element of the form  $ap^{s-1}$  equally often for  $a = 0, \dots, p - 1$ . This is a consequence of  $\zeta_k^{ap^{s-1}}$  being a  $p^{\text{th}}$  root of unity. By Lemma 2.13, if  $x - y = ap^{s-1}$  then  $\Phi(x - y) = \Phi(x) - \Phi(y)$ . Since  $\Phi(ap^{s-1}) = a \mathbf{1}$  for  $a \in \mathbb{Z}_p$ , it follows that if the set of differences  $[L(H)]_{i,l} - [L(H)]_{j,l}$  contains  $m$  repetitions of each element of the form  $ap^{s-1}$ , then the set of corresponding differences in  $[L(H^\Phi)]_{i,l} - [L(H^\Phi)]_{j,l}$  contains  $mp^{s-1}$  repetitions of each element of  $\mathbb{Z}_p$ . Finally, if  $x - y \not\equiv 0 \pmod{p^{s-1}}$ , then  $\Phi(x) - \Phi(y) = \Phi(x - y) + \alpha \mathbf{1}$  for some  $\alpha$ , where  $x - y = ap^{s-1} + b$  and  $b \neq 0$ . Thus  $\Phi(x - y) = a \mathbf{1} + [L(D)]_b$  which contains every element of  $\mathbb{Z}_p$  exactly  $p^{s-2}$ -times, and so too does  $\Phi(x) - \Phi(y)$ .  $\square$

**Corollary 2.15.** *The image of any BH-code over  $\mathbb{Z}_{p^s}$  of length  $n$  by  $\Phi$  is a BH-code over  $\mathbb{Z}_p$  of length  $n \cdot p^{s-1}$  and minimum Hamming distance  $d_H = np^{s-2}(p - 1)$ .*

**Remark 2.16.** Let us point out that Theorem 1 of [9] is a particular case of Corollary 2.15 (when the BH-code is of type  $\mathcal{H}^{t_1, \dots, t_s}$  and  $p = 2$ ).

**Proposition 2.17.** *Any BH-code  $C_H$  of length  $n$  over  $\mathbb{Z}_{p^s}$  has minimum distance  $d^* = np^{s-2}(p-1)$ .*

*Proof.* Taking into account that  $\text{BH}(n, p) = \text{GH}(p, n/p)$  where  $\text{GH}(p, n/p)$  denotes the set of generalized Hadamard matrices of order  $n$  over  $\mathbb{F}_p$  (see [7, Lemma 2.2]). Thus,  $C_{H^\Phi} = \Phi(C_H)$  is a generalized Hadamard code as well since  $H^\Phi \in \text{BH}(p^{s-1}n, p)$ . The minimum Hamming distance of these codes is well known to be  $np^{s-2}(p-1)$ . The fact that  $\Phi$  is an isometric embedding (Proposition 2.12) concludes the proof.  $\square$

Now let  $k = mp^s$  where  $p$  does not divide  $m$  and recall that every element  $x \in \mathbb{Z}_k$  can be written uniquely as  $x = ap^s + bm \pmod k$  for some  $0 \leq a \leq m-1$  and  $0 \leq b \leq p^s-1$ . Then let

$$\Psi_p(ap^s + bm) = m\Phi_p(b) + ap\mathbf{1}$$

define a map  $\mathbb{Z}_k \rightarrow \mathbb{Z}_{mp}^{p^{s-1}}$ .

**Proposition 2.18.** *The entrywise application of  $\Psi_p$  is an isometric embedding of  $(\mathbb{Z}_{mp^s}^n, d^\dagger)$  into  $(\mathbb{Z}_{mp}^{p^{s-1}n}, d_H)$ . Furthermore, if  $\mathcal{C}$  is a code with parameters  $(n, M, d^\dagger)$  over  $\mathbb{Z}_{mp^s}$ , then the image code  $C = \Psi_p(\mathcal{C})$  is a code with parameters  $(p^{s-1}n, M, d_H)$  over  $\mathbb{Z}_{mp}$ .*

*Proof.* This follows from a straight forward extension of Proposition 2.12.  $\square$

Given  $H \in \mathcal{M}_n(\langle \zeta_k \rangle)$  where  $k = p^s m$ , we write  $L(H^{\Psi_p})$  for the entrywise application of  $\Psi_p$  to

$$\begin{bmatrix} L(H) \\ L(H) + mJ \\ L(H) + 2mJ \\ \vdots \\ L(H) + (p^{s-1} - 1)mJ \end{bmatrix}.$$

Then  $H^{\Psi_p}$  is the corresponding matrix in  $\mathcal{M}_{np^{s-1}}(\langle \zeta_{pm} \rangle)$ . We will devote the rest of this section to a proof of the following.

**Theorem 2.19.** *If  $H \in \text{BH}(n, k)$  where  $k = p^s m$ , then  $H^{\Psi_p} \in \text{BH}(np^{s-1}, pm)$ .*

Repeated application of  $\Psi_p$  for all primes  $p$  dividing  $k$  gives the following.

**Corollary 2.20.** *If there exists a  $\text{BH}(n, k)$  where  $k = p_1^{s_1} \cdots p_r^{s_r}$ , then there exists a  $\text{BH}(nk/\ell, \ell)$  where  $\ell = p_1 \cdots p_r$ .*

Before we can prove Theorem 2.19, we will need to establish some preliminary results. Hereafter we fix a prime  $p$  and let  $\Psi = \Psi_p$ .

