Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-022-01110-7

Butson full propelinear codes

José Andrés Armario[1] · **Ivan Bailera**[2] · **Ronan Egan**[3]

Received: 2 October 2021 / Revised: 24 May 2022 / Accepted: 29 August 2022

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 kth roots of unity, we can construct a larger Butson matrix over the ℓth roots of unity for any ℓ dividing k, provided that any prime p dividing k also divides ℓ. 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 05B20 · 05E18 · 94B60

1 Introduction

Let n and k be positive integers, and $\zeta_k = \exp(2\pi\sqrt{-1}/k)$ be a complex kth root of unity. We write $\langle\zeta_k\rangle = \{\zeta_k^j\}_{0\le j\le k-1}$. Let $\mathbb{Z}_k$ be the ring of integers modulo k with $k > 1$, and

Communicated by K. T. Arasu.

✉ José Andrés Armario
armario@us.es

Ivan Bailera
bailera@unizar.es

Ronan Egan
ronan.egan@dcu.ie

[1] Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n, 41012 Sevilla, Spain

[2] Departamento de Matemática Aplicada, Universidad de Zaragoza, 50018 Zaragoza, Spain

[3] School of Mathematical Sciences, Dublin City University, Dublin, Ireland

Published online: 17 September 2022

denote by $\mathbb{Z}_k^n$ the set of n-tuples over $\mathbb{Z}_k$. We use bold notation $\mathbf{x} = [x_1, \ldots, x_n] \in \mathbb{Z}_k^n$ 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

Let H be a matrix of order n with complex entries of modulus 1. If the rows of H are pairwise orthogonal under the Hermitian inner product, then H is a *Hadamard matrix*. The term Hadamard matrix is more commonly used in the literature to refer to the special case with entries in $\{\pm 1\}$. In this paper, such a matrix will be call a *real Hadamard matrix*. 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 $\mathrm{BH}(n, k)$ for the set of such matrices. The simplest examples of Butson matrices are the Fourier matrices $F_n = [\zeta_n^{(i-1)(j-1)}]_{i,j=1}^n \in \mathrm{BH}(n, n)$. Real Hadamard matrices of order n, as they are usually defined, are the elements of $\mathrm{BH}(n, 2)$. The phase and orthogonality of a matrix $H \in \mathrm{BH}(n, k)$ is preserved by multiplication on the left or right by an $n \times n$ monomial matrix with non-zero entries in the set of k^{th} roots of unity. The action of pairs (P, Q) of such monomial matrices on $\mathcal{M}_n(\langle \zeta_k \rangle)$ is defined by $H(P, Q) = PHQ^*$, and this action is an equivalence operation. If $H(P, Q) = H'$, then H and H' are said to be *equivalent*. If $H = H'$, then (P, Q) is an automorphism of H.

A Butson matrix $H \in \mathrm{BH}(n, k)$ 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 $L(H) = [\varphi_{i,j} \mod k]_{i,j=1}^n$ with the convention that $L_{i,j} \in \mathbb{Z}_k$ for all $i, j \in \{1, \ldots, n\}$.

Example 1 The following is a matrix $H \in \mathrm{BH}(4, 8)$, displayed 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 2 Let p be a prime number. If $L(D) = [xy^T]_{x,y \in \mathbb{Z}_p^n}$ then $D \in \mathrm{BH}(p^n, p)$. 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 example, for any n, the set $\mathrm{BH}(n, k)$ is non-empty for some k, (the Fourier matrix with $k = n$ for example), but real Hadamard matrices exist when $n > 2$ only if $n \equiv 0 \mod 4$, and this condition is famously not yet known to be sufficient. A Butson morphism [10] is a map $\mathrm{BH}(n, k) \to \mathrm{BH}(m, \ell)$. This motivates the study of Butson matrices even if real Hadamard matrices are the primary interest. In Sect. 3 we construct an explicit morphism $\mathrm{BH}(n, k) \to \mathrm{BH}(nm, k/m)$ 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 [7]. This requires a generalization of the well known Gray map which we define in Sect. 3, and as a consequence certain minimum distance properties of the corresponding codes are controlled. But the applications of Butson matrices in applied sciences most strongly motivate their

study. The rows of any $H \in \mathrm{BH}(n,k)$ 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, i.e., the matrix such that the rows are the basis vectors is Hadamard (but not necessarily Butson). 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. One application is in the construction of propelinear codes, as we discuss in the next section. Another is in the construction of Hermitian self-orthogonal codes over the finite field of order 4, which in turn are used to construct quantum codes, see [4, 5].

1.2 BH-codes and propelinear codes

Interest in studying codes over finite rings increased significantly after it was proved in [13] 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 linear codes over $\mathbb{Z}_4$ under a non-linear map (the Gray map). Codes constructed from Butson matrices [12, 21, 22, 24] 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 $\mathbf{x} \in \mathbb{Z}_k$, denoted by $\mathrm{wt}_H(\mathbf{x})$, 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 $d_H(\mathbf{x},\mathbf{y}) = \mathrm{wt}_H(\mathbf{x}-\mathbf{y})$, 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 $d_L(\mathbf{x},\mathbf{y}) = \mathrm{wt}_L(\mathbf{x}-\mathbf{y})$ where the Lee weight of a vector $\mathbf{z} = [z_1, \ldots, z_n] \in \mathbb{Z}_k^n$ is $\mathrm{wt}_L(\mathbf{z}) = \sum_{i=1}^n \mathrm{wt}_L(z_i)$ with $\mathrm{wt}_L(z_i) = \min\{z_i, k - z_i\}$.

