Generalized Hadamard full propelinear codes

José Andrés Armario1 · Ivan Bailera2 · Ronan Egan3

Received: 14 June 2019 / Revised: 25 November 2020 / Accepted: 27 November 2020 / Published online: 19 January 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC part of Springer Nature 2021

Abstract

Codes from generalized Hadamard matrices have already been introduced. Here we deal with these codes when the generalized Hadamard matrices are cocyclic. As a consequence, a new class of codes that we call generalized Hadamard full propelinear codes turns out. We prove that their existence is equivalent to the existence of central relative $(v, w, v, v/w)$-difference sets. Moreover, some structural properties of these codes are studied and examples are provided. Some of the propelinear codes constructed for the examples perform better than any comparable linear code.

Keywords
Cocycles · Generalized Hadamard matrices · Difference sets · Propelinear codes · Rank · Kernel

Mathematics Subject Classification 05B20 · 05E18 · 94B60

1 Introduction

Robust or secure communications are often based on codes built from Hadamard matrices or from relative difference sets. When it is necessary to have an alphabet larger than the binary field, then generalized Hadamard matrices are used. The concept of binary Hadamard matrices was generalized by Butson [5] and Drake [10] independently. Butson Hadamard matrices...
have entries in the complex $m$th roots of unity such that rows are pairwise orthogonal under the Hermitian inner product, but they are not necessarily pairwise row and column balanced. The generalized Hadamard matrices introduced by Drake have entries in a finite group. The main characteristics that they have in common with the binary Hadamard matrices are that rows are pairwise balanced, and they exhibit a kind of orthogonality over the group ring, but they are not necessarily invertible. Throughout this paper, generalized Hadamard matrices are the matrices presented by Drake. The codes built from generalized Hadamard matrices meet the Plotkin bound, i.e., when the length and minimum distance are fixed, the generalized Hadamard codes have the maximum number of codewords. As such, some of these codes have more codewords than is possible for any linear code attaining the same minimum distance, and the examples in Sect. 4 reflect this.

Binary propelinear codes were introduced by Rifà et al. in [21]. They have been deeply studied in the literature, see [1,2,19] among other references. These codes have a group structure that allows them to be studied from an algebraic point of view. As a propelinear code is also a group, it is possible to define a kind of generator matrix even if the code is non-linear. The rows of the generator matrix are the codewords that are associated with the generators of the group. Thus, the code can be built from a few codewords using the propelinear operation associated to the propelinear code. This offers the data storage benefits of a linear code, i.e., we store just a set of generators and the group operation, but the code need not be linear as several of our examples indicate. In this paper we focus on Hadamard full propelinear codes which have a very rich algebraic structure. The Hadamard full propelinear codes are a subclass of propelinear codes which are equivalent to Hadamard groups [20]. The equivalences between Hadamard groups, relative difference sets and cocyclic Hadamard matrices has been proved in [8,13,17]. Cocyclic generalized Hadamard matrices have been studied by Horadam [14] and Horadam and Perera [18]. However, aside from [3] not much has been done for $q$-ary propelinear codes, especially for the class of full propelinear codes. To build generalized Hadamard full propelinear codes we will endow generalized Hadamard matrices with a full propelinear structure. We take the theory of cocycles as starting point.

Let $G$ and $U$ be finite groups, with $U$ abelian, of orders $v$ and $w$, respectively. A map $\psi : G \times G \to U$ such that

$$\psi(g, h)\psi(gh, k) = \psi(g, hk)\psi(h, k) \ \forall g, h, k \in G \quad (1)$$

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 $\phi : G \to U$, the cocycle $\partial \phi$ defined by $\partial \phi(g, h) = \phi(g)\phi(h^{-1})\phi(gh)$ is a coboundary. The set of all cocycles $\psi : G \times G \to U$ 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 $\psi_T : G \times G \to U$ 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 cocycle $\psi \in Z^2(G, U)$ is called orthogonal if, for each $g \neq 1 \in G$ and each $u \in U$, $\{|h \in G : \psi(g, h) = u\| = v/w$. This definition arose as an equivalent formulation of the
condition that the $G$-cocyclic matrix $M_\psi$ be a generalized Hadamard matrix $GH(w, v/w)$ over $U$. We recall that a $v \times v$ matrix $H$ with entries in $U$, where $w$ divides $v$, is a generalized Hadamard matrix $GH(w, v/w)$ if, for every $i, j$, $1 \leq i < j \leq v$, each of the multisets $\{h_{ik}^{-1}h_{jk}^{-1} \mid 1 \leq k \leq v\}$ contains every element of $U$ exactly $v/w$ times. A $GH(w, v/w)$ is normalized if the first row and first column consist entirely of the identity element of $U$. We can always assume that our GH matrices are normalized.

Let $E$ be a group of order $wv$ with a normal subgroup $Z$ of order $w$. Suppose that $R$ is a $k$-subset of $E$, such that the multiset of quotients $r_1r_2^{-1}$, $r_i \in R$, $r_1 \neq r_2$, contains each element of $E \setminus Z$ exactly $\lambda$ times, and contains no element of $Z$. Then $R$ is called a $(v, m, k, \lambda)$-relative difference set in $E$ with forbidden subgroup $Z$. If $Z$ is a central subgroup of $E$ then we call $R$ a central relative difference set.

For certain parameters, the existence of relative difference sets is equivalent to the existence of Hadamard matrices. The following result addresses this situation.

**Theorem 1** [18, Theorem 4.1] The following statements are equivalent.

1. $\psi \in Z^2(G, U)$ is orthogonal.
2. $M_\psi$ is a (normalized) $GH(w, v/w)$.
3. There is a (central) relative $(v, w, v, v/w)$-difference set $T(\psi) = \{(1, g) : g \in G\}$ in the central extension $E_\psi$ of $U$ by $G$, relative to $U \times \{1\}$.

**Example 1** [15, Example 9.2.1.4 and Theorem 9.48] Let $G$ be the additive group of the finite field $\mathbb{F}_{3^a}$ and $\phi_{(a,b)}(g) = g^{(3^a+1)/2}$, $g \in G$ where $(a, b) = 1$, $b$ is odd and $1 < b < 2a - 1$. Then

$$\partial \phi_{(a,b)}(g, h) = \phi_{(a,b)}(g + h) - \phi_{(a,b)}(g) - \phi_{(a,b)}(h)$$

is an orthogonal coboundary. Hence, $M_{\partial \phi_{(a,b)}}$ is a $GH(3^a, 1)$. Later, we will deal with $a = 4$ and $b = 3$.

**Remark 1**

1. Coulter and Mathews found $\phi_{(a,b)}$ as a new class of planar power functions over $\mathbb{F}_{3^a}$ (see [6]).
2. The symmetric orthogonal coboundaries $\partial \phi_{(a,b)}$ cannot be multiplicative. In particular, the resulting ternary Hadamard codes are not linear $3^a$-ary codes (see [15, p. 227]).
3. The orthogonal coboundaries $\partial \phi_{(a,b)}$ and $\partial \phi_{(a,2a-b)}$ determine equivalent Hadamard codes (see [16, Lemma 4.1]). Hence we may restrict to the range $3 \leq b \leq a - 1$.

Let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, where $p$ is prime. In particular, $\mathbb{F}_q$ is an additive elementary abelian group $G$ of order $q$. Let $H$ be a normalized generalized Hadamard matrix $GH(q, v/q)$ over $\mathbb{F}_q$. We denote by $F_H$ the $q$-ary code consisting of the rows of $H$, and by $C_H$ the one defined as $C_H = \cup_{a \in \mathbb{F}_q}(F_H + a \mathbf{1})$ where $\mathbf{1}$ denotes the all-one vector (and $a \mathbf{1}$ the all-$a$ vector). The code $C_H$ over $\mathbb{F}_q$ is called a generalized Hadamard code (briefly, GH-code) which has length $v$, $qv$ codewords and minimum distance $v - \frac{q}{v}$ (i.e., they are $(v, qv, v - \frac{v}{q})_q$-codes). Hence, generalized Hadamard codes meet the Plotkin bound [15].

Note that $F_H$ and $C_H$ are generally nonlinear codes over $\mathbb{F}_q$.

An ordinary Hadamard matrix of order $v = 4t$ corresponds to a $GH(2, 2t)$, where $U = \langle -1 \rangle$. In this case two further equivalences are known.

**Proposition 1** When $U = \langle -1 \rangle \cong \mathbb{Z}_2$, the equivalent statements of Theorem 1 are further equivalent to the following statements.