**Lemma 2.21.** *For all  $0 \leq x, y < k = mp^s$ ,  $\Psi(x - y) = \Psi(x) - \Psi(y) + m\alpha\mathbf{1}$  where  $\alpha \in \{0, p - 1\}$ .*

*Proof.* Let  $x = ap^s + bm$  and  $y = cp^s + dm$ . Observe that  $\Psi(x - y) = (a - c)p\mathbf{1} + m\Phi(b - d)$ . By Lemma 2.13,  $\Phi(b - d) = \Phi(b) - \Phi(d) + \alpha\mathbf{1}$  where  $\alpha \in \{0, p - 1\}$ . The result follows.  $\square$

**Lemma 2.22.** *Let  $z \neq fp^{s-1}$  for any  $0 \leq f \leq mp - 1$ . Then  $\sum_{i=1}^{p^{s-1}} \omega^{\Psi(z)_i} = 0$  where  $\omega$  is a primitive  $k^{\text{th}}$  root of unity. Otherwise,  $\Psi(z) = f\mathbf{1}$ , and  $\sum_{i=1}^{p^{s-1}} \omega^{\Psi(z)_i} = p^{s-1}\omega^f$ .*

*Proof.* First suppose that  $z \neq fp^{s-1}$ . Observe that  $\Psi(z) = m[L(D)]_j + \alpha\mathbf{1}$  for some  $\alpha \in \mathbb{Z}_{pm}$  and  $j \neq 0$ . Then  $\sum_{i=0}^{p^{s-1}-1} \omega^{\Psi(z)_i} = \sum_{i=1}^{p^{s-1}} \omega^{[L(D)]_{j,i} + \alpha} = \omega^\alpha \sum_{i=0}^{p^{s-1}-1} \omega^{[L(D)]_{j,i}} = 0$ .

Now suppose that  $z = fp^{s-1}$ . Then  $f = gm + hp \pmod{mp}$  where  $0 \leq g \leq p - 1$  and  $0 \leq h \leq m - 1$ . Thus  $fp^{s-1} = hp^s + gmp^{s-1} \pmod{p^s m}$ . It follows that  $\Psi(z) = hp\mathbf{1} + m\Phi(gp^{s-1}) = hp\mathbf{1} + gm\mathbf{1} = f\mathbf{1}$ .  $\square$

**Corollary 2.23.** *If  $x = fp^{s-1}$  and  $y \neq 0 \pmod{p^{s-1}}$ , then  $\Psi(x - y) = \Psi(x) - \Psi(y) + m(p - 1)\mathbf{1}$ . Consequently, for any multiset  $X$  of elements of  $\mathbb{Z}_k$  such that  $x \in X$  only if  $x = fp^{s-1}$ , and for any  $y \neq 0 \pmod{p^{s-1}}$ , then  $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x-y)_i} = 0$ .*

*Proof.* Since  $x = fp^{s-1}$ , by Lemma 2.22 we have  $\Psi(x) = f\mathbf{1}$ . Since  $y = cp^s + dm \neq 0 \pmod{p^{s-1}}$ , by Lemma 2.22 we have  $\sum_{i=1}^{p^{s-1}} \omega^{\Psi(y)_i} = 0$ . Complex conjugation is a field automorphism so it follows too that  $\sum_{i=1}^{p^{s-1}} \omega^{-\Psi(y)_i} = 0$ . It follows from Lemma 2.21 that  $\Psi(x - y) = \Psi(x) - \Psi(y) + m(p - 1)\mathbf{1}$ , and so  $\sum_{i=1}^{p^{s-1}} \omega^{\Psi(x-y)_i} = \omega^{f+m(p-1)} \sum_{i=1}^{p^{s-1}} \omega^{-\Psi(y)_i} = 0$ .  $\square$

We will require the following result of Lam and Leung.

**Lemma 2.24** (Corollary 3.2, [15]). *If  $\alpha_1 + \cdots + \alpha_r = 0$  is a minimal vanishing sum of  $n^{\text{th}}$  roots of unity, then after a suitable rotation, we may assume that all  $\alpha_i$ 's are  $n_0^{\text{th}}$  roots of unity where  $n_0$  is square-free.*

The sum  $\alpha_1 + \dots + \alpha_r = 0$  is *minimal* if no proper subsums can be zero. A rotation in this context is a multiplication of the sum by an  $n^{\text{th}}$  root of unity.

Suppose that for some multiset  $X$  of elements of  $\mathbb{Z}_k$ , we have that  $\sum_x \omega^x = 0$  is minimal, and further assume that each  $\omega^x$  is an  $n_0^{\text{th}}$  root of unity for  $n_0$  square-free. Then for each  $x \in X$ ,  $x = fp^{s-1}$  for some  $f$ . Lemma 2.22 implies that  $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x)_i} = 0$ , and then applying Corollary 2.23, we get that  $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x-y)_i} = 0$  for all  $y \neq 0 \pmod{p^{s-1}}$ . Any vanishing sum with terms that are not  $n_0^{\text{th}}$  roots of unity can only be scaled so that the terms are all  $n_0^{\text{th}}$  roots of unity by some  $\omega^y$  where  $y \neq 0 \pmod{p^{s-1}}$ . Thus we prove the following.

**Lemma 2.25.** *If  $\sum_x \omega^x = 0$  is minimal, then  $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x)_i} = 0$ .*

*Proof.* If the terms  $\omega^x$  are  $n_0^{\text{th}}$  roots of unity then this is immediate from Lemma 2.22. Otherwise, we scale by some  $\omega^y$  such that  $y \neq 0 \pmod{p^{s-1}}$  so that the terms are then  $n_0^{\text{th}}$  roots of unity. Then again we apply Lemma 2.22 and prove the original equality using Corollary 2.23.  $\square$

Finally, we can prove Theorem 2.19.