Definition 1 Let $H \in \mathrm{BH}(n,k)$. We denote by F_H the $\mathbb{Z}_k$-code of length n consisting of the rows of $L(H)$, and we denote 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-α vector). The code C_H over $\mathbb{Z}_k$ is called a *Butson Hadamard code* (briefly, BH-code).

Example 3 Given $H \in \mathrm{BH}(4,8)$ of Example 1. Then

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

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

Remark 1 The BH-code associated to $D \in \mathrm{BH}(p^n, p)$, defined in Example 2, is in fact first order p-ary Reed-Muller code, $\mathcal{R}_p(1, n-1)$ (see [20, p. 373]).

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

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

where $\mathrm{Sym}\,\mathbb{Z}_k$ and $\mathcal{S}_n$ denote, respectively, the symmetric group of permutations on $\mathbb{Z}_k$ and on the set $\{1, \ldots, n\}$. The action of (σ, π) 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 $\mathrm{Aut}(\mathbb{Z}_k^n)$ is the composition

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

for all $(\sigma, \pi), (\sigma', \pi') \in \mathrm{Aut}(\mathbb{Z}_k^n)$. Observe that this is a wreath product.

Definition 2 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 $\sigma_{\mathbf{x}} = (\sigma_{\mathbf{x},1}, \ldots, \sigma_{\mathbf{x},n})$ with $\sigma_{\mathbf{x},i} \in \mathrm{Sym}\,\mathbb{Z}_k$ satisfying:

(i) $(\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(C) = C$ and $(\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{0}) = \mathbf{x}$,
(ii) if $\mathbf{y} \in C$ and $\mathbf{z} = (\sigma_{\mathbf{x}}, \pi_{\mathbf{x}})(\mathbf{y})$, 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 [25] for binary codes, and it was generalized in [3] for q-ary codes, i.e., codes over the finite field $\mathbb{F}_q$ where q is a prime power.

For a code $C \subseteq \mathbb{Z}_k^n$, we denote by $\mathrm{Aut}(C)$ 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. The action of $\mathrm{Aut}(C)$ preserves the Hamming metric. A code C over $\mathbb{Z}_k$ is called $t$ransitive if $\mathrm{Aut}(C)$ 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 $i \in \{1, \ldots, n\}$. 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 $i \in \{1, \ldots, n\}$. We call $(C, \star)$ a *propelinear code*. Henceforth we use C instead of $(C, \star)$ if there is no confusion.

Definition 3 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 no fixed coordinate when $\mathbf{a} \neq \alpha\mathbf{1}$ for $\alpha \in \mathbb{Z}_k$. Otherwise, $\pi_{\mathbf{a}} = Id_n$. Here, $\mathbf{a} + \mathbf{x}$ is the ordinary vector addition of $\mathbf{a}$ and $\mathbf{x}$.

Remark 2 Every linear code is propelinear but not necessarily full. The linear code $\{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$ generated by

$$G_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

is propelinear with group structure $\mathbb{Z}_2 \times \mathbb{Z}_2$ but not full propelinear since the unique permutations that move all coordinates have order 3, which do not divide the size of the code. Moreover, the linear code generated by

$$G_r = \left(\begin{array}{c|c|c} 0 \cdots 0 & 1 & 1 \cdots 1 \\ \hline & 0 & \\ G_{r-1} & \vdots & G_{r-1} \\ & 0 & \end{array}\right)$$

is a simplex code (see [15, pp. 30–31]) which is not full propelinear. Indeed, if it will be full propelinear, there would exist a permutation whose order would be a multiple of an odd number, but the size of the code is a power of two.

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 [26] and their equivalence with Hadamard groups was proven. In the q-ary case, the generalized Hadamard full propelinear codes were introduced in [1]. Their existence is shown to be equivalent to the existence of central relative $(n, q, n, n/q)$-difference sets.

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, 13]. 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. While it may seem arbitrary at first, it will be useful for determining the Hamming distance between codewords constructed via the generalized Gray map that we discuss in Sect. 3. Initially, let $k = p^s$ for a prime p. The weight function $\mathrm{wt}^*(x)$ with $x \in \mathbb{Z}_{p^s}$ is defined by

$$\mathrm{wt}^*(x) = \begin{cases} (p-1)p^{s-2} & x \neq cp^{s-1} \mod p^s,\ c \in \{0, \ldots, p-1\} \\ p^{s-1} & x = cp^{s-1} \mod p^s, c \in \{1, \ldots, p-1\} \\ 0 & x = 0 \mod p^s \end{cases}$$

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

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

where $\mathbf{x} = [x_1, \ldots, x_n]$ and $\mathbf{y} = [y_1, \ldots, y_n]$ 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 $x = ap^s + bm \mod k$ where $0 \leq a \leq m-1$ and $0 \leq b \leq p^s - 1$. Define the weight function $\mathrm{wt}^\dagger(x)$ on $\mathbb{Z}_k$ by

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

The corresponding distance $d^\dagger$ on $\mathbb{Z}_{mp^s}^n$ is defined as follows:

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

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

Given $H \in \mathrm{BH}(n, k)$, recall that F_H is the $\mathbb{Z}_k$-code of length n consisting of the rows of $L(H)$, and $C_H = \cup_{\alpha \in \mathbb{Z}_k}(F_H + \alpha \mathbf{1})$. In the sequel, we recall some results concerning distances of these codes.