4. There is a Hadamard group $E_\psi$ [13].
5. $C_H$ is a Hadamard full propelinear code [20].

In this paper, we prove the analog of Proposition 1 when $U$ is the additive group of a finite field (i.e. additive elementary abelian group). As a consequence, the class of generalized Hadamard full propelinear codes is introduced. Concerning equivalence 4., let us mention that the Hadamard group $E_\psi$ in the binary case is effectively what is referred to as the extension group of a cocyclic Hadamard matrix, which is also defined for generalized Hadamard matrices with entries in $U$. Therefore, if the existence of a generalized Hadamard full propelinear code is equivalent to the existence of an orthogonal cocycle $\psi$, then there is an extension group $E_\psi$. Finally, let us point out that it seems that a generalized Hadamard matrix over any abelian group $U$ (should it exist) would afford the same theory, assuming similar definitions of propelinear codes over groups and so forth.

2 Propelinear codes

Let $\mathbb{F}_q^n$ be the vector space of dimension $n$ over $\mathbb{F}_q$. The Hamming distance between two vectors $v$, $w \in \mathbb{F}_q^n$, denoted by $d(v, w)$, is the number of the coordinates in which $v$ and $w$ differ. A $(q$-ary) code $C$ over $\mathbb{F}_q$ of length $n$ is a nonempty subset of $\mathbb{F}_q^n$. A code $C$ over $\mathbb{F}_q$ is called linear if and only if its rank and the dimension of the kernel, they are nonisomorphic. A code is linear if and only if its rank and the dimension of the kernel. Two structural parameters of (nonlinear) codes are the rank and dimension of the kernel. The rank of a code $C$, $r = \text{rank}(C)$, is the dimension of the linear span of $C$. The kernel of a $q$-ary code, denoted by $K(C)$, is defined as $K(C) := \{x \in \mathbb{F}_q^n : C + \alpha x = C \text{ for all } \alpha \in \mathbb{F}_q\}$. The $p$-kernel of $C$ is defined as $K_p(C) = \{x \in \mathbb{F}_q^n : C + x = C\}$. Note that $K(C)$ is a linear subspace and $K_p(C)$ is $\mathbb{F}_p$-additive. We will denote the dimension of the kernel of $C$ by $k = \text{ker}(C)$. These two parameters do not always give a full classification of codes, since two nonisomorphic codes could have the same rank and dimension of the kernel. In spite of that, they can help in classification, since if two codes have different rank or dimension of the kernel, they are nonisomorphic. A code is linear if and only if its rank and the dimension of its kernel are equal to the dimension of the code. In some sense, these two parameters give information about the linearity of a code.

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

$$\text{Aut}(\mathbb{F}_q^n) = \{(\sigma, \pi) : \sigma = (\sigma_1, \ldots, \sigma_n) \text{ with } \sigma_i \in \text{Sym} \mathbb{F}_q, \pi \in S_n\}$$

where Sym $\mathbb{F}_q$ and $S_n$ denote, respectively, the symmetric group of permutations on $\mathbb{F}_q$ and on the set $\{1, \ldots, n\}$. For any $\sigma = (\sigma_1, \ldots, \sigma_n)$ where $\sigma_i \in \text{Sym} \mathbb{F}_q$, $\pi \in S_n$ and $v \in \mathbb{F}_q^n$, $v = (v_1, \ldots, v_n)$, we write $\sigma(v)$ and $\pi(v)$ to denote $(\sigma_1(v_1), \ldots, \sigma_n(v_n))$ and $(v_{\pi^{-1}(1)}, \ldots, v_{\pi^{-1}(n)})$, respectively. The action of $(\sigma, \pi)$ is defined as

$$(\sigma, \pi)(v) = \sigma(\pi(v)) \text{ for any } v \in \mathbb{F}_q^n,$$

and the group operation in Aut$(\mathbb{F}_q^n)$ is the composition

$$(\sigma, \pi) \circ (\sigma', \pi') = ((\sigma_1 \circ \sigma'_{\pi^{-1}(1)}), \ldots, \sigma_n \circ \sigma'_{\pi^{-1}(n)}), \pi \circ \pi') \text{ for all } (\sigma, \pi), (\sigma', \pi') \in \text{Aut}(\mathbb{F}_q^n).$$
Here and throughout the entire paper, we use the convention \( f \circ g(v) = f(g(v)) \), for \( v \in \mathbb{F}_q^n \).

We denote by \( \text{Aut}(C) \) the group of all isometries of \( \mathbb{F}_q^n \) fixing the code \( C \) and we call it the automorphism group of the code \( C \).

At this point, we introduce some basic background on automorphism groups of a matrix. Let \( K \) be a multiplicative group isomorphic to the additive elementary abelian group \( \mathbb{F}_q \), and let \( \phi : \mathbb{F}_q \rightarrow K \) be an isomorphism. An automorphism of a matrix \( M \) with entries in the group \( K \) is a pair of monomial matrices \( (P, Q) \) with non-zero entries in \( K \) such that \( PMQ^* = M \), where \( Q^* \) denotes the matrix obtained from the transpose of \( Q \) by replacing each non-zero entry with its inverse in \( K \), and matrix multiplication is carried out over the group ring \( \mathbb{Z}[K] \). The automorphism group \( \text{Aut}(M) \) of \( M \) is the set of all such pairs of matrices, closed under the multiplication \( (P, Q)(R, S) = (PR, QS) \). The permutation automorphism group of \( M \) is the subgroup \( \text{PAut}(M) \subset \text{Aut}(M) \) comprised of all pairs of permutation matrices in \( \text{Aut}(M) \).

**Lemma 1** [7] Let \( M \) be a \( K \)-monomial matrix of order \( n \). Then \( M \) has a unique factorization \( D_M P_M \) where \( D_M \) is a diagonal matrix and \( P_M \) is a permutation matrix.

Here we will focus on GH-codes, \( C_H \), where \( H \) denotes a generalized Hadamard matrix of order \( v \) with entries in the additive elementary abelian group \( \mathbb{F}_q \) and write \( \phi(H) = [\phi(h_{ij})]_{1 \leq i, j \leq v} \).

In what follows, we will make explicit the correspondence between the elements of the automorphism group \( \text{Aut}(\phi(H)) \) and certain isometries of \( C_H \) (elements of \( \text{Aut}(C_H) \)). Let \( (M, N) \in \text{Aut}(\phi(H)), x = [\phi^{-1}([D_M]_{1,1}), \ldots, \phi^{-1}([D_M]_{v,v})] \) and \( X \) be the \( v \times v \) matrix such that each column is equal to \( x \). It follows that \( \phi(X + H) = D_M \phi(H) \).

Around, if \( Y \) is a \( v \times v \) matrix over \( \mathbb{F}_q \) with each row equal to \( y = [\phi^{-1}([D_N]_{1,1}), \ldots, \phi^{-1}([D_N]_{v,v})] \), then \( \phi(H - Y) = \phi(H)D_N^* \). So, \( \phi(X + PMHP_N^T - Y) = M \phi(H)N^* = \phi(H) \).

Thus \( X + PMHP_N^T - Y = H \) and \( (\sigma, \pi) \in \text{Aut}(C_H) \) where \( \sigma(u) = u + [D_N]_{ii} \) and \( \pi(1, \ldots, v) = (1, \ldots, v)P_N \).

Now, the following question arises naturally: Given an isometry \( (\sigma, \pi) \) of \( C_H \), is it possible to define an automorphism \( (M, N) \) of \( \phi(H) \) associated to \( (\sigma, \pi) \)? We will answer this question affirmatively in a particular case in the next section.

**Definition 1** [3] A \( q \)-ary code \( C \) of length \( n \), \( 0 \in C \), has a propelinear structure if for any codeword \( x \in C \) there exist \( \pi_x \in S_n \) and \( \sigma_x = (\sigma_{x,1}, \ldots, \sigma_{x,n}) \) with \( \sigma_{x,i} \in \text{Sym} \mathbb{F}_q \) satisfying:

(i) \( (\sigma_x, \pi_x)(C) = C \) and \( (\sigma_x, \pi_x)(0) = x \),

(ii) if \( y \in C \) and \( z = (\sigma_x, \pi_x)(y) \), then \( (\sigma_z, \pi_z) = (\sigma_x, \pi_x) \circ (\sigma_y, \pi_y) \).