*Proof.* Observe that the rows of  $H^\Psi$  can be partitioned into  $p^{s-1}$  blocks of size  $n$  corresponding to the images of the rows of  $L(H) + rmJ$  for  $0 \leq r \leq p^{s-1} - 1$ . Given  $H \in \text{BH}(n, k)$ , the Hermitian inner product of two distinct rows is zero. That is, for any two distinct rows  $\mathbf{x} = [x_1, \dots, x_n]$  and  $\mathbf{y} = [y_1, \dots, y_n]$  of  $L(H)$ , the Hermitian inner product of the corresponding rows of  $H$  is of the form

$$\sum_{i=1}^n \omega^{x_i - y_i} = 0.$$

Since we can partition this equation into minimal sums, it follows that  $\sum_{i=1}^n \sum_{j=1}^{p^{s-1}} \omega^{(\Psi(x_i) - \Psi(y_i))_j} = 0$ . That is, distinct rows of  $H^\Psi$  from each block of  $n$  rows are pairwise orthogonal. To see that two rows taken from distinct blocks are orthogonal, we observe that  $tm \neq 0 \pmod{p^{s-1}}$  for any  $1 \leq t \leq p^{s-1} - 1$ , and so we also apply Corollary 2.23.  $\square$

**Remark 2.26.** The application of the map  $\Psi_2$  to  $H \in \text{BH}(n, 4)$  is equivalent to a familiar morphism  $\text{BH}(n, 4) \rightarrow \text{BH}(2n, 2)$  of Turyn [26]. That is, for any  $H \in \text{BH}(n, 4)$ , the Hadamard matrix obtained from Turyn's morphism applied to  $H$  is Hadamard equivalent to  $H^{\Psi_2}$ .

By Proposition 2.18 we know that  $d^\dagger(\mathbf{x}, \mathbf{y}) = d_H(\Psi(\mathbf{x}), \Psi(\mathbf{y}))$ . We may also relate the minimum Hamming distance of  $\Psi(\mathcal{C})$  directly to the minimum Hamming distance of  $\mathcal{C}$ , but less precisely.

**Proposition 2.27.** *Let  $\mathcal{C}$  be a BH-code of minimum Hamming distance  $d$  obtained from a  $\text{BH}(n, p^s m)$  with  $p$  a prime not dividing  $m$ . Then the minimum distance  $d'$  of  $\Psi(\mathcal{C})$  is in the range  $d(p-1)p^{s-2} \leq d' \leq dp^{s-1}$ .*

*Proof.* If  $x_i \neq y_i$ , then  $p^{s-1} - p^{s-2} \leq d_H(\Psi(x_i), \Psi(y_i)) \leq p^{s-1}$ . Hence  $d_H(\mathbf{x}, \mathbf{y})(p-1)p^{s-2} \leq d_H(\Psi(\mathbf{x}), \Psi(\mathbf{y})) \leq d_H(\mathbf{x}, \mathbf{y})p^{s-1}$ .  $\square$

**Remark 2.28.** The upper bound above is attainable. For example, the code  $\mathcal{C}$  obtained from the Fourier matrix of order 27 has minimum distance 18. The code  $\Psi(\mathcal{C})$  is a BH-code of length 243, with minimum distance  $162 = 18(3^2)$ .

### 3 Propelinear codes and cocyclic matrices

The BH-matrix given in Example 2.11,  $H$ , is cocyclic over  $\mathbb{Z}_8$  and its BH-code associated  $C_H$  is not linear. Can we define a propelinear structure in  $C_H$ ? Certainly, we can and this is not an isolated situation.

Let  $G$  and  $U$  be finite groups, with  $U$  abelian, of orders  $n$  and  $k$ , respectively. A map  $\psi : G \times G \rightarrow U$  such that

$$\psi(g, h)\psi(gh, k) = \psi(g, hk)\psi(h, k) \quad \forall g, h, k \in G \quad (3)$$

is a *cocycle* (over  $G$ , with coefficients in  $U$ ). We may assume that  $\psi$  is normalized, i.e.,  $\psi(g, 1) = \psi(1, g) = 1$  for all  $g \in G$ . For any (normalized) map  $\phi : G \rightarrow U$ , the cocycle  $\partial\phi$  defined by  $\partial\phi(g, h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$  is a *coboundary*. The set of all cocycles  $\psi : G \times G \rightarrow U$  forms an abelian group  $Z^2(G, U)$  under pointwise multiplication. Factoring out the subgroup of coboundaries gives  $H^2(G, U)$ , the *second cohomology group of  $G$  with coefficients in  $U$* .

Given a group  $G$  and  $\psi \in Z^2(G, U)$ , denote by  $E_\psi$  the canonical central extension of  $U$  by  $G$ ; this has elements  $\{(u, g) \mid u \in U, g \in G\}$  and multiplication  $(u, g)(v, h) = (uv\psi(g, h), gh)$ . The image  $U \times \{1\}$  of  $U$  lies in the centre of  $E_\psi$  and the set  $T(\psi) = \{(1, g) : g \in G\}$  is a normalized transversal of  $U \times \{1\}$  in  $E_\psi$ . In the other direction, suppose that  $E$  is a finite group with normalized transversal  $T$  for a central subgroup  $U$ . Put  $G = E/U$  and  $\sigma(tU) = t$  for  $t \in T$ . The map  $\psi_T : G \times G \rightarrow U$  defined by  $\psi_T(g, h) = \sigma(g)\sigma(h)\sigma(gh)^{-1}$  is a cocycle; furthermore,  $E_{\psi_T} \cong E$ .

Each cocycle  $\psi \in Z^2(G, U)$  is displayed as a cocyclic matrix  $M_\psi$ : under some indexing of the rows and columns by  $G$ ,  $M_\psi$  has entry  $\psi(g, h)$  in position  $(g, h)$ .

A  $n \times n$  matrix  $A = (a_{g,h})_{g,h \in G}$  is called  *$G$ -invariant* (or just group invariant) if  $a_{gk, hk} = a_{g,h}$  for all  $g, h, k \in G$ .