Lemma 3.1 of [19] establishes a necessary condition for the sum of roots of unity of order $k = p^s$ to vanish. Concretely, if $\sum_{i=0}^{k-1} \alpha_i \zeta_k^i = 0$ with $\sum_{i=0}^{k-1} \alpha_i = n$ where α_i are non-negative integers and $\alpha_i > 0$ for some positive i then

$$\alpha_i \leq \begin{cases} \frac{n}{p} & i = hp^{s-1} \text{ where } h \in \{0, \ldots, p-1\} \\ \frac{n}{p} - 1 & \text{Otherwise.} \end{cases}$$

As a consequence, $n - \frac{n}{p}$ is an upper bound for the minimum Hamming distance of F_H when $k = p^s$ (since if $\mathbf{x}, \mathbf{y} \in L(H)$, then $\sum \zeta_k^{x_i - y_i} = 0$). Furthermore, the minimum Hamming distance of both codes, F_H and C_H, are the same in this case.

In [22, 24], 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 1 and $m = t_1 - 1$ for $t_1 > 0$ and $t_2 = \cdots = t_s = 0$.

Finally, Theorem 5.4 of [12] claims that for any pair (n, k) such that $\mathrm{BH}(n, k) \neq \emptyset$, if $H \in \mathrm{BH}(n, k)$ 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 γ is the average homogeneous weight over $\mathbb{Z}_k$.

2.1 A Fourier type construction and simplex codes

Throughout this section we assume that s is a positive integer, $t_1, t_2, \ldots, t_s$ are non-negative integers with $t_1 \geq 1$ and p is a prime. In what follows, we describe a method to construct Butson matrices of order $n = p^{st_1+(s-1)t_2+(s-2)t_3+\cdots+t_s-s}$ and phase $k = p^s$. The matrix $A^{t_1,t_2,\ldots,t_s}$, where $\mathbf{p^{i-1}}$ denotes the all-p^{i-1} vector, is defined recursively according to the following algorithm, where initially, $(t_1', t_2', \ldots, t_s') = (1, 0, \ldots, 0)$ and $A^{1,0,\ldots,0} = [0]$.

for i=1 until s **do**
  while $t_i' < t_i$ **do**
    $A \leftarrow A^{t_1',\ldots,t_s'}$
    $t_i' \leftarrow t_i' + 1$
    $A^{t_1',\ldots,t_s'} \leftarrow A_i = \begin{bmatrix} A & A & \ldots & A \\ 0 \cdot \mathbf{p^{i-1}} & 1 \cdot \mathbf{p^{i-1}} & \ldots & (p^{s-i+1} - 1) \cdot \mathbf{p^{i-1}} \end{bmatrix}$
  end while
end for

By construction, it is clear that $A^{t_1,t_2,\ldots,t_s}$ is a $(t_1 + t_2 + \ldots + t_s) \times (p^{st_1+(s-1)t_2+\ldots+t_s-s})$ matrix. This is a generalization of the construction of [22] as we will point out in Corollary 1.

Example 4 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 1 *Let* $k = p^s$ *and* $\mathbf{u_i} = [0 \cdot \mathbf{p^{i-1}}, 1 \cdot \mathbf{p^{i-1}}, \ldots, (p^{s-i+1}-1) \cdot \mathbf{p^{i-1}}] \in \mathbb{Z}_{p^s}^{p^{s-i+1}}$ *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 the vectors* $m\mathbf{u_i}$ *and* $\mathbf{u_i}$ *have the same entries but in a different order, in general.*
- *If* $\gcd(m, p^{s-i+1}) = p^h$ *then the vectors* $m\mathbf{u_i}$ *and* $\frac{m}{p^h}\mathbf{u_{i+h}}$ *have the same entries but in a different order, in general.*

Proof The first two points are straightforward. For the third, we have to take into account that the map $f(x) = mx$ is a bijection in $\mathbb{Z}_{p^{s-i+1}}$ and this identity $\left(m \cdot x \mod p^{s-i+1}\right) p^{i-1} \mod p^s = m \cdot x \cdot p^{i-1} \mod p^s$. The fourth is similar. □

Theorem 1 *Let* $n = p^{st_1+(s-1)t_2+\ldots+t_s-s}$ *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* $A^{t_1,t_2,\ldots,t_s}$. *Then,* $H \in \mathrm{BH}(n, p^s)$.

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 $A^{t_1,t_2,\ldots,t_s}$. Hence, it is a row of $L(H)$. It follows that the inner product of two distinct rows of H is a row sum of 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 $A^{t_1,t_2,\ldots,t_s}$, this holds as a consequence of Lemma 1. Finally, the proof for the rows of H corresponding to a linear combination of the rows of $A^{t_1,t_2,\ldots,t_s}$ is by a simple induction. First observe that a linear combination of rows of $A^{1,0,\ldots,0} = [0]$ clearly sums to zero. Now assume that the claim holds for $A = A^{t_1,t_2,\ldots,t_s}$. It follows immediately that any linear combination of the rows of $\begin{bmatrix} A & A & \ldots & A \\ 0 \cdot \mathbf{p^{i-1}} & 1 \cdot \mathbf{p^{i-1}} & \ldots & (p^{s-i+1}-1) \cdot \mathbf{p^{i-1}} \end{bmatrix}$ also sums to zero. □

We provide some examples of Butson matrices coming from Theorem 1.