A \( q \)-ary code 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

\[
x \star y = (\sigma_x, \pi_x)(y) \quad \text{for any } x, y \in C.
\]

Therefore, \( (C, \star) \) is a group, which is not abelian in general. This group structure is compatible with the Hamming distance, that is, \( d(x \star u, x \star v) = d(u, v) \) where \( u, v \in \mathbb{F}_q^n \). The vector \( 0 \) is always a codeword where \( \pi_0 = I_{d_q} \) the identity coordinate permutation and \( \sigma_0,i = I_{d_q} \) is the identity permutation on \( \mathbb{F}_q \) for all \( i \in [1, \ldots, n] \). Hence, \( 0 \) is the identity element in \( C \) and \( \pi_{x^{-1}} = \pi_x^{-1} \) and \( \sigma_{x^{-1},i} = \sigma_{x^{-1},\pi_x(i)} \) for all \( x \in C \) 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.
Clearly, the propelinear class is more general than the linear code class, since every linear code \( C \) has the following trivial propelinear structure:

\[
\sigma_a(x) = a + x, \quad \text{and} \quad \pi_a(x) = x \quad \forall a, x \in C.
\]

In Examples 3, 4, 5 we show linear codes which can be endowed with a nontrivial propelinear structure. In Example 6 we present a nonlinear propelinear code.

**Proposition 2** Let \((C, \star) \subset \mathbb{F}_q^n\) be a group. \( C \) is propelinear code if and only if the group \( \text{Aut}(C) \) (the isometries) contains a regular subgroup acting transitively on \( C \).

**Proof** Firstly, we assume \( C \) is propelinear. Let \( \rho_x : C \to C \) given by \( \rho_x(v) = x \star v \). Let \( x, y, z \) be any codewords in \( C \), we have \( \rho_x(yz) = \rho_x(yz) = x \star (yz) = (x \star y)z = \rho_x(z) \). From [3, Lemma 5], we have \( d(x \star y, x \star z) = d(y, z) \), and so \( d(\rho_x(y), \rho_x(z)) = d(x \star y, x \star z) = d(y, z) \). Therefore, \( G = \{ \rho_x | x \in G \} \) is a subgroup of \( \text{Aut}(C) \), and \(|G| = |C| \). Given \( x, y \in C \), we take \( z = y \star x^{-1} \), and so we have \( \rho_z(x) = z \star x = y \star x^{-1} \star x = y \). Hence, \( G \) acts transitively on \( C \).

Conversely, we assume \( \text{Aut}(C) \) contains a regular subgroup \( G \) acting transitively on \( C \), so \(|G| = |C| \). We call \( \rho_x \) the element of \( G \) such that \( \rho_x(0) = x \). Note that \( G \to C \) given by \( \rho_x \to x \) is a bijection since \( G \) is regular and acts transitively on \( C \). For \( x \in C \), we define \( (\sigma_x, \pi_x)(y) = \rho_x(y) \). Note that \((\sigma_x, \pi_x) \in \text{Aut}(C) \) because \( \rho_x \) is an isometry on \( C \). We define \( x \star y = (\sigma_x, \pi_x)(y) = \rho_x(y) \), where \( x \in C \). Let us see that the operation \( \star \) is propelinear, and so \( C \) has a propelinear structure. It is clear that \((\sigma_x, \pi_x)(C) = \rho_x(C) = C \), and \( x \star \mathbf{0} = \rho_x(0) = x \) for any \( x \in C \). As \( G \) acts transitively on \( C \), we have \( \rho_x \rho_y = \rho_{xy} \) if and only if \( \rho_x \rho_y(0) = \rho_{xy}(0) \). Let \( x, y \in C \), then \( \rho_{xy}(0) = x \star y = \rho_x(y) = \rho_x(\rho_y(0)) = \rho_{xy}(0) \). Thus, \((\sigma_{xy}, \pi_{xy})(z) = \rho_{xy}(z) = \rho_x \rho_y(z) = \rho_x((\sigma_y, \pi_y)(z)) = (\sigma_x, \pi_x) \circ (\sigma_y, \pi_y)(z) \). \( \square \)

In the binary case, when \( q = 2 \), taking the usual addition on \( \mathbb{F}_2 \), the above definition is reduced to the following:

A binary code \( C \) of length \( n \) is **propelinear** [21] if for each codeword \( x \in C \) there exists \( \pi_x \in S_n \) satisfying the following conditions for all \( y \in C \):

(i) \( x + \pi_x(y) \in C \).

(ii) \( \pi_x \pi_y = \pi_{x+y} \).

Furthermore, \( C \) is called **full propelinear** [20] if the permutation \( \pi_x \) has no fixed coordinates when \( x \neq 0, x \neq 1 \); and if \( 1 \in C \) then \( \pi_1 = I_{dn} \).

Let \( C \) be a binary propelinear code. In [2, Lemma 5.1], it is proved that \( x \in K(C) \) if and only if \( \pi_x \in \text{Aut}(C) \). As a code is linear if and only if its dimension is equal to the dimension of its kernel and to its rank, we have that a binary propelinear code \( C \) is linear if and only if \( \pi_x \in \text{Aut}(C) \) for all \( x \in C \). The analog of this result about the linearity for \( q \)-ary propelinear codes remains an open problem.

**Definition 2** A **full propelinear code** is a propelinear code \( C \) such that for every \( a \in C \), \( \sigma_a(x) = a + x \) and \( \pi_a \) has no fixed coordinates when \( a \neq \alpha \mathbf{1} \) for \( \alpha \in \mathbb{F}_q \). Otherwise, \( \pi_a = I_{dn} \).

A generalized Hadamard code, which is also full propelinear, is called a generalized Hadamard full propelinear code (briefly, GHFP-code). In the binary case, we have the Hadamard full propelinear codes, they were introduced in [20] and their equivalence with Hadamard groups was proven.

**Lemma 2** Let \( C \) be a GHFP-code and \( a, b \in C \). If \( a - b = \lambda \mathbf{1} \) where \( \lambda \in \mathbb{F}_q \) then \( \pi_a = \pi_b \).
Proof} We have $b \star \lambda 1 = b + \pi_b(\lambda 1) = b + \lambda 1 = a$ and $a \star \lambda 1 = \lambda 1 \star a$. On the other hand, $\pi_d(x) = a \star x - a = (b \star \lambda 1) \star x - (b + \lambda 1) = (b \star x) \star \lambda 1 - (b + \lambda 1) = b \star x - b = \pi_b(x)$, for all $x \in C$.

Lemma 3 Let $C$ be a GHFP-code and $e_i$ be the unitary vector with only nonzero coordinate at the $i$-th position. If $x, y \in C$ then $\pi_x^{-1}(e_i) = \pi_y^{-1}(e_i)$ if and only if $x = y + \lambda 1$, $\lambda \in \mathbb{F}_q$. Furthermore, if $x, y \in F_H$ then $x = y$.

Proof We have $\pi_x^{-1}(e_i) = \pi_y^{-1}(e_i) \iff e_i = \pi_x \pi_y^{-1}(e_i) = \pi_x \pi_y^{-1}(e_i) = \pi_{x \star y^{-1}}(e_i)$. Since $C$ is full propelinear then $x \star y^{-1} = \lambda 1$, $\lambda \in \mathbb{F}_q$.

Lemma 4 Let $C$ be a GHFP-code, $\Pi = \{\pi_x: x \in C\}$ and $C_1 = \{\lambda 1: \lambda \in \mathbb{F}_q\}$. Then $C_1 \subset K(C)$ and $\Pi$ is isomorphic to $C/C_1$.

Proof It is immediate that $C_1 = \{\lambda 1: u \in \mathbb{F}_q\}$. The map $x \to \pi_x$ is a group homomorphism from $C$ to $\Pi$. Since $C$ is full propelinear, the kernel of this homomorphism is $C_1$. Hence, we conclude with the desired result.

3 GHFP-codes and cocyclic generalized Hadamard matrices

In this section we establish the connection between GHFP-codes and the cocyclic generalized Hadamard matrices, of which a great deal is already known. This informs us of the group structure and generating codewords of GHFP-codes, which can be constructed directly from known cocyclic generalized Hadamard matrices.

From now on, $H$ denotes a generalized Hadamard matrix of order $v$ with entries in the additive elementary abelian group $\mathbb{F}_q$. $K$ denotes a multiplicative group isomorphic to the additive elementary abelian group $\mathbb{F}_q$, and let $\phi: \mathbb{F}_q \to K$ be an isomorphism. Write $\phi(H) = [\phi(h_{ij})]_{1 \leq i, j \leq n}$.