**Lemma 3.1.** *If  $A$  is  $G$ -invariant and  $a_{g,h} \in U$  then  $\psi(g, h) = a_{g,0}^{-1}a_{g,h^{-1}}a_{0,h^{-1}}^{-1}$  is a cocycle.*

**Remark 3.2.** Every group invariant matrix with entries in  $U$  is equivalent to a cocyclic matrix.

Fixing  $U = \langle \zeta_k \rangle$ . A cocycle  $\psi \in Z^2(G, \langle \zeta_k \rangle)$  is called *orthogonal* if, for each  $g \neq 1 \in G$ ,  $\sum_{h \in G} \psi(g, h) = 0$ .

**Proposition 3.3.** [12]  $H_\psi \in \text{BH}(n, k)$  if and only if  $\psi \in Z^2(G, \langle \zeta_k \rangle)$  is orthogonal.

**Fact:** A cocyclic Butson Hadamard matrix is not necessarily pairwise row and column balanced.

**Proposition 3.4.** *Given  $\psi \in Z^2(G, \langle \zeta_k \rangle)$  and  $\mathbf{x} = \zeta_k^\lambda [\psi(g, g_1), \dots, \psi(g, g_n)]$  for a fixed order in  $G = \{g_1 = 1, g_2, \dots, g_n\}$ . Define  $\pi_{\mathbf{x}} \in \mathcal{S}_n$  so that  $\pi_{\mathbf{x}}^{-1}(j) = k$  where  $g_k = gg_j$ . Then*

1.  $\mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y}) = \zeta_k^{\lambda+\mu} \psi(h, g) [\psi(hg, g_1), \dots, \psi(hg, g_n)]$  where  $+$  means the componentwise product and  $\mathbf{y} = \zeta_k^\mu [\psi(h, g_1), \dots, \psi(h, g_n)]$ .
2.  $\pi_{\mathbf{x}+\pi_{\mathbf{x}}(\mathbf{y})} = \pi_{\mathbf{x}}(\pi_{\mathbf{y}})$ .

*Proof.* 1. Observe that  $\pi_{\mathbf{x}}(\mathbf{y}) = \zeta_k^\mu [\psi(h, gg_1), \dots, \psi(h, gg_n)]$ . Hence the  $i^{\text{th}}$  component of  $\mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$  is  $\zeta_k^{\lambda+\mu} \psi(g, g_i) \psi(h, gg_i)$ . Apply (3) letting  $(g, h, k) = (h, g, g_i)$  and the result follows.

2. Let  $\mathbf{z} = \zeta_k^\gamma [\psi(\ell, g_1), \dots, \psi(\ell, g_n)]$ . From part 1 we know that  $\mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$  is a scalar multiple of the  $n$ -tuple defined by  $\psi(hg, -)$ , and thus the  $j^{\text{th}}$  component of  $\pi_{\mathbf{x}+\pi_{\mathbf{x}}(\mathbf{y})}(\mathbf{z})$  is  $\psi(\ell, hgg_j)$ . Now observe that the  $k^{\text{th}}$  component of  $\pi_{\mathbf{y}}(\mathbf{z})$  is  $\psi(\ell, hg_k)$ . We have  $\pi_{\mathbf{x}}(k) = j$  where  $g_k = gg_j$ , and thus the  $j^{\text{th}}$  component of  $\pi_{\mathbf{x}}(\pi_{\mathbf{y}}(\mathbf{z}))$  is  $\psi(\ell, hg_k) = \psi(\ell, hgg_j)$ .  $\square$

**Corollary 3.5.** *Let  $\psi \in Z^2(G, \langle \zeta_k \rangle)$  and  $H_\psi \in \text{BH}(n, k)$ . Then the corresponding BH-code  $C_H$  is a BHFP-code where  $\mathbf{x} \star \mathbf{y} = \mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$  for all  $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ .*

*Proof.* Extend the definition of  $\pi_{\mathbf{x}}$  for the rows  $\mathbf{x}$  of  $L(H_\psi)$  to all of  $C_H$  by letting  $\pi_{\mathbf{x}+\alpha\mathbf{1}} = \pi_{\mathbf{x}}$  for all  $\alpha \in \mathbb{Z}_k$ . The code  $C_H$  is propelinear by Proposition 3.4, and since  $\mathbf{x} \star \mathbf{y} = \mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$  for all  $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ , the first property of Definition 1.5 is satisfied. Finally observe that because  $\pi_{\mathbf{x}} \in \mathcal{S}_n$  is defined so that  $\pi_{\mathbf{x}}^{-1}(j) = k$  where  $g_k = gg_j$ , it follows that  $\pi_{\mathbf{x}}$  fixes no coordinate when  $\mathbf{x} \neq \alpha\mathbf{1}$ , and  $\pi_{\alpha\mathbf{1}} = \text{Id}_{\mathcal{S}_n}$  for all  $\alpha \in \mathbb{Z}_k$ .  $\square$

**Remark 3.6.** A notorious class of cocyclic Butson matrices are those that are equivalent to group invariant (if  $G$  is a cyclic group, they are called circulant Butson matrices). A construction method based on bilinear forms on finite abelian groups is given in [6] which, in turn, provides BHFP-codes. Furthermore, for  $G$  abelian it is known that Bent functions, group invariant generalized Hadamard matrices and abelian semiregular relative different sets are all either equivalent to group invariant Butson matrices or to group invariant Butson matrices with additional properties (see [25]). Characterising group invariant Butson matrices in terms of BHFP codes is an open problem.

We refer the reader to [1, Section 3] for a detailed discussion on cocyclic generalized Hadamard matrices and the corresponding generalized Hadamard full propelinear codes. Rather than repeat this discussion, we note that the converse of Corollary 3.5 holds under the assumption that the  $\text{BH}(n, k)$  is row and column balanced. A  $\text{BH}(n, p)$  is necessarily balanced, and is equivalent to a generalized Hadamard matrix over the cyclic group  $C_p$  when  $p$  is prime.