Example 5 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. For $t_1 = 1,\ t_2 = 1,\ t_3 = 1$ then $H \in \mathrm{BH}(8, 8)$ 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 3 Let $L(H)$ be the matrix of Example 5 for $t_1 = 1,\ t_2 = 1,\ t_3 = 1$. Then $L(H) = L(F_2 \otimes F_4)$ where we have used that $F_2 \otimes F_4 \in \mathrm{BH}(8, 8)$ by means of $\zeta_2 = \zeta_8^4$ and $\zeta_4 = \zeta_8^2$.

In general we have the following.

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

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

where $F_{p^{s-j}}$ denotes the Fourier matrix of order p^{s-j} embedded in $\mathrm{BH}(p^{s-j}, p^s)$ 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 $t_1, t_2, \ldots, t_s = 1, 0, \ldots, 0$ is trivial, so consider the case $t_1 = 2$ and $t_2 = \ldots = t_s = 0$. It is clear that $L(H) = L(F_{p^s})$ since $A^{2,0\ldots,0} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & p^s-1 \end{bmatrix}$. For the next step of the induction, we assume that $t_{i+1} = \ldots = t_s = 0$ and $L(H) = L((F_{p^{s-(i-1)}})^{t_i'} \otimes (F_{p^{s-(i-1)}})^{t_{i-1}} \otimes \ldots \otimes (F_{p^{s-1}})^{t_2} \otimes (F_{p^s})^{t_1-1})$. Now, we have to distinguish two possibilities:

- $t_i' < t_i$; then let $t_i' \leftarrow t_i' + 1$ and $t_{i+1} = \ldots = t_s = 0$. All the possible linear combinations of the rows of $A^{t_1,\ldots,t_{i-1},t_i'+1,0\ldots,0}$ are the rows of $B = L(F_{p^{s-(i-1)}} \otimes H)$.
- $t_i' = t_i$; then take $t_{i+1} = 1$ with $t_{i+2} = \ldots = t_s = 0$. 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 4 For $t_1 \neq 0$, $t_2 = \ldots = t_s = 0$ and $p = 2$, the code generated with the rows of $A^{t_1,0,\ldots,0}$ is a $\mathbb{Z}_{p^s}$-simplex code of type α (see [22, Definition 4.1]). Furthermore, this code is self-orthogonal if $s = 2$.

Corollary 1 *A simplex code of type α over $\mathbb{Z}_{2^s}$ of length 2^{sm}* (see [22]) *and the code whose codewords are the rows of $L((F_{2^s})^m)$ are the same. Therefore the cocyclic matrix $M_\psi \in \mathrm{BH}(2^{sm}, 2^s)$ of* [22, Theorem 5.1, ii)] *is equivalent to $(F_{2^s})^m$. Similarly, when $p > 2$ prime, the analogous classifying result for the cocyclic matrix in $\mathrm{BH}(p^{sm}, p^s)$ of* [24, Proposition 3.1, ii)] *holds.*

Proof Attending to the Remark above, a simplex code of type α 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 1. Applying Proposition 1, the results follows. □

The classifying result above follows also as a consequence of [21, 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 $t_1, \ldots, t_s$ such that $\mathcal{C}$ is isomorphic (as an abelian group) to $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \ldots \times \mathbb{Z}_p^{t_s}$. Thus, $\mathcal{C}$ is said to be of type $(n; t_1, \ldots, t_s)$. Note that $|\mathcal{C}| = p^{st_1} p^{(s-1)t_2} \ldots p^{t_s}$ since there are t_1 (generators) codewords of order p^s, t_2 of order p^{s-1} and so on.

Remark 5 Let $t_1, \ldots, t_s$ be non-negative integers and taking $A^{1,0,\ldots,0} = [1]$ instead of $[0]$, the method described at the beginning of this section provides $A^{t_1,t_2,\ldots,t_s}$ as a generator matrix for a $\mathbb{Z}_{p^s}$-additive code of type $(n; t_1, \ldots, t_s)$ where $n = p^{st_1+(s-1)t_2+\ldots+t_s-s}$. The description of recursive constructions of these matrices are in [11, 16, 17] for $p = 2$. The case $p \neq 2$ has been studied in [27]. We will denote the codes associated to these matrices by $\mathcal{H}^{t_1,\ldots,t_s}$. Let us point out that $\mathcal{H}^{0,t_2,\ldots,t_s} \subset \mathcal{H}^{1,t_2,\ldots,t_s}$.

Now, we establish the following result.

Theorem 2 *For $t_1 > 0$, every $\mathcal{H}^{t_1,\ldots,t_s}$ 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 1. It is clear that C_H is equivalent to $\mathcal{H}^{t_1,\ldots,t_s}$. Now, the result follows from Proposition 1. □

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

Example 6 Let $H \in \mathrm{BH}(8, 4)$ 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 the class of BH-codes encompasses strictly the class of $\mathbb{Z}_{p^s}$-additive BH-codes.