Consider the $qv \times v$ matrix $E_{\phi(H)}$ comprised of the $q$ blocks $k_0\phi(H), \ldots, k_{q-1}\phi(H)$ where $K = \{1 = k_0, \ldots, k_{q-1}\}$. Assuming that $C_H$ is a GHFP-code and $a, x \in C_H$, then the action of $a$ on $C_H$ defined by

$$\rho_a(x) = a \star x = a + \pi_a(x) \in C_H,$$

($\rho_a \in \text{Aut}(C_H)$) is equivalent to the action of $N^*$ on $E_{\phi(H)}$ by right matrix multiplication where $N^* = Q^*D_{-a}^*$, with $Q$ being the permutation matrix according to $\pi_a$, and $D_a$ the diagonal matrix with diagonal $\phi(a)$. Since the action of $a$ on $C$ preserves $C$, there is a $qv \times qv$ permutation matrix $P'$ such that $P'E_{\phi(H)}N^* = E_{\phi(H)}$. Moreover, the rows of $E_{\phi(H)}$ are the rows of $\phi(H), k_1\phi(H), \ldots, k_{q-1}\phi(H)$. Thus there is a $v \times v$ monomial matrix $M = D_kP$ with $k$ a vector of length $v$ over $K$ such that $M\phi(H)N^* = \phi(H)$, where for all $1 \leq i, j \leq v$ and $0 \leq d \leq q - 1$, if $P'$ permutes row $j + dv$ to row $i$ then

- $P'$ permutes row $j$ to row $i$, and
- the $i$-th entry of $k$ is $q_d$.

Thus $(M, N)$ is an automorphism of $\phi(H)$, and if $a = \lambda 1$ for some $\lambda \in \mathbb{F}_q$, then the corresponding automorphism is of the form $(\phi(-\lambda)I, \phi(-\lambda)J)$. This proves the following result where $R$ denotes the subset of $\text{Aut}(\phi(H))$ with elements $(M, N)$, the corresponding automorphism associated to $a \in C_H$.

Theorem 2 If $H$ is a generalized Hadamard matrix over the additive abelian group of $\mathbb{F}_q$ such that the rows of $H$ comprise a GHFP-code $C$, then the group $(C, \star) \cong R \subseteq \text{Aut}(\phi(H))$. Moreover, $(kI, kI) \in R$ for all $k \in K$, and $R$ acts transitively on rows of $\phi(H)$.
Remark 2 \( R \) acts transitively on rows of \( \phi(H) \) since \( \rho_a(x) = \rho_b(x) \) if and only if \( a = b \) but not regularly since \( |R| \neq v \).

Now, for a generalized Hadamard matrix \( M \) with entries in \( K \), \( \Aut(M) \cong \PAut(E_M) \) where \( E_M = [k_i j_M]_{0 \leq i, j \leq q - 1} \) (this is a special case of [7, Theorem 9.6.14]). Where \( \Theta : \Aut(M) \to \PAut(E_M) \) is the isomorphism outlined in [7, pp. 110–111], we note that the center of \( \Aut(M) \) contains the group of pairs of diagonal matrices \( Z = \{(kI, kI) : k \in K\} \), and thus \( \Theta(Z) \) is a central subgroup of \( \PAut(E_M) \). We require that \( \pi_{1,1} = Id_n \) in order for \( C \) to be full propelinear. The transitivity requirement of the group \( (C, \star) \) on \( C \) for full propelinear codes then gives the following.

Theorem 3 \( C \) is a generalized Hadamard full propelinear code if and only if there is a subgroup \( R \subseteq \Aut(\phi(H)) \) with \( Z \subseteq R \) such that \( \PAut(E_{\phi(H)}) \) contains a regular subgroup \( \Theta(R) \), with \( \Theta(Z) \subseteq \Theta(R) \).

Proof Let \( K = \{1 = k_0, \ldots, k_{q - 1}\} \) and \( Z = \{z_i = (k_i I, k_i I) : i \in \{0, \ldots, q - 1\}\} \) and let \( C \) be a generalized Hadamard full propelinear code. Theorem 2 gives that \((C, \star) \cong R \subseteq \Aut(\phi(H))\) where \( Z \subseteq R \), and \( R \) acts transitively on the rows of \( \phi(H) \). Since \( Z \) is central and acts only by multiplication on rows of \( \phi(H) \), there is a right transversal \( S \) of \( Z \) in \( R \) where for any \( j \in \{1, \ldots, n\} \) there is \( s_j \in S \) such that \( \phi(H)(j) = (s_j \phi(H))_1 \). Thus \( \Theta(z_is_j) \) permutes row 1 of \( E_{\phi(H)} \) to row \( iq + j \), proving that \( \Theta(R) \) is transitive on rows of \( E_{\phi(H)} \). By Theorem 2, \(|R| = |(C, \star)|\) and thus \( \Theta(R) \) acts regularly.

Conversely, assume that \( H \) is generalized Hadamard over \( \mathbb{F}_q \) and that there is a subgroup \( R \subseteq \Aut(\phi(H)) \) with \( Z \subseteq R \) such that \( \Theta(R) \subseteq \PAut(E_{\phi(H)}) \) is regular and \( \Theta(Z) \subseteq \Theta(R) \). Label the rows of \( E_{\phi(H)} \) with the codewords of \( C_H \) in the order of the rows of \( E_H \) such that the first \( n \) entries of the row of \( E_{\phi(H)} \) are the entries in the codeword labelling the row. For any \( x \in C_H \) there is \( (M_x N_x) \in \Theta(R) \) such that \( M_x \) sends row \( x \) to row 0. In the preimage of \( \Theta \), \( N_x \) corresponds to a monomial matrix \( D_{-x} Q_x \). For each \( x \), let \( \pi_x \) be the coordinate permutation according to the action of \( Q^* \) on columns of \( \phi(H) \), and let \( \sigma_x(a) = a + x \) for all \( a \in E_H \) (i.e., \( \pi_x \) and \( \sigma_x \) are determined by the column action of \( N_x \)). It follows that if \( (\pi_x, \sigma_x) \circ (\pi_y, \sigma_y) = (\pi_z, \sigma_z) \) then \( N_x N_y = N_z \). It also follows that \( (\sigma_x, \pi_x)(0) = x \) for all \( x \).

Then let \( f : \Theta(R) \to C_H \) be the map such that \( f(M_x, N_x) = x \). Clearly this map is bijective. Further, if \( \lambda \in \mathbb{F}_q \) then it follows that \( (M_\lambda, N_\lambda) \in \Theta(Z) \), where \( \pi_{1,1} = Id_n \). Because \( R \subseteq \Aut(\phi(H)) \), it follows that \( (\sigma_x, \pi_x)(C_H) = C_H \) for all \( x \).

Now observe that if \( N_x N_y = N_z \), then \( z = (\sigma_z, \pi_z)(0) = (\sigma_x, \pi_x)(\sigma_y, \pi_y)(0) = (\sigma_x, \pi_x)(y) \) and so \( z = x \star y \). Thus \( f(M_x, N_x) \star f(M_y, N_y) = x \star y = z = f(M_z, N_z) \), and so \( f \) is a homomorphism and \( C_H \) has a propelinear structure.

Let \( G \) be a group of order \( n \) and let \( \psi : G \times G \to K \) be a 2-cocycle. Then let \( E_{\psi} \) denote the canonical central extension of \( K \) by \( G \) obtained from \( \psi \). The following is a special case of [7, Theorem 14.6.4].

Theorem 4 A generalized Hadamard matrix \( H \) over \( K \) is cocyclic with cocycle \( \psi \) if and only if there exists a centrally regular embedding of \( E_{\psi} \) into \( \PAut(E_H) \).

Corollary 1 The code \( C_H \) comprised of the rows of \( E_H \) is a generalized Hadamard full propelinear code if and only if the matrix \( H \) is cocyclic over some cocycle \( \psi \), with extension group \( E_{\psi} \cong R \cong (C_H, \star) \) where \( R \) is a regular subgroup of \( \PAut(E_H) \).
Remark 3 We observe that a generalized Hadamard matrix $H$ may be cocyclic over several distinct cocycles $\psi$, and that the extension groups $E_{\psi}$ are not necessarily isomorphic. As such, given a cocyclic generalized Hadamard matrix $H$, there may be several codes $(C_H, \star)$ that are equal setwise, i.e., they contain the same set of codewords, but are not isomorphic as groups.

In what follows, we will make explicit the correspondence between the elements of $E_{\psi}$ and $(C_H, \star)$.

Assuming $\psi \in Z^2(G, K)$. For a fixed ordering in $G = \{g_0 = 1, g_1, \ldots, g_{v-1}\}$ and in $K = \{k_0 = 1, k_1, \ldots, k_{q-1}\}$ (we recall that $K$ denotes the multiplicative group isomorphic to the additive elementary abelian group $\mathbb{F}_q$), we can define the following map:

$$\Phi: E_{\psi} \to K^v$$

given an element $(k, g) \in E_{\psi},$

$$[\Phi(k, g)]_j = k_1, \quad \text{if} \ (k, g)^{-1}t_j \in T(\psi)(k_1, 1),$$

where $T(\psi) = \{(t_0 = (1, 1), t_2 = (1, g_1), \ldots, t_{v-1} = (1, g_{v-1})\}$. Obviously, $T(\psi)(c_1, 1) = (c_1, 1)T(\psi)$ and $\Phi$ is well-defined. After some calculations,

$$[\Phi(k, g)]_j = (k(g, g^{-1}))^{-1}\psi^{-1}(g^{-1}, g_j).$$

Hence, $\Phi(k, g)$ is equal to $(k\psi(g, g^{-1}))^{-1}$-times the row of $M_{\psi}$ indexed with the element $g^{-1}$.