**Corollary 3.7.** *Let  $C_H$  be a BHFP-code of length  $n$  over  $\mathbb{Z}_k$  coming from  $H \in \text{BH}(n, k)$ , where  $H$  is row and column balanced. Then  $H$  is cocyclic.*

*Proof.* The proof follows the proof of Proposition 4 and Corollary 2 of [1].  $\square$

Let  $H$  be a  $\text{BH}(n, k)$ . We consider the following partition of its corresponding code.  $C_H = \cup_{1 \leq \alpha \leq n} C_\alpha$  where  $C_\alpha = \{[L(H)]_\alpha + \lambda \mathbf{1}\}_{\lambda \in \mathbb{Z}_k}$  and  $[L(D)]_i$  denotes the  $i$ -th row of  $L(D)$ .

**Example 3.8.** Let  $H$  be the BH-matrix of Example 2.11 since it is cocyclic over  $\mathbb{Z}_8$ . Then,

$$C_H = C_1 \cup C_2 \cup \dots \cup C_8$$

can be endowed with a **full propelinear structure** with the following group  $\Pi$  of permutations

$$\pi_{\mathbf{x}} = \begin{cases} I & \mathbf{x} \in C_1 \\ (1, 2, 3, 4, 5, 6, 7, 8) & \mathbf{x} \in C_2 \\ (1, 3, 5, 7)(2, 4, 6, 8) & \mathbf{x} \in C_3 \\ (1, 4, 7, 2, 5, 8, 3, 6) & \mathbf{x} \in C_4 \\ (1, 5)(2, 6)(3, 7)(4, 8) & \mathbf{x} \in C_5 \\ (1, 6, 3, 8, 5, 2, 7, 4) & \mathbf{x} \in C_6 \\ (1, 7, 5, 3)(2, 8, 6, 4) & \mathbf{x} \in C_7 \\ (1, 8, 7, 6, 5, 4, 3, 2) & \mathbf{x} \in C_8 \end{cases}$$

$C_H$  is a BHFP-code with group structure  $\mathbb{Z}_8 \times \mathbb{Z}_4$  and  $\Pi \cong \mathbb{Z}_8$ . The codewords are

$$\begin{aligned} C_1 &= \{[0, 0, 0, 0, 0, 0, 0, 0] + \lambda \mathbf{1}\}, \\ C_2 &= \{[0, 1, 3, 0, 2, 3, 1, 2] + \lambda \mathbf{1}\}, \\ C_3 &= \{[0, 3, 2, 1, 0, 3, 2, 1] + \lambda \mathbf{1}\}, \\ C_4 &= \{[0, 0, 1, 1, 2, 2, 3, 3] + \lambda \mathbf{1}\}, \\ C_5 &= \{[0, 2, 0, 2, 0, 2, 0, 2] + \lambda \mathbf{1}\}, \\ C_6 &= \{[0, 3, 3, 2, 2, 1, 1, 0] + \lambda \mathbf{1}\}, \\ C_7 &= \{[0, 1, 2, 3, 0, 1, 2, 3] + \lambda \mathbf{1}\}, \\ C_8 &= \{[0, 2, 1, 3, 2, 0, 3, 1] + \lambda \mathbf{1}\} \end{aligned}$$

where  $\lambda$  runs through  $\mathbb{Z}_4$ , and  $C_H$  is a  $(8, 32, 4)$ -code over  $\mathbb{Z}_4$ .  $C_H$  has a group structure  $\mathbb{Z}_8 \times \mathbb{Z}_4 \simeq \langle \mathbf{a}, \mathbf{1} \mid \mathbf{a}^8 = \mathbf{1}^4 = \mathbf{0} \rangle$ , where  $\mathbf{a} = [0, 1, 3, 0, 2, 3, 1, 2]$ .

An interesting family of BH-codes over  $\mathbb{Z}_{p^s}$  are those associated to Kronecker products of Fourier matrices. They are denoted by  $\mathcal{H}^{t_1, t_2, \dots, t_s}$  (see Remark 2.9 and Proposition 2.10) and since these matrices are cocyclic over  $G = \mathbb{Z}_p^{t_s} \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \dots \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \mathbb{Z}_p^{t_1-1}$ , these codes can be endowed with a full propelinear structure by Corollary 3.5. Furthermore, for  $p = 2$  and  $s = 2$  in [20], it is shown that the image of  $\mathcal{H}^{t_1, t_2}$  under the Gray map are in fact propelinear codes.

**Example 3.9.** *Considering  $\mathcal{H}^{1,1,1}$ , the  $\mathbb{Z}_8$ -additive code of length  $n = 8$  associated to  $L(H)$  of Example 2.4. Then, it can be endowed with a **full propelinear structure** with the following group  $\Pi$  of permutations  $\Pi \cong \mathbb{Z}_2 \times \mathbb{Z}_4$  generated by  $\pi_{\mathbf{x}}$  and  $\pi_{\mathbf{y}}$  where*

$$\begin{aligned} \mathbf{x} &= [0, 2, 4, 6, 0, 2, 4, 6], & \mathbf{y} &= [0, 0, 0, 0, 4, 4, 4, 4], \\ \pi_{\mathbf{x}} &= (1, 4, 3, 2)(5, 8, 7, 6), & \pi_{\mathbf{y}} &= (1, 5)(2, 6)(3, 7)(4, 8). \end{aligned}$$

*The full propelinear code is a group  $(\mathcal{H}^{1,1,1}, \star) \cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2 = \langle \mathbf{x}, \mathbf{y}, \mathbf{1} \mid \mathbf{x}^8 = \mathbf{0}, \mathbf{y}^2 = \mathbf{1}^4 = \mathbf{x}^4 \rangle$ .*