3 A Butson morphism via 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 Φ_p from $\mathbb{Z}_{p^s}$ to $\mathbb{Z}_p^{p^{s-1}}$, and extend this to a yet more general function Ψ_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 $\mathrm{BH}(n, k) \to \mathrm{BH}(nk/\ell, \ell)$. Although our morphism matches the parameters of Ó Catháin and Swartz's morphism in [7], our construction is completly different. One advantage of this construction from our point of view is that we can control the minimum distance of the BH-codes corresponding to the obtained matrices. Where $\mathbf{x} = [x_1, \ldots, x_n] \in \mathbb{Z}_k^n$ and φ is any function with domain $\mathbb{Z}_k$, we will write $\varphi(\mathbf{x}) = [\varphi(x_1), \ldots, \varphi(x_n)]$. 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 element of $\mathrm{BH}(p^{s-1}, p)$ defined in Example 2 and label the rows of $L(D)$ in the order $0, 1, \ldots, p^{s-1} - 1$. Let $[L(D)]_i$ denote the row of $L(D)$ labeled by i. Then we let $\Phi_p : \mathbb{Z}_{p^s} \to \mathbb{Z}_p^{p^{s-1}}$ 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 $p = 2$, Φ_p is the well-known Carlet's map [6] and for $p > 2$, Φ_p is of type φ given in [27]. For what remains of this section we write $\Phi = \Phi_p$ for brevity unless there is some confusion.

Proposition 2 [27] *The entrywise application of Φ 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 $(p^{s-1}n, M, d)$ over $\mathbb{Z}_p$.*

Lemma 2 *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 $\Phi(b_1 - b_2 \mod p^{s-1}) = [L(D)]_{b_1 - b_2} = [L(D)]_{b_1} - [L(D)]_{b_2} = \Phi(b_1) - \Phi(b_2)$. 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. □

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

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

where J denotes the $n \times n$ matrix of all ones. Then H^Φ is the corresponding matrix in $\mathcal{M}_{np^{s-1}}(\langle\zeta_p\rangle)$.

Theorem 3 *If $H \in \mathrm{BH}(n, p^s)$, then $H^\Phi \in \mathrm{BH}(np^{s-1}, p)$.*

Proof Observe that H^Φ 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 $a = 0, \ldots, p - 1$. This is a consequence of $\zeta_k^{ap^{s-1}}$ being a p^{th} root of unity. By Lemma 2, 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 $x - y \not\equiv 0 \mod p^{s-1}$, then $\Phi(x) - \Phi(y) = \Phi(x - y) + \alpha\mathbf{1}$ for some α, 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 $\Phi(x) - \Phi(y)$. □

Corollary 2 *The image of any BH-code over $\mathbb{Z}_{p^s}$ of length n by Φ 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 6 Let us point out that Theorem 1 of [11] is a particular case of Corollary 2 (when the BH-code is of type $\mathcal{H}^{t_1,\ldots,t_s}$ and $p = 2$).

Proposition 3 *Any BH-code C_H of length n over $\mathbb{Z}_{p^s}$ has minimum distance $d^* = np^{s-2}(p - 1)$.*

Proof First note that $\mathrm{BH}(n, p) = \mathrm{GH}(p, n/p)$ where $\mathrm{GH}(p, n/p)$ denotes the set of generalized Hadamard matrices of order n over $\mathbb{F}_p$ (see [9, Lemma 2.2]). Thus, $C_{H^\Phi} = \Phi(C_H)$ is a generalized Hadamard code as well since $H^\Phi \in \mathrm{BH}(p^{s-1}n, p)$. The minimum Hamming distance of these codes is well known to be $np^{s-2}(p-1)$. The fact that Φ is an isometric embedding (Proposition 2) concludes the proof. □

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 $x = ap^s + bm \mod k$ for some $0 \le a \le m-1$ and $0 \le b \le p^s - 1$. Then let

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

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

Proposition 4 *The entrywise application of Ψ_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) over $\mathbb{Z}_{mp^s}$, then the image code $C = \Psi_p(\mathcal{C})$ is a code with parameters $(p^{s-1}n, M, d)$ over $\mathbb{Z}_{mp}$.*

Proof This follows from a straightforward extension of Proposition 2. □

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 Ψ_p to

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

Then H^{Ψ_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 4 *If $H \in \mathrm{BH}(n, k)$ where $k = p^s m$, then $H^{\Psi_p} \in \mathrm{BH}(np^{s-1}, pm)$.*

Repeated application of Ψ_p for all primes p dividing k gives the following.

Corollary 3 *If $H \in \mathrm{BH}(n, k)$ where $k = p_1^{s_1} \cdots p_r^{s_r}$, then $H^\Psi \in \mathrm{BH}(nk/\ell, \ell)$ where $\ell = p_1 \cdots p_r$, and $\Psi = \Psi_{p_1} \cdots \Psi_{p_r}$.*

Before we can prove Theorem 4, we will need to establish some preliminary results. Hereafter we fix a prime p and let $\Psi = \Psi_p$ and $\Phi = \Phi_p$.