Clearly, $\Phi$ is an injective map. The inverse of $\Phi$ (over the Im $\Phi$) is

$$\Phi^{-1}(\lambda(\psi(g, g_1), \ldots, \psi(g, g_v))) = ((\lambda\psi^{-1}(g), g^{-1}), g^{-1}),$$

where $\lambda \in K$ and $g \in G$.

Proposition 3 If $\psi \in Z^2(G, K)$ is orthogonal then $C = (\Phi(E_{\psi}), \star)$ is a GHFP-code where $x \star y = \Phi(\Phi^{-1}(x) \cdot \Phi^{-1}(y))$ with $x, y \in \Phi(E_{\psi})$.

Proof Firstly, we will show that $\pi_x \in S_v$ where $\pi_x(y) = x \star y - x$. We know that every codeword has to be a multiple of a row of $M_{\psi}$. We take $x = \lambda(\psi(g, g_1), \ldots, \psi(g, g_v))$ and $y = \mu(\psi(h, g_1), \ldots, \psi(h, g_v))$. By a routine computation, we get that

$$[x \star y]_j = \lambda\mu\psi(g^{-1}, g)(\psi(h^{-1}, h)(\psi(g^{-1}, h^{-1})\psi((hg)^{-1}, hg))^{-1}\psi(hg, g_j)(\psi(g, g_j))^{-1}\psi(hg, g_j).$$

Putting together,

$$[\pi_x(y)]_j = [x \star y]_j - [x]_j$$

$$= \mu\psi(g^{-1}, g)(\psi(h^{-1}, h)(\psi(g^{-1}, h^{-1})\psi((hg)^{-1}, hg))^{-1}\psi(hg, g_j)(\psi(g, g_j))^{-1}\psi(hg, g_j).$$

In the last identity we have used these properties coming from (1):

- $\psi(hg, g_j)(\psi(g, g_j))^{-1} = \psi(hg, g_j)(\psi(h, g))^{-1}.$
- $\psi(h^{-1}, h)(\psi(h, g))^{-1} = \psi(h^{-1}, hg).$
- $\psi(g^{-1}, h^{-1})\psi(g^{-1}h^{-1}, hg) = \psi(g^{-1}, g)(\psi(h^{-1}, hg).$

Hence, the map $\pi_x$ is an element of $S_v$. Specifically, for any $y, \pi_x$ moves the $l$-th coordinate of $y$ to the $j$-th coordinate where $g_l = gg_j$. As a consequence of this fact, it is immediate that if $x = \lambda \mathbf{1}$, $\lambda \in \mathbb{F}_q$ then $\pi_x = Id_v$ since $g = 1$ the identity of $G$. Furthermore, if $g \neq 1$ (or equivalently $x \neq \lambda \mathbf{1}$), then $\pi_x$ has not any fixed coordinate.
Secondly, we show an important property of these permutations. Concretely, given \( x, y \in C \), we have that \( \pi_x \pi_y = \pi_{x \star y} \). To prove this, let \( z \) be an element of \( C \) then

\[
\pi_x \pi_y (z) = (x \star y) \star z - x \star y \\
= x \star (y \star z) - x \star y \\
= x + \pi_x (y \star z) - \pi_x (y) - x \\
= \pi_x (y \star z - y) = \pi_x (\pi_y (z)).
\]

\(\Box\)

Let \( H \) be a normalized Hadamard matrix \( GH(q, v/q) \) over \( \mathbb{F}_q \) and \( f \) be any row of \( H \). \( D_j \) denotes the subset of \( C_H \) such that \( x \in D_j \) if \( [x]_j = 0 \in \mathbb{F}_q \). Let us observe the following facts:

1. \( D_j = \bigcup_{\alpha \in \mathbb{F}_q} \{ f + (-\alpha)1 : f \in F_H \wedge [f]_j = \alpha \} \).
2. \( D_1 = F_H \).
3. For \( j > 1 \), \( |\{ f \in F_H : [f]_j = \alpha \} = v/q \). Since \( \mathbb{F}_q \) is abelian then \( H^T \) is a \( G\)(\( q, v/q) \) (over \( \mathbb{F}_q \)) too [15, Lemma 4.10]. Thus, the number of entries equal to \( \alpha \) in the \( j \)-th column of \( H \) is \( v/q \), for all \( \alpha \in \mathbb{F}_q \).

**Proposition 4** Let \( (C, \star) \) be a GHFP-code of length \( v \) over \( \mathbb{F}_q \) coming from \( H \), which is a \( G\)(\( q, v/q) \). Then \( F_H = D_1 \) is a (central) relative \( (v, q, v, v/q) \)-difference set in \( C \) relative to the normal subgroup \( C_1 = \{ \alpha 1 : \alpha \in \mathbb{F}_q \} \equiv \mathbb{F}_q \).

**Proof** \( C_1 \) is a central subgroup. We have to prove:

\[
|F_H \cap x \star F_H| = \begin{cases} 
 v & x = 0 \\
 0 & x \in C_1 \setminus \{ 0 \} \\
 v/q & x \in C \setminus C_1
\end{cases}
\]

- Let us observe that if \( x \in C_1 \) then \( \pi_x = Id_v \). Now, if \( f \in F_H \) then the first entry of \( x \star f = x + f \) is 0 if and only if \( x = 0 \). So, we concluded with the desired result for the first and the second identities.
- Let \( x \notin C_1 \) and \( \pi_x(1) = j \) (\( j \neq 1 \) since it is full propelinear). Let \( \alpha_0 \in \mathbb{F}_q \) be such that \( [x + \alpha_0 1]_j = 0 \). Since \( (x + \alpha_0 1) \star f \in D_j \) for all \( f \in F_H \) and \( |y \star F_H| = v \) for all \( y \in C_H \) then \( (x + \alpha_0 1) \star F_H = D_j \). As a consequence,

\[
x \star F_H = D_j - \alpha_0 1.
\]

Therefore, \( |F_H \cap x \star F_H| = \) number of entries equal to \( -\alpha_0 \) in the \( j \)-th column of \( H \) what it is equal to \( v/q \). This concludes the proof.

\(\Box\)

**Corollary 2** Let \( (C, \star) \) be a GHFP-code of length \( v \) over \( \mathbb{F}_q \) coming from \( H \), a \( G\)(\( q, v/q) \). Let \( G = C/C_1 \) and \( \sigma(f \star C_1) = f \) for \( f \in F_H \). The map \( \psi_{F_H} : G \times G \to K \) defined by

\[
\psi_{F_H}(g, h) = k, \quad \text{if} \quad \sigma(g) \star \sigma(h) \in k1 \star F_H
\]

is an orthogonal cocycle, i.e. \( M_{\psi_{F_H}} \) is a \( G\)(\( q, v/q) \). Furthermore, \( (C, \star) \equiv E_{\psi_{F_H}} \) where \( F_{H}^* = \{(1, g) : g \in G \} \) is the isomorphic image of \( F_H \).

**Proof** It is a consequence of [18, Theorem 3.1] and Proposition 4.  

\(\Box\)
4 Examples

In this section, we provide some examples of generalized Hadamard full propelinear codes coming from cocyclic generalized Hadamard matrices. The last one has a special interest since this family is not linear. We will study their rank and the dimension of their kernel. In [9] the study of the rank and dimension of the kernel of codes coming from generalized Hadamard matrices was initiated. Recall that a GH-code over $F_q$ has $q^v$ codewords, length $v$ and minimum distance $v - \frac{v}{q}$. Hence, the GH-codes in this section meet the Plotkin bound [15], and are generally non-linear. In particular, the number of codewords in a code over $F_q$ need not be a power of $q$, unlike a linear code, and we can take advantage of this to construct codes which slightly improve on the best comparable linear codes. As a small example, we take the GH$(3,2)$ constructed by Butson [5] and build a $[6,18,4]_3$. This has more codewords than the optimal linear $[6,3,4]_3$ code, and beats the minimum distance bound of 3 on a $[6,3]_3$ code, albeit with fewer codewords. More generally, a GH$(p,2)$ exists for all primes $p$ by the same construction of Butson, and we obtain similar results. The matrices are not necessarily cocyclic however. To take a cocyclic example, up to equivalence there are two cocyclic matrices in GH$(3,4)$, see [12]. Thus we get propelinear codes with parameters $[12,36,8]_4$ which have more codewords than the optimal linear $[12,3,8]_3$ code, and beats the minimum distance bound of 6 on a linear $[12,4]_3$ code.