## 4 Propelinear codes via the Gray map

A natural question that arises is whether or not the generalized Gray preserves the property of being propelinear, or full propelinear. It is certainly true that the number of codewords in a BH-code  $C$  obtained from  $H$ , a  $\text{BH}(n, mp^s)$ , is the same as the number of codewords in the BH-code  $C'$

obtained from  $H^\Psi$ . However, in general, it is not the case that  $C'$  will be an isomorphic propelinear structure. A simple example to demonstrate this arises from the  $\mathbb{Z}_9$ -code  $C$  obtained from the trivial  $\text{BH}(1,9)$ , and the  $\mathbb{Z}_3$ -code  $\Psi(C)$  obtained from the  $\text{BH}(3,3)$  matrix  $H' = (1)^\Psi$  which written in log form is

$$L(H') = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

The code  $C$  is clearly linear, and as a group is isomorphic to the cyclic group  $\mathbb{Z}_9$ . It is also easily seen to be full propelinear by definition. However it is a short exercise to verify that  $\Psi(C)$  cannot be both full propelinear and isomorphic to a cyclic group  $G \cong \mathbb{Z}_9$  generated by any single element  $\mathbf{x}$ , no matter what the coordinate permutation  $\pi_{\mathbf{x}}$  may be. The code  $\Psi(C)$  does form a 2-dimensional linear code (so it is also propelinear, but not full propelinear with  $\mathbf{x} \star \mathbf{y} = \mathbf{x} + \mathbf{y}$  for all  $\mathbf{x}, \mathbf{y} \in \Psi(C)$ ), and  $\Psi$  is a bijective map between codewords, but in general it is not always the case that  $\Psi(\mathbf{x} \star \mathbf{y}) = \Psi(\mathbf{x}) \star' \Psi(\mathbf{y})$  for any operation  $\star'$ , and as a consequence  $\Psi$  will generally not preserve a group structure. The code  $\Psi(C)$  of this example can also be with a full propelinear structure, but it will not be isomorphic as a group to  $C$ . It is generated by the codewords  $\mathbf{x} = [0, 1, 2]$ , and  $\mathbf{1}$ , where  $\pi_{\mathbf{x}} = (1, 3, 2)$ . It is isomorphic to  $\mathbb{Z}_3^2$ .

However, we find that for the special case  $\Psi_2 : \mathbb{Z}_{4m} \rightarrow \mathbb{Z}_{2m}^2$ , we can carefully construct an isomorphism between the groups of codewords  $C$  and  $C' = \Psi_2(C)$ , and determine the group operation  $\star'$  so that  $(C, \star) \cong (C', \star')$ . Let  $\Psi = \Psi_2$ .

**Theorem 4.1.** *Let  $m$  be an odd positive integer, and let  $C \subseteq \mathbb{Z}_{4m}^n$  be a full propelinear code. Then the code  $C' = \Psi(C)$  is full propelinear with group structure  $(C', \star') \cong (C, \star)$ .*

*Proof.* First observe that  $\Psi$  is a bijection from  $C$  to  $C'$ , so we need to determine the group of permutations for  $C'$  and show that  $\Psi : (C, \star) \rightarrow (C', \star')$  is a homomorphism. We start with the  $n = 1$  case, so we just need to show that we can choose  $\rho_x \in \mathcal{S}_2$  for each  $x \in \mathbb{Z}_{4m}$  so that  $\Psi(x) + \rho_x(\Psi(y)) = \Psi(x + y)$  for all  $y$ . We will see that  $\rho_x = (1, 2)^x$ , i.e.,  $\rho_x$  permutes the two coordinates of a word in  $\mathbb{Z}_{2m}^2$  or not, according to the parity of  $x$ . We adhere to the notation of the proof of Lemma 2.21. Fix  $x = 4a + mb$  and let  $y = 4c + md$  where  $0 \leq b, d \leq 3$ , so  $x + y = 4(a + c) + m(b + d)$  with the value of  $b + d$  taken modulo 4. A complete proof requires a verification that  $\Psi(x) + \rho_x(\Psi(y)) = \Psi(x + y)$  for each pair  $(b, d) \in \mathbb{Z}_4$ , but for brevity we take  $(b, d) = (3, 1)$  as an example

and leave the rest to the reader. Observe that

$$\begin{aligned}\Psi(x) &= [2a, 2a] + m\Phi(3) = [2a, 2a] + m([0, 1] + [1, 1]) = [2a + m, 2a], \\ \Psi(y) &= [2c, 2c] + m\Phi(1) = [2c, 2c] + m([0, 1] + [0, 0]) = [2c, 2c + m], \\ \Psi(x + y) &= [2(a + c), 2(a + c)] + m\Phi(0) = [2(a + c), 2(a + c)].\end{aligned}$$

Since  $b = 3$ ,  $x$  is odd, and so  $\rho_x = (1, 2)$ . It follows that  $\Psi(x) + \rho_x(\Psi(y)) = \Psi(x + y)$ . This verifies the 1-dimensional case.

Now suppose that  $C$  is full propelinear of length  $n$ , and let  $\mathbf{x}, \mathbf{y} \in C$ , with  $\mathbf{x} \star \mathbf{y} = \mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$ . Let  $\pi_{\Phi(\mathbf{x})} \in \mathcal{S}_{2n}$  permute the  $n$  blocks of size 2, labelled  $b_1, \dots, b_n$ , according to the action of  $\pi_{\mathbf{x}}$  on a word of length  $n$ . That is,  $\pi_{\Phi(\mathbf{x})}(b_i) = b_j$  if and only if  $\pi_{\mathbf{x}}(i) = j$ . Then  $\pi_{\Phi(\mathbf{x})}(\Psi(\mathbf{y})) = \Psi(\pi_{\mathbf{x}}(\mathbf{y}))$ . Further, let  $\rho_i = (2i - 1, 2i)$  be the permutation swapping the entries of the block  $b_i$ , and write  $\rho_{\mathbf{x}} = \prod_{i=1}^n \rho_i^{x_i}$ . It follows that  $\Psi(\mathbf{x}) \star' \Psi(\mathbf{y}) := \Psi(\mathbf{x}) + \rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})}(\Psi(\mathbf{y})) = \Psi(\mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})) = \Psi(\mathbf{x} \star \mathbf{y})$ . Thus  $\Psi$  is a bijective homomorphism from  $(C, \star)$  to  $(C', \star')$ .