Lemma 3 *For all $0 \le x, y < k = mp^s$, $\Psi(x - y) = \Psi(x) - \Psi(y) + m\alpha\mathbf{1}$ 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, $\Phi(b-d) = \Phi(b) - \Phi(d) + \alpha\mathbf{1}$ where $\alpha \in \{0, p-1\}$. The result follows. □

Lemma 4 *Let $z \ne fp^{s-1}$ for any $0 \le f \le mp - 1$. Then $\sum_{i=1}^{p^{s-1}} \omega^{\Psi(z)_i} = 0$ where ω is a primitive k^{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 $f = gm + hp \mod mp$ where $0 \leq g \leq p-1$ and $0 \leq h \leq m-1$. Thus $fp^{s-1} = hp^s + gmp^{s-1} \mod p^s m$. It follows that $\Psi(z) = hp\mathbf{1} + m\Phi(gp^{s-1}) = hp\mathbf{1} + gm\mathbf{1} = f\mathbf{1}$. □

Corollary 4 *If $x = fp^{s-1}$ and $y \neq 0 \mod p^{s-1}$, 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 $y \neq 0 \mod p^{s-1}$, then $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x-y)_i} = 0$.*

Proof Since $x = fp^{s-1}$, by Lemma 4 we have $\Psi(x) = f\mathbf{1}$. Since $y = cp^s + dm \neq 0 \mod p^{s-1}$, by Lemma 4 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 3 that $\Psi(x-y) = \Psi(x) - \Psi(y) + m(p-1)\mathbf{1}$, and so $\sum_{i=1}^{p^{s-1}} \omega^{\Psi(x-y)_i} = \omega^{f+m(p-1)} \sum_{i=1}^{p^{s-1}} \omega^{-\Psi(y)_i} = 0$. □

We will require the following result of Lam and Leung.

Lemma 5 (Corollary 3.2, [18]) *If $\alpha_1 + \cdots + \alpha_r = 0$ is a minimal vanishing sum of n^{th} roots of unity, then after a suitable rotation, we may assume that all α_i's are n_0^{th} roots of unity where n_0 is square-free.*

The sum $\alpha_1 + \cdots + \alpha_r = 0$ is *minimal* if no proper subsums can be zero. A rotation in this context is a multiplication of the sum by an n^{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 ω^x is an n_0^{th} root of unity for n_0 square-free. Then for each $x \in X$, $x = fp^{s-1}$ for some f. Lemma 4 implies that $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x)_i} = 0$, and then applying Corollary 4, we get that $\sum_x \sum_{i=1}^{p^{s-1}} \omega^{\Psi(x-y)_i} = 0$ for all $y \neq 0 \mod p^{s-1}$. Any vanishing sum with terms that are not n_0^{th} roots of unity can only be scaled so that the terms are all n_0^{th} roots of unity by some ω^y where $y \neq 0 \mod p^{s-1}$. Thus we prove the following.

Lemma 6 *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 ω^x are n_0^{th} roots of unity then this is immediate from Lemma 4. Otherwise, we scale by some ω^y such that $y \neq 0 \mod p^{s-1}$ so that the terms are then n_0^{th} roots of unity. Then again we apply Lemma 4 and prove the original equality using Corollary 4. □

Finally, we can prove Theorem 4.

Proof Observe that the rows of H^{Ψ} 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 $\mathbf{x} = [x_1, \ldots, x_n]$ and $\mathbf{y} = [y_1, \ldots, y_n]$ of $L(H)$, the Hermitian inner product of the corresponding rows of H is of the form

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

We can partition this equation into minimal sums. This partition might not be unique, but any such partition allows us to invoke Lemma 6. 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^Ψ from each block of n rows are pairwise orthogonal. To see that two rows taken from distinct blocks are orthogonal, we observe that $tm \neq 0 \mod p^{s-1}$ for any $1 \leq t \leq p^{s-1} - 1$, and so we also apply Corollary 4.

That is, distinct rows of H^Ψ from each block of n rows are pairwise orthogonal. To see that two rows taken from distinct blocks are orthogonal, we observe that $tm \neq 0 \mod p^{s-1}$ for any $1 \leq t \leq p^{s-1} - 1$, and so we also apply Corollary 4. □

Remark 7 The application of the map Ψ_2 to $H \in \mathrm{BH}(n, 4)$ is equivalent to a familiar morphism $\mathrm{BH}(n, 4) \to \mathrm{BH}(2n, 2)$ of Turyn [29]. That is, for any $H \in \mathrm{BH}(n, 4)$, the Hadamard matrix obtained from Turyn's morphism applied to H is Hadamard equivalent to H^{Ψ_2}.

By Proposition 4 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 5 *Let $H \in \mathrm{BH}(n, p^s m)$ with p a prime not dividing m. Let d be the minimum Hamming distance of C_H. Then the minimum distance d' of $\Psi(C_H)$ 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 $d_H(\mathbf{x}, \mathbf{y})(p-1)p^{s-2} \leq d_H(\Psi(\mathbf{x}), \Psi(\mathbf{y})) \leq d_H(\mathbf{x}, \mathbf{y})p^{s-1}$. □

Remark 8 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 $162 = 18(3^2)$.

4 Propelinear codes and cocyclic matrices

The Butson matrix given in Example 6, 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 $\psi : G \times G \to U$ such that

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

is a *cocycle* (*over G, with coefficients in U*). We may assume that ψ is normalized, i.e., $\psi(g, 1) = \psi(1, g) = 1$ for all $g \in G$. The set of all cocycles $\psi : G \times G \to U$ forms an abelian group $Z^2(G, U)$ under pointwise multiplication.