Example 2 We use the cocyclic GH$(4,8)$ over $F_4$ obtained by taking the Kronecker product of the cocyclic GH$(4,1)$ and GH$(4,2)$

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & ab & b \\ 1 & ab & b & a \\ 1 & b & a & ab \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & a & b & b & ab & ab & ab \\ 1 & a & ab & b & b & a & 1 & 1 \\ 1 & a & ab & b & 1 & a & b & ab \\ 1 & b & 1 & a & ab & ab & a & a \\ 1 & b & a & ab & a & 1 & b & 1 \\ 1 & ab & b & a & ab & 1 & b & a \\ 1 & ab & a & ab & 1 & a & b & b \end{pmatrix}.$$

where $U = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle \cong Z_2^2$. From $H_1 \otimes H_2$, which is cocyclic by [7, Theorem 15.8.4], we extract a $[32,128,24]_4$ propelinear code. This code has more codewords than the optimal linear $[32,3,24]_4$ code, and beats the minimum distance bound of 22 on a $[32,4]_4$ code. For other examples of propelinear codes obtained in this way, we rely on the existence of cocyclic generalized Hadamard matrices over $F_q$. We refer to [15] and the references therein for known existence results of this type.

For the remainder of this section we give examples that demonstrate the theory in full, and provide infinite families in some cases. We begin with a definition of an infinite family of cocyclic generalized Hadamard matrices.

Definition 3 [7, Section 9.2] Let $q = p^m$ be a prime power and denote the $k$-dimensional vector space over $F_q$ by $V$. Then

$$D_{(p,m,k)} = [xy^\top]_{x,y \in V}$$

is a GH$(q,q^{k-1})$. These are known as the generalized Sylvester matrices.

It is well known that the generalized Sylvester matrices are cocyclic, see [15, p. 122] for example. They were analyzed in terms of their cocyclic development in [11]. The analysis
shows that these matrices have several non-isomorphic indexing and extension groups, and
the number of non-isomorphic indexing and extension groups grows with \( k \) and \( m \). They are
closely related to the regular subgroups of the affine general linear group \( AGL_{k+1}(V) \). Hence
the matrix \( H = D_{(p,m,k)} \) of order \( q^k \) is cocyclic with multiple cocycles \( \psi \) and has multiple
non-isomorphic extension groups \( E_\psi \) of order \( q^{k+1} \). As such, for each \( \psi \) the associated codes
\((C,\star)\) each have the same set of codewords (the rows of \( E_H \)), but are non-isomorphic as
groups. Some of the examples below are members of the generalized Sylvester matrices.

**Example 3** If \( G = U = \langle a,b \mid a^2 = b^2 = (ab)^2 = 1 \rangle \cong \mathbb{Z}_2^2 \) (the additive group of \( \mathbb{F}_4 \)
but with multiplicative notation) with indexing \( \{1,a,b,ab\} \), then the \( G \)-cocyclic matrix with
coefficients in \( U \)
\[
H = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & a & ab & b \\
1 & ab & b & a \\
1 & b & a & ab
\end{pmatrix}
\]
is a generalized Hadamard matrix, \( GH(4,1) \), with entries in \( \mathbb{F}_4 \).

Now, set \( C_i = \{ f_i + \alpha \mathbf{1} \mid \alpha \in G \} \), where \( f_i \) denotes the vector corresponding to the
\( i \)-th row of \( H \) and \( \mathbf{1} \) denotes the all-one vector. (We will follow this notation in the sequel
examples). For instance,
\[
C_1 = \{ (1, 1, 1, 1), (a, a, a, a), (b, b, b, b), (ab, ab, ab, ab) \}.
\]
The generalized Hadamard code over \( U \)
\[
C = C_1 \cup C_2 \cup C_3 \cup C_4
\]
can be endowed with a full propelinear structure with the following group \( \Pi \) of permutations
\[
\pi_x = \begin{cases}
\mathbf{1} & x \in C_1 \\
(1, 2)(3, 4) & x \in C_2 \\
(1, 3)(2, 4) & x \in C_3 \\
(1, 4)(2, 3) & x \in C_4
\end{cases}
\]
That is, \( x \star y = x + \pi_x(y) \) where \( (C, \star) \cong \mathbb{Z}_4^2 \) and \( \Pi \cong \mathbb{Z}_2^2 \). The rank and the dimension of
the kernel of this \((4, 16, 3)_4\)-code are 2.

**Example 4** If \( G = \mathbb{Z}_3^2 \) with indexing \((0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\), then the \( G \)-cocyclic matrix over \( \mathbb{Z}_3 \)
\[
H = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 \\
0 & 2 & 1 & 0 & 2 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 2 & 2 \\
0 & 1 & 2 & 1 & 2 & 0 & 2 \\
0 & 2 & 1 & 1 & 0 & 2 & 2 \\
0 & 0 & 0 & 2 & 2 & 2 & 1 \\
0 & 1 & 2 & 2 & 0 & 1 & 1 \\
0 & 2 & 1 & 2 & 0 & 1 & 0 \\
0 & 0 & 2 & 1 & 0 & 1 & 0
\end{pmatrix}
\]
is a generalized Hadamard matrix (of Sylvester type), \( GH(3, 3) \), with entries in \( \mathbb{F}_3 \). The
generalized Hadamard code over \( G \)
\[
C = C_1 \cup C_2 \cup \ldots \cup C_9
\]
can be endowed with a \textit{full propelinear structure} with the following group $\Pi$ of permutations

$$
\pi_x = \begin{cases}
I & x \in C_1 \\
(1, 2, 3)(4, 5, 6)(7, 8, 9) & x \in C_2 \\
(1, 3, 2)(4, 6, 5)(7, 9, 8) & x \in C_3 \\
(1, 4, 7)(2, 5, 8)(3, 6, 9) & x \in C_4 \\
(1, 5, 9)(2, 6, 7)(3, 4, 8) & x \in C_5 \\
(1, 6, 8)(2, 4, 9)(3, 5, 7) & x \in C_6 \\
(1, 7, 4)(2, 8, 5)(3, 9, 6) & x \in C_7 \\
(1, 8, 6)(2, 9, 4)(3, 7, 5) & x \in C_8 \\
(1, 9, 5)(2, 7, 6)(3, 8, 4) & x \in C_9
\end{cases}
$$

We have $C \cong \mathbb{Z}_3^4$ and $\Pi \cong \mathbb{Z}_3^2$. The rank and the dimension of the kernel of this $(9, 27, 6)_3$-code are 3.

**Example 5** Let $G = U = \mathbb{Z}_2^3$ be with indexing $\{0, 1, x, x^2, x^3, x^4, x^5, x^6\}$ where

$$
\begin{array}{cccccccc}
+ & 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\
0 & 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\
1 & x^3 & x^6 & x & x^5 & x^4 & x & x^5 & x^6 \\
x & 0 & x^4 & 1 & x^2 & x^6 & 1 & x^6 & x^5 \\
x^2 & 0 & x^5 & x & x^3 & 1 & 0 & x & x^3 \\
x^3 & 0 & x^6 & x & x^2 & x^4 & 0 & x & x^3 \\
x^4 & 0 & 1 & x^3 & 0 & 0 & 0 & 0 & 0 \\
x^5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
x^6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}
$$

then the $G$-cocyclic matrix over $U$

$$
H = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\
0 & x & x^2 & x^3 & x^4 & x^5 & x^6 & 1 \\
0 & x^2 & x^3 & x^4 & x^5 & x^6 & 1 & x \\
0 & x^3 & x^4 & x^5 & x^6 & 1 & x & x^2 \\
0 & x^4 & x^5 & x^6 & 1 & x & x^2 & x^3 \\
0 & x^5 & x^6 & 1 & x & x^2 & x^3 & x^4 \\
0 & x^6 & 1 & x & x^2 & x^3 & x^4 & x^5
\end{pmatrix}
$$

is a generalized Hadamard matrix, $\text{GH}(8, 1)$, with entries in $\mathbb{F}_8$. The generalized Hadamard code over $G$

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

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

$$
\pi_x = \begin{cases}
I & x \in C_1 \\
(1, 2)(3, 5)(4, 8)(6, 7) & x \in C_2 \\
(1, 3)(2, 5)(4, 6)(7, 8) & x \in C_3 \\
(1, 4)(2, 8)(3, 6)(5, 7) & x \in C_4 \\
(1, 5)(2, 3)(4, 7)(6, 8) & x \in C_5 \\
(1, 6)(2, 7)(3, 4)(5, 8) & x \in C_6 \\
(1, 7)(2, 6)(3, 8)(4, 5) & x \in C_7 \\
(1, 8)(2, 4)(3, 7)(5, 6) & x \in C_8
\end{cases}
$$
Table 1 The pairs \((r, k)\) of the entries of this table denote the rank and the dimension of the kernel of the GHFP-codes \(C_{a,b}\) associated to \(\partial \phi(a,b)\) of Example 1 with parameters \((3^a, 2^{2a}, 3^a - 1)_3\).

| \(b\) | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|
| 3 | (11,1) | (11,1) | (11,1) | (11,1) | (11,1) |
| 5 | (47,1) | (47,1) | (47,1) | (47,1) |
| 7 | (191,1) | (191,1) | (191,1) |
| 9 | (767,1) |

We have \((C, \ast) \cong \mathbb{Z}_4^3\) and \(\Pi \cong \mathbb{Z}_2^3\). The rank and the dimension of the kernel of this \((8, 64, 7)_8\)-code are 2.