It remains to verify that the permutation  $\rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})} = Id_{\mathcal{S}_{2n}}$  whenever  $\Psi(\mathbf{x}) = \alpha \mathbf{1}_{2n}$  for any  $\alpha \in \mathbb{Z}_{2m}$ , and has no fixed coordinate otherwise. Let  $S = C \cap \{\alpha \mathbf{1}_n : 0 \leq \alpha \leq 4m - 1\}$  and let  $X \subset S$  be the subset  $X = C \cap \{2\alpha \mathbf{1}_n : 0 \leq \alpha \leq 2m - 1\}$ . Note first that  $\Psi(X)$  is the set  $X' = C' \cap \{\alpha \mathbf{1}_{2n} : 0 \leq \alpha \leq 2m - 1\}$ . It is clear that  $\rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})} = Id_{\mathcal{S}_{2n}}$  for all  $\mathbf{x} \in X$ . Further, for any  $\mathbf{s} \in S \setminus X$ ,  $\rho_{\mathbf{s}} = (1, 2)(3, 4) \cdots (2n - 1, 2n)$ , and so does not fix any coordinate. Finally, for any codeword  $\mathbf{c} \in C \setminus S$ ,  $\pi_{\mathbf{c}}$  does not fix any coordinate of  $\mathbb{Z}_{4m}^n$ , and it follows that  $\pi_{\Phi(\mathbf{c})}$  does not fix any coordinate of  $\mathbb{Z}_{2m}^{2n}$ .  $\square$

**Corollary 4.2.** *Let  $m$  be an odd positive integer, and let  $H \in \text{BH}(n, 4m)$ . If the BH-code  $C$  obtained from  $H$  is full propelinear with group structure  $G$ , then the BH-code  $C'$  obtained from  $H^\Psi$  where  $\Psi$  is full propelinear with group structure  $G' \cong G$ .*

**Example 4.3.** Let  $\mathcal{H}^{3,0}$  be the BH-code associated to  $F_4 \otimes F_4 \in \text{BH}(16, 4)$  and  $H^{3,0}$  be its image by the Gray map which is known to be a nonlinear code (see [9, Table 1]).  $\mathcal{H}^{3,0}$  is full propelinear, with permutation group  $\Pi \cong \mathbb{Z}_4^2$  generated by  $\pi_{\mathbf{x}}$  and  $\pi_{\mathbf{y}}$  where

$$\begin{aligned}\mathbf{x} &= [0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3], \\ \mathbf{y} &= [0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 3], \\ \pi_{\mathbf{x}} &= (1, 4, 3, 2)(5, 8, 7, 6)(9, 12, 11, 10)(13, 16, 15, 14), \\ \pi_{\mathbf{y}} &= (1, 13, 9, 5)(2, 14, 10, 6)(3, 15, 11, 7)(4, 16, 12, 8).\end{aligned}$$

The corresponding permutations  $\rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})}$  and  $\rho_{\mathbf{y}}\pi_{\Phi(\mathbf{y})}$  are as follows:

$$\begin{aligned}\rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})} &= (1, 7, 6, 4)(2, 8, 5, 3)(9, 15, 14, 12)(10, 16, 13, 11) \\ &\quad (17, 23, 22, 20)(18, 24, 21, 19)(25, 31, 30, 28)(26, 32, 29, 27), \\ \rho_{\mathbf{y}}\pi_{\Phi(\mathbf{y})} &= (1, 25, 17, 9)(2, 26, 18, 10)(3, 28, 19, 12)(4, 27, 20, 11) \\ &\quad (5, 29, 21, 13)(6, 30, 22, 14)(7, 32, 23, 16)(8, 31, 24, 15).\end{aligned}$$

Thus,  $H^{3,0}$  can be endowed with a **full propelinear structure** with the group  $\langle \rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})}, \rho_{\mathbf{y}}\pi_{\Phi(\mathbf{y})} \rangle$  of permutations, which is non-abelian of order 32. This group contains the element  $(\rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})})(\rho_{\mathbf{y}}\pi_{\Phi(\mathbf{y})})(\rho_{\mathbf{x}}\pi_{\Phi(\mathbf{x})})^{-1}(\rho_{\mathbf{y}}\pi_{\Phi(\mathbf{y})})^{-1} = \rho_{\mathbf{1}}\pi_{\Phi(\mathbf{1})} = (1, 2)(3, 4) \cdots (31, 32)$ . The groups  $(\mathcal{H}^{3,0}, \star) \cong (H^{3,0}, \star')$  are isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$ .

**Remark 4.4.** Even though the codes  $C$  and  $C'$  are isomorphic as groups according to Theorem 4.1, the example above shows that the underlying groups of coordinate permutations are not necessarily isomorphic. As a simpler example, take the trivial 1-dimensional  $\mathbb{Z}_4$  code and its image in  $\mathbb{Z}_2^2$ . Here,  $\Psi : [0], [1], [2], [3] \mapsto [0, 0], [0, 1], [1, 1], [1, 0]$ . Both are cyclic, generated by  $[1]$  and  $[0, 1]$  respectively, but the group of coordinate permutations of  $\mathbb{Z}_4$  is necessarily trivial, and the group of coordinate permutations of the image is generated by  $\rho_{[1]}\pi_{[0,1]} = (1, 2)$ . More generally, if  $C$  is a BHFP-code obtained from a  $\text{BH}(n, 4m)$  with group  $\Pi$  of coordinate permutations then by Definition 1.5,  $|\Pi| = n$ , and the group of coordinate permutations for  $\Psi(C)$  will be of order  $|\Pi'| = 2n$ .