Each cocycle $\psi \in Z^2(G, U)$ is displayed as a cocyclic matrix M_ψ: under some indexing of the rows and columns by G, M_ψ has entry $\psi(g, h)$ in position (g, h). For a comprehensive background on cocyclic matrices, we refer the reader to [14].

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 $g, h, k \in G$.

Remark 9 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 6 [14] *$H_\psi \in \mathrm{BH}(n, k)$ 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 7 *Given $\psi \in Z^2(G, \langle\zeta_k\rangle)$ and $\mathbf{x} = \zeta_k^{\lambda}[\psi(g, g_1), \ldots, \psi(g, g_n)]$ for a fixed order in $G = \{g_1 = 1, g_2, \ldots, g_n\}$. Define $\pi_{\mathbf{x}} \in \mathcal{S}_n$ so that $\pi_{\mathbf{x}}^{-1}(j) = k$ where $g_k = gg_j$. Then*

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

Proof 1. Observe that $\pi_{\mathbf{x}}(\mathbf{y}) = \zeta_k^{\mu}[\psi(h, gg_1), \ldots, \psi(h, gg_n)]$. Hence the i^{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 $\mathbf{z} = \zeta_k^{\gamma}[\psi(\ell, g_1), \ldots, \psi(\ell, g_n)]$. 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^{th} component of $\pi_{\mathbf{x}+\pi_{\mathbf{x}}(\mathbf{y})}(\mathbf{z})$ is $\psi(\ell, hgg_j)$. Now observe that the k^{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^{th} component of $\pi_{\mathbf{x}}(\pi_{\mathbf{y}}(\mathbf{z}))$ is $\psi(\ell, hg_k) = \psi(\ell, hgg_j)$. □

Corollary 5 *Let $\psi \in Z^2(G, \langle\zeta_k\rangle)$ and $H_\psi \in \mathrm{BH}(n, k)$. Then the corresponding BH-code C_{H_ψ} is a BHFP-code where $\mathbf{x}\star\mathbf{y} = \mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in C_{H_\psi}$.*

Proof Extend the definition of $\pi_{\mathbf{x}}$ for the rows $\mathbf{x}$ of $L(H_\psi)$ to all of C_{H_ψ} by letting $\pi_{\mathbf{x}+\alpha\mathbf{1}} = \pi_{\mathbf{x}}$ for all $\alpha \in \mathbb{Z}_k$. The code C_{H_ψ} is propelinear by Proposition 7, and since $\mathbf{x}\star\mathbf{y} = \mathbf{x} + \pi_{\mathbf{x}}(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in C_{H_\psi}$, the first property of Definition 3 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 $\pi_{\alpha\mathbf{1}} = Id_{\mathcal{S}_n}$ for all $\alpha \in \mathbb{Z}_k$. □

Remark 10 A notorious class of cocyclic Butson matrices are those that are equivalent to group invariant matrices (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 [8] 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 [28]). 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 5 holds under the assumption that any matrix in $\mathrm{BH}(n, k)$ is row and column balanced. A matrix $H \in \mathrm{BH}(n, p)$ is necessarily balanced, and is equivalent to a generalized Hadamard matrix over the cyclic group C_p when p is prime.

Corollary 6 *Let C_H be a BHFP-code of length n over $\mathbb{Z}_k$ coming from $H \in \mathrm{BH}(n, k)$, 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]. □

Let $H \in \mathrm{BH}(n, k)$. 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 $[L(H)]_i$ denotes the i-th row of $L(H)$.

Example 7 Let H be the Butson matrix of Example 6 since it is cocyclic over $\mathbb{Z}_8$. Then,

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

can be endowed with a **full propelinear structure** with the following group Π 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 λ 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 $\mathcal{H}^{t_1,t_2,\ldots,t_s}$ (see Remark 5 and Theorem 2) and since these matrices are cocyclic over $G = \mathbb{Z}_p^{t_s} \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \ldots \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \mathbb{Z}_{p^s}^{t_1-1}$, these codes can be endowed with a full propelinear structure by Corollary 5 . Furthermore, for $p = 2$ and $s = 2$ in [23], it is shown that the image of $\mathcal{H}^{t_1,t_2}$ under the Gray map are in fact propelinear codes.

Example 8 Considering $\mathcal{H}^{1,1,1}$, the $\mathbb{Z}_8$-additive code of length $n = 8$ associated to $L(H)$ of Example 5. Then, it can be endowed with a **full propelinear structure** with the following group Π of permutations $\Pi \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ generated by $\pi_{\mathbf{x}}$ and $\pi_{\mathbf{y}}$ where

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

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

5 Propelinear codes via the Gray map

A natural question that arises is whether or not the generalized Gray map 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 $H \in \mathrm{BH}(n, mp^s)$, is the same as the number of codewords in the BH-code C' obtained from H^{Ψ}. 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 matrix $(1) \in \mathrm{BH}(1, 9)$, and the $\mathbb{Z}_3$-code $\Psi(C)$ obtained from the 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 Ψ 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 Ψ 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 $\Psi_2 : \mathbb{Z}_{4m} \to \mathbb{Z}_{2m}^2$, 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 $\Psi = \Psi_2$ hereafter.