Example 6 Let \(G = U = \mathbb{Z}_4^3\) be with indexing \(\{0000, 0001, 0002, 0010, \ldots, 2222\}\), the irreducible polynomial which defines multiplication in the field is \(2 + x + x^4\) and let \(\phi(4,3)\) as in Example 1. Then the \(G\)-cocyclic matrix over \(U\)

\[
[H]_{g,h} = \partial \phi(4,3)(g, h)
\]

is a generalized Hadamard matrix, \(\text{GH}(81, 1)\), with entries in \(\mathbb{F}_{81}\).

\[
C = C_1 \cup C_2 \cup \ldots \cup C_{81}
\]

can be endowed with a full propelinear structure. The group \(\Pi\) of permutations and the matrix \([H]_{g,h}\) can be downloaded from the following website (ddd.uab.cat/record/204295).

We have that \((C, \ast) \cong \mathbb{Z}_4^3\) and \(\Pi \cong \mathbb{Z}_4^3\). The rank of this \((81, 81^2, 80)_{81}\)-code is 11 and the dimension of the kernel is 1. So, \(C\) is not linear as we knew.

In Table 1, we consider the codes associated to \(\partial \phi(a,b)\) of Example 1. Let us recall that \(\phi(a,b)(g) = g^{(3^b + 1)}/2\), with \(g \in \mathbb{F}_{3^a}\). Moreover, if \((a, b) = 1, b\) odd and \(3 \leq b \leq a - 1\) then \(\partial \phi(a,b)\) are orthogonal cocycles and the associated GHFP-codes \(C_{a,b}\) are not linear but are they inequivalent? That is, fixing \(a\) and assuming that \(b_1\) and \(b_2\) with \(b_1 \neq b_2\) are admissible values, are \(C_{a,b_1}\) and \(C_{a,b_2}\) inequivalent? If the conjecture below in the last statement of this section were true, we would have an affirmative answer. For instance, for \(a = 7\) we have two (cocyclic) \(\text{GH}(3^7, 1)\) matrices (one for \(b = 3\) and another for \(b = 5\)) where their codes \((C_{7,3}\) and \(C_{7,5})\) are inequivalent since they have different rank. Consequently, the GH matrices are nonequivalent as well.

Let us notice that in Table 1, we have computed the rank and dimension of the kernel for all admissible value of \(b\) for each \(a\) in the range \(3 \leq b \leq a - 1\) and \(4 \leq a \leq 10\). All these computations have been carried out with \textsc{magma} \[4\]. We prove in Corollary 3 that always \(k = 1\) and for the rank we conjecture that \(r\) depends only on \(b\) by \(r(b) = 3 \cdot 2^{b-1} - 1\) with \(b\) odd.

5 Kronecker sum construction

In this section we extend the classical construction of Hadamard codes, based on Kronecker products, to the case of GHFP-codes. As application, we construct an infinite family of nonlinear GHFP-codes for each \(\text{GH}(3^a, 1)\) matrix as in Example 1. Some properties of their rank and the dimension of their kernel are studied and they have been used to prove their nonlinearity.
The Kronecker sum construction [22] is a standard method to construct GH matrices from other GH matrices. That is, if \( H = (h_{i,j}) \) is any \( GH(w, v/w) \) matrix over \( U \) and \( B_1, B_2, \ldots, B_v \) are any \( GH(w, v'/w) \) matrices over \( U \) then the matrix

\[
H \oplus [B_1, B_2, \ldots, B_v] = \begin{pmatrix}
  h_{11} + B_1 & \cdots & h_{1v} + B_1 \\
  \vdots & \ddots & \vdots \\
  h_{v1} + B_v & \cdots & h_{vv} + B_v
\end{pmatrix}
\]

is a \( GH(w, vv'/w) \) matrix. If \( B_1 = B_2 = \ldots = B_v = B \), then we denote \( H \oplus [B_1, B_2, \ldots, B_v] \) by \( H \oplus B \).

If \( \psi \in Z^2(G, U) \) and \( \psi' \in Z^2(G', U) \), then their tensor product \( \psi \otimes \psi' \in Z^2(G \times G', U) \), where

\[
(\psi \otimes \psi')(\langle g, g' \rangle, \langle h, h' \rangle) = \psi(g, h)\psi(g', h'),
\]

and \( M_{\psi \otimes \psi'} = M_{\psi} \oplus M_{\psi'} \).

Let \( S_q \) be the normalized \( GH(q, 1) \) matrix given by the multiplication table of \( \mathbb{F}_q \). We can recursively define \( S' \) as a \( GH(q, q^{t-1}) \) matrix, constructed as \( S' = S_q \oplus S'^{-1} \) for \( t > 1 \) (this is an alternative definition for the generalized Sylvester Hadamard matrices). It is well-known that \( S_q \) is cocyclic (see [15, p. 122]) and \( rank(C_{S_q}) = ker(C_{S_q}) = 2 \).

**Lemma 5** [9, Lemma 3] Let \( H_1 \) and \( H_2 \) be two GH matrices over \( \mathbb{F}_q \) and \( H = H_1 \oplus H_2 \). Then \( rank(C_H) = rank(C_{H_1}) + rank(C_{H_2}) - 1 \) and \( ker(C_H) = ker(C_{H_1}) + ker(C_{H_2}) - 1 \).

Immediate consequences of the result above are that \( rank(C_{S_q}) = ker(C_{S_q}) = l + 1 \). On the other hand, if \( H_1 \) is linear and \( H_2 \) is not (or vice versa) then \( H = H_1 \oplus H_2 \) is not linear.

**Lemma 6** [9, Corollary 28] Let \( H \) be a \( GH(q, q^{h-1}) \) matrix over \( \mathbb{F}_q \), with \( q > 3 \) and \( h \geq 1 \), or \( q = 3 \) and \( h \geq 2 \). Then \( rank(C_H) \in \{h + 1, \ldots, [q^{h}/2]\} \).

**Lemma 7** [9, Proposition 9] Let \( H \) be a \( GH(q, \lambda) \) over \( \mathbb{F}_q \), where \( q = p^e \) and \( p \) prime. Let \( v = q\lambda = p^j \) such that \( gcd(p, s) = 1 \). Then \( 1 \leq ker(C_H) \leq ker(C_H) \leq 1 + t/e \).

**Lemma 8** Let \( C \) be a generalized full propelinear code. Then \( K(C) \) is a subgroup of \( C \).

**Proof** As \( 0 \in C \), we have that \( K(C) \) is linear. Let \( x, y \) be in \( K(C) \), so \( \alpha x + C = C \) and \( \alpha y + C = C \) for all \( \alpha \in \mathbb{F}_q \). Therefore, \( \alpha(x \circ y) + C = \alpha(x + \pi_x(y)) + x \circ C = \alpha x + \alpha \pi_x(y) + x + \pi_x(C) = \alpha x + x + \pi_x(\alpha y + C) = \alpha x + x + \pi_x(C) = \alpha x + x \circ C = \alpha x + C = C \), and so \( x \circ y \in K(C) \). Thus, the operation \( \circ \) is closed on \( K(C) \). Since \( K(C) \) is finite and \( 0 \in C \), we have that \( K(C) \) is a subgroup. \( \Box \)

**Proposition 5** Let \( H \) be a \( GH(3^a, 1) \) over \( \mathbb{F}_{3^a} \) where \( C_H \) is a GHFP-code. Then \( ker(C_H) \in \{1, 2\} \). If \( ker(C_H) = 2 \) then \( C_H \) is linear. Furthermore, if \( a > 1 \), then \( rank(C_H) \geq 2 \).