## Acknowledgements

The authors would also like to thank Kristeen Cheng for her reading of this manuscript. The first author was supported by the project FQM-016 funded by JJAA (Spain). The second author was supported by the Spanish grant TIN2016-77918-P (AEI/FEDER, UE). The third author was supported by the Irish Research Council (Government of Ireland Postdoctoral Fellowship, GOIPD/2018/304).

## References

- [1] Armario, J.A., Bailera, I., Egan R.: Generalized Hadamard full propelinear codes. Des. Codes Cryptogr., to appear.
- [2] Bengtsson, I., Zyczkowski, K.: Geometry of Quantum States: An Introduction to Quantum Entanglement. Cambridge University Press, (2006).

- [3] Borges, J., Mogilnykh, I.Y., Rifà, J. Solov'eva, F.: On the number of nonequivalent propelinear extended perfect codes. *Electronic J. Combinatorics* **20**, 1–14 (2013).
- [4] Carlet, C.:  $\mathbb{Z}_{2^k}$ -linear codes. *IEEE Trans. Inf. Theory* **44**, 1543–1547 (1998).
- [5] Constantinescu, I., Heise, W.: A metric for codes over residue class rings of integers. *Problems Inf. Transmiss.* **33**, 22–28 (1997).
- [6] Duc, T. D., Schmidt, B.: Bilinear Forms on Finite Abelian Groups and Group Invariant Butson Hadamard Matrices. *J. Comb. Theory Ser. A* **166**, 337–351 (2019).
- [7] Egan, R., Flannery, D.L., Ó Catháin, P.: Classifying cocyclic Butson Hadamard matrices. In: Colbourn, C. (Ed.) *Algebraic Design Theory and Hadamard Matrices*, Springer Proc. Math. Stat. **133**, 93–106 (2015).
- [8] Egan, R., Ó Catháin, P.: Morphisms of Butson classes. *Linear Algebra Appl.* **577**, 78–93 (2019).
- [9] Fernández-Córdoba, C., Vela, C., Villanueva, M.: On  $\mathbb{Z}_{2^s}$ -linear Hadamard codes: kernel and partial classification. *Des. Codes and Cryptogr.* **87**, 417–435 (2019).
- [10] Greferath, M., McGuire, G., O’Sullivan, M.: On Plotkin-optimal codes over finite Frobenius rings. *J. Algebra Appl.* **5**, 799–815.
- [11] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The  $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory* **40** (2), 301–319 (1994).
- [12] Horadam, K.J.: *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton, NJ (2007).
- [13] Krotov, D. S.:  $\mathbb{Z}_4$ -linear Hadamard and extended perfect codes. *International workshop on coding and cryptography, ser. Electron. Notes Discret. Math.* **6**, 107–112 (2001).
- [14] Krotov, D. S.: On  $\mathbb{Z}_{2^k}$ -dual binary codes. *IEEE Trans. Inf. Theory* **53**, 1532–1537 (2007).
- [15] Lam, T. Y., Leung, K. H.: On vanishing sums of roots of unity. *J. Algebra* **224**(1), 91–109 (2000).

- [16] Lampio, P., Östergård, P., Szöllösi, F.: Orderly generation of Butson Hadamard matrices. *Math. Comp.* **89**, 313–331 (2020).
- [17] McGuire, G., Ward, H.: Cocyclic Hadamard matrices from forms over finite Frobenius rings. *Linear Algebra Appl.* **430**, 1730–1738 (2009).
- [18] Ó Catháin, P., Swartz, E.: Homomorphisms of matrix algebras and constructions of Butson-Hadamard matrices. *Disc. Math.* **342**(12), 111606 (2019).
- [19] Pinnawala, N., Rao, A.: Cocyclic simplex codes of type  $\alpha$  over  $Z_4$  and  $Z_{2^s}$ . *IEEE Trans. Inf. Theory* **50**, 2165–2169 (2004).
- [20] Pujol, J., Rifà, J.: Translation invariant propelinear codes. *IEEE trans. Inf. Theory* **43**, 590–598 (1997).
- [21] Rao, A., Pinnawala, N.: New linear codes over  $Z_{p^s}$  via the trace map. 2005 IEEE International Symposium on Information Theory (Adelaide, Australia), 4–9 September 2005, pp. 124–126.
- [22] Rifà, J., Basart, J.M., Huguet, L.: On completely regular propelinear codes. In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. LNCS 357, pp. 341–355. Springer, Berlin (1989).
- [23] Rifà, J., Suárez, E.: Hadamard full propelinear codes of type  $Q$ . Rank and kernel. *Des. Codes Cryptogr.* **86**, 1905–1921 (2018).
- [24] Shi, M., Wu, R., Krotov, D. S.: On  $Z_p Z_{p^k}$ -additive codes and their duality. *IEEE trans. Inf. Theory* **65**, 3841–3847 (2019).
- [25] Schmidt, B.: A Survey of Group Invariant Butson Matrices and Their Relation to Generalized Bent Functions and Various Other Objects. *Radon Series on Computational and Applied Mathematics* **23**, 241–251 (2019).
- [26] Turyn, R. J.: Complex Hadamard matrices. In: *Combinatorial Structures and Their Applications*, Proc. Calgary Internat. Conf., Calgary, Alta., 1969, Gordon and Breach, New York, 435–437, (1970).