Theorem 5 *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 Ψ is a bijection from C to C', so we need to determine the group of permutations for C' and show that $\Psi : (C, \star) \to (C', \star')$ 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., ρ_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 3. Fix $x = 4a + mb$ and let $y = 4c + md$ where $0 \le b, d \le 3$, 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 $b_1, \ldots, b_n$, 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 Ψ 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 $\mathbb{Z}_{2m}^{2n}$. □

Corollary 7 *Let m be an odd positive integer, and let $H \in \mathrm{BH}(n, 4m)$. If the BH-code C obtained from H is full propelinear with group structure G, then the BH-code C' obtained from H^{Ψ} is full propelinear with group structure $G' \cong G$.*

Example 9 Let $\mathcal{H}^{3,0}$ be the BH-code associated to $F_4 \otimes F_4 \in \mathrm{BH}(16, 4)$ and $H^{3,0}$ be its image by the Gray map which is known to be a non-linear code (see [11, 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:

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

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 $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$. Note that the linear binary Hadamard code of size 64 has 6 generators, but we can generate a nonlinear binary Hadamard code with the same minimum distance just from 3 generators. This improves the data storage benefits of a linear code.

Remark 11 Even though the codes C and C' are isomorphic as groups according to Theorem 5, 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 matrix $H \in \mathrm{BH}(n, 4m)$ with group Π of coordinate permutations then by Definition 3, $|\Pi| = n$, 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 PID2019-104664GB-I00 (AEI/FEDER, UE). The third author was supported by the Irish Research Council (Government of Ireland Postdoctoral Fellowship, GOIPD/2018/304) during the early stages of this project.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

1. Armario J.A., Bailera I., Egan R.: Generalized Hadamard full propelinear codes. Des. Codes Cryptogr. **89**(4), 599–615 (2021).
2. Bengtsson I., Zyczkowski K.: Geometry of Quantum States: An Introduction to Quantum Entanglement. Cambridge University Press, Cambridge (2006).
3. Borges J., Mogilnykh I.Y., Rifà J., Solov'eva F.: On the number of nonequivalent propelinear extended perfect codes. Electron. J. Comb. **20**(2), 1–14 (2013).
4. Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.: Quantum error correction via codes over $GF(4)$. IEEE Trans. Inform. Theory **44**(4), 1369–1387 (1998).
5. Crnković D., Egan R., Švob A.: Constructing self-orthogonal and Hermitian self-orthogonal codes via weighing matrices and orbit matrices. Finite Fields Appl. **55**, 64–77 (2019).
6. Carlet C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inf. Theory **44**(4), 1543–1547 (1998).
7. Catháin P.Ó., Swartz E.: Homomorphisms of matrix algebras and constructions of Butson-Hadamard matrices. Discret. Math. **342**(12), 111606 (2019).
8. 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).
9. Egan R., Flannery D.L., Catháin P.: Classifying cocyclic Butson Hadamard matrices algebraic design theory and hadamard matrices. Proc. Math. Stat. **133**, 93–106 (2015).
10. Egan R., Catháin P.Ó.: Morphisms of Butson classes. Linear Algebra Appl. **577**, 78–93 (2019).
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. Greferath M., McGuire G., O'Sullivan M.: On Plotkin-optimal codes over finite Frobenius rings. J. Algebra Appl. **5**, 799–815 (2006).
13. 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).
14. Horadam K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007).
15. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
16. Krotov D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. International workshop on coding and cryptography. Electron. Notes Discret. Math. **6**, 107–112 (2001).
17. Krotov D.S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Trans. Inf. Theory **53**(4), 1532–1537 (2007).
18. Lam T.Y., Leung K.H.: On vanishing sums of roots of unity. J. Algebra **224**(1), 91–109 (2000).
19. Lampio P., Östergård P., Szöllósi F.: Orderly generation of Butson Hadamard matrices. Math. Comp. **89**(321), 313–331 (2020).
20. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. Elsevier, Amsterdam (1977).
21. McGuire G., Ward H.: Cocyclic Hadamard matrices from forms over finite Frobenius rings. Linear Algebra Appl. **430**(7), 1730–1738 (2009).
22. Pinnawala N., Rao A.: Cocyclic simplex codes of type α over Z_4 and $\mathbb{Z}_{2^s}$. IEEE Trans. Inf. Theory **50**(9), 2165–2169 (2004).
23. Pujol J., Rifà J.: Translation invariant propelinear codes. IEEE Trans. Inf. Theory **43**(2), 590–598 (1997).

24. Rao A., Pinnawala N.: New linear codes over $\mathbb{Z}_{p^s}$ via the trace map. In: Proceedings of the 2005 IEEE International Symposium on Information Theory, Adelaide, Australia, pp. 124–126. 4–9 Sept (2005)
25. Rifà J., Basart J.M., Huguet L.: On completely regular propelinear codes. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 341–355. LNCS 357. Springer, Berlin (1989)
26. Rifà J., Suárez E.: Hadamard full propelinear codes of type Q: rank and kernel. Des. Codes Cryptogr. **86**(9), 1905–1921 (2018).
27. 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).
28. Schmidt B.: A survey of group invariant Butson matrices and their relation to generalized bent functions and various other objects. Radon Ser. Comput. Appl. Math. **23**, 241–251 (2019).
29. Turyn R.J.: Complex Hadamard matrices. In: Proceedings of the Calgary International Conference on Combinatorial Structures and Their Applications, Calgary, Alta., 1969, Gordon and Breach, New York. pp. 435–437 (1970)