**Proof** From Lemma 7, we have that \( ker(C_H) \in \{1, 2\} \). We suppose that \( K(C_H) = \{1, x\} \), for some \( x \in C_H \) with \( x \neq aI \) for any \( \alpha \in \mathbb{F}_{3^a} \). As the kernel is a linear subspace of \( C_H \), we have that \( K(C_H) = \{aI + \beta x : \alpha, \beta \in \mathbb{F}_{3^a}\} \). Thus, \( |K(C_H)| = 3^{2a} = |C_H| \). Therefore \( C_H = K(C_H) \) and so \( C_H \) is linear.

From Lemma 6, we have that \( rank(C_H) \geq 2 \) if \( a > 1 \). \( \Box \)

**Corollary 3** Let \( H = M_{\partial \phi(a, b)} \) be as in Example 1. Then \( ker(C_H) = 1 \).

**Proof** \( C_H \) is a nonlinear GHFP-code by Remark 1. \( \Box \)
Corollary 4 If \( q = 3^n \) with \( n > 1 \), \( H \) a GH matrix over \( \mathbb{F}_q \) where \( C_H \) is a nonlinear GHFP-code and \( H' = S_q \oplus H \). Then \( \text{rank}(C_{H'}) = \text{rank}(C_H) + 1 > \text{ker}(C_{H'}) = 2 \).

Proposition 6 [15, Theorem 6.9] Let \( \psi_i \in Z^2(G_i, U) \), \( 1 \leq i \leq n \) and \( \psi = \psi_1 \otimes \cdots \otimes \psi_n \in Z^2(G_1 \times \cdots \times G_n, U) \). Then \( \psi \) is orthogonal if and only if \( \psi_i \) is orthogonal, \( 1 \leq i \leq n \).

Remark 4 As a direct consequence of Proposition 6, the Sylvester generalized Hadamard matrix \( S^i \) is cocyclic.

Proposition 7 Let \( B_1 \) be a GH\((w, v/w)\) matrix over \( U \) and \( B_2 \) be a GH\((w, v'/w)\) matrix over \( U \). If \( C_{B_1} \) and \( C_{B_2} \) are GHFP-codes then \( C_H \) is a GHFP-code too where \( H = B_1 \oplus B_2 \).

Moreover,
\[
\pi_{a\oplus b}(x \oplus y) = \pi_a(x) \oplus \pi_b(y), \\
(a \oplus b)*(x \oplus y) = (a*x) \oplus (b*y)
\]
where \( a = (a_1, a_2, \ldots, a_v) \), \( b = (b_1, b_2, \ldots, b_{v'}) \) and \( a \oplus b = (a_1 + b_1, \ldots, a_1 + b_{v'}, a_2 + b_1, \ldots, a_2 + b_{v'}, \ldots, a_v + b_1, \ldots, a_v + b_{v'}) \) are rows in \( B_1 \), \( B_2 \) and \( H \), respectively; \( x \in C_{B_1} \) and \( y \in C_{B_2} \).

Proof By Corollary 2, we have that \( B_i = M_{\psi_i} \) for \( \psi_i \in Z^2(G_i, U) \) for a specific ordering of the elements of \( G_i \) (for the rest of this proof, we are assuming that this ordering in \( G_i \) is fixed) with \( i = 1, 2 \). Now, using Proposition 6, we have \( H = M_{\psi_1} \oplus M_{\psi_2} = M_{\psi_1 \otimes \psi_2} \) for \( \psi_1 \otimes \psi_2 \in Z^2(G_1 \otimes G_2, U) \) which is orthogonal, i.e., \( H \) is a cocyclic GH\((w, vv'/w)\). Therefore, by Proposition 3, \( C_H \) is a GHFP-code.

Now, assume that \( a \) (resp. \( b \)) corresponds with a row of \( B_1 \) (resp. \( B_2 \)) indexed with the element \( g \in G_1 \) (resp. \( h \in G_2 \)). By the proof of Proposition 3, we have \( \pi_a(l) = l \iff g_l = g_l \) and \( \pi_b(l) = j \iff h_m = h_j \), where \( g_j \in G_1 \) and \( h_j \in G_2 \). For the same reason, \( \pi_{a\oplus b}((l-1)v + m) = (i-1)v + j \iff (g_l, h_m) = (g, h)(g_i, h_j) \). Therefore, \( \pi_{a\oplus b}(x \oplus y) = \pi_a(x) \oplus \pi_b(y) \). Finally, as a direct consequence, we conclude with the desired result \( (a \oplus b)*(x \oplus y) = (a*x) \oplus (b*y) \).

Corollary 5 Let \( \partial \phi_{(a,b)} \) be as in Example 1 then \( C_H \) are not linear GHFP-codes with parameters \( (3^a(l+1)/3, 3^a(l+2)/3, 3^a(3^a-1)/3) \) where \( H = S^l \oplus M_{\phi(a,b)}, \) for \( l \geq 1 \), are GH\((3^a, 3^a/l)\) matrices with \( S = S_{3^a} \). Moreover, \( \text{ker}(H) = l + 1 < \text{rank}(H) \).

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 JJA(Spain). The second author was supported by the Catalan grant Borsa Ferran Sunyer i Balaguer and 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., Borges J., Rifà J.: Quasi-Hadamard full propelinear codes. Math. Comput. Sci. 12(4), 419–428 (2018).
2. Borges J., Mogilnykh I.Y., Rifà J., Solov’eva F.I.: Structural properties of binary propelinear codes. Adv. Math. Commun. 6(3), 329–346 (2012).
3. Borges J., Mogilnykh I.Y., Rifà J., Solov’eva F.: On the number of nonequivalent propelinear extended perfect codes. Electron. J. Combin. 20(2), 1–14 (2013).
4. Bosma W., Cannon J.J., Fieker C., Steel A.: Handbook of Magma Functions, Edition 2.22. Springer, Cham (2016).
5. Butson A.T.: Generalized Hadamard matrices. Proc. Am. Math. Soc. 13(6), 894–898 (1962).
6. Coulter R., Matthews R.: Planar functions and planes of Lenz–Barlotti class II. Des. Codes Cryptogr. 10(2), 167–184 (1997).
7. de Launey W., Flannery D.L.: Algebraic Design Theory. Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence (2011).
8. de Launey W., Flannery D.L., Horadam K.J.: Cocyclic Hadamard matrices and difference sets. Discrete Appl. Math. 102(1–2), 47–61 (2000).
9. Dougherty S.T., Rifà J., Villanueva M.: Ranks and kernels of codes from generalized Hadamard matrices. IEEE Trans. Inf. Theory 62(2), 687–694 (2016).
10. Drake D.A.: Partial λ-Geometries and generalized Hadamard matrices over groups. Can. J. Math. 31(3), 617–627 (1979).
11. Egan R., Flannery D.L.: Automorphisms of generalized Sylvester Hadamard matrices. Discrete Math. 340(3), 516–523 (2017).
12. Egan R., Flannery D.L., Ó Catháin P.: Classifying cocyclic Butson Hadamard matrices. In: Algebraic Design Theory and Hadamard Matrices. Springer Proceedings in Mathematics & Statistics, vol. 133. Springer, Cham, pp. 93–106 (2015).
13. Flannery D.L.: Cocyclic Hadamard matrices and Hadamard groups are equivalent. J. Algebra 192(2), 749–779 (1997).
14. Horadam K.J.: An introduction to cocyclic generalised Hadamard matrices. Discrete Appl. Math. 102(1–2), 115–131 (2000).
15. Horadam K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007).
16. Horadam K.J., Udaya P.: A new class of ternary cocyclic Hadamard codes. Appl. Algebra Eng. Commun. Comput. 14(1), 65–73 (2003).
17. Ito N.: On Hadamard groups II. J. Algebra 169(3), 936–942 (1994).
18. Perera A.A.I., Horadam K.J.: Cocyclic generalized Hadamard matrices and central relative difference sets. Des. Codes Cryptogr. 15(2), 187–200 (1998).
19. Phelps K.T., Rifà J.: On binary 1-perfect additive codes: some structural properties. IEEE Trans. Inf. Theory 48(9), 2587–2592 (2002).
20. Rifà J., Suárez E.: Hadamard full propelinear codes of type Q. Rank and kernel. Des. Codes Cryptogr. 86(9), 1905–1921 (2018).
21. Rifà, J., Basart, J.M., Huguet, L.: On completely regular propelinear codes. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS, vol. 357, pp. 341–355. Springer, Berlin (1989).
22. Shrikhande S.S.: Generalized Hadamard matrices and orthogonal arrays of strength two. Can. J. Math. 16, 736–740 (1964).

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