Generalized Hadamard full propelinear codes

José Andrés Armario*
Universidad de Sevilla, Sevilla, Spain
Ivan Bailera†
Universitat Autònoma de Barcelona, Bellaterra, Spain
Ronan Egan‡
National University of Ireland Galway, Galway, Ireland

June 17, 2019

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.

Keywords: Cocycles, generalized Hadamard matrices, difference sets, propelinear codes, rank, kernel.

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

*E-mail:armario@us.es
†E-mail:ivan.bailera@uab.cat
‡E-mail:ronan.egan@nuigalway.ie

1 Introduction

Let 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

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

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 $g \in G$. For any (normalized) map $\phi : G \to U$, the cocycle $\partial\phi$ defined by $\partial\phi(g,h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$ is a *coboundary*. The set of all cocycles $\psi : G \times G \to U$ 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_ψ 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_ψ and the set $T(\psi) = \{(1,g) : g \in G\}$ is a normalized transversal of $U \times \{1\}$ in E_ψ. 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_ψ: under some indexing of the rows and columns by G, M_ψ 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_ψ be a generalized Hadamard matrix $\mathrm{GH}(w, v/w)$ over U. We recall that a $v \times v$ matrix H with entries in U, where w divides v, is *a generalized Hadamard matrix* $\mathrm{GH}(w, v/w)$ if, for every i,j, $1 \le i < j \le v$, each of the multisets $\{h_{ik}h_{jk}^{-1} \mid 1 \le k \le v\}$ contains every element of U exactly v/w times. A $\mathrm{GH}(w, v/w)$ 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 vw 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 λ times, and contains no element of Z. Then R is called *a* (v,m,k,λ)*-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 1.1. *[12, Theorem 4.1] The following statements are equivalent.*

1. *$\psi \in Z^2(G, U)$ is orthogonal.*
2. *M_ψ is a (normalized) $\mathrm{GH}(w, v/w)$.*
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_ψ of U by G, relative to $U \times \{1\}$.*

Example 1.2. *[11, Example 9.2.1.4 and Theorem 9.48] Let G be the additive group of the finite field $\mathbb{F}_{3^a}$ and $\phi_{(a,b)}(g) = g^{(3^b+1)/2}$, $g \in G$ 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 $\mathrm{GH}(3^a, 1)$. Later, we will deal with $a = 4$ and $b = 3$.

Remark 1.3.
1. *Coulter and Mathews found $\phi_{(a,b)}$ as a new class of planar power functions over $\mathbb{F}_{3^a}$ (see [5]).*
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 [11, p.227]).*
3. *The orthogonal coboundaries $\partial\phi_{(a,b)}$ and $\partial\phi_{(a,2a-b)}$ determine equivalent Hadamard codes (see [10, Lemma 4.1]). Hence we may restrict to the range $3 \le b \le a - 1$.*

Let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, where p is prime. $\mathbb{F}_q$ is an additive elementary abelian group of order q. From H a normalized generalized Hadamard matrix $\mathrm{GH}(q, v/q)$ over $\mathbb{F}_q$, we denote by F_H the q-ary code consisting of the rows of H, and C_H the one defined as $C_H = \cup_{\alpha\in\mathbb{F}_q}(F_H + \alpha\mathbf{1})$ where $\mathbf{1}$ denotes the all-one vector (and $\alpha\mathbf{1}$ the all-α vector). The code C_H over $\mathbb{F}_q$ is called *generalized Hadamard code* which has qv codewords, length v and minimum distance $v - \frac{v}{q}$. 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 $\mathrm{GH}(2, 2t)$, where $U = \langle -1 \rangle$. In this case two further equivalences are known.

Proposition 1.4. *When $U = \langle -1 \rangle \cong \mathbb{Z}_2$, the equivalent statements of Theorem 1.1 are further equivalent to the following statements.*

4. *There is a Hadamard group E_ψ [9].*

5. *C_H is a Hadamard full propelinear code [15].*

Binary propelinear codes have been deeply studied in the literature, see [1, 2, 13, 14] among other references. The Hadamard full propelinear codes are an important family of this type of codes. However, aside from [3] not much has been done for q-ary propelinear codes, especially for the class of full propelinear codes. In this paper, we prove the analog of Proposition 1.4 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_ψ 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 ψ, then there is an extension group E_ψ. 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 $\mathbb{F}_q^n$. The elements of C are called *codewords.* A code C over $\mathbb{F}_q$ is called *linear* if it is a linear space over $\mathbb{F}_q$. The *minimum distance* of a code is the smallest Hamming distance between any pair of distinct codewords. Without loss of generality, we shall assume, unless stated otherwise, that the all-zero vector, denoted by $\mathbf{0}$, is in C.

Two structural properties of (nonlinear) codes are the rank and dimension of the kernel. The *rank* of a code C, $r = \mathrm{rank}(C)$, is the dimension of the linear span of C. The *kernel* of a q-ary code, denoted by $\mathcal{K}(C)$, is defined as $\mathcal{K}(C) := \{x \in \mathbb{F}_q^n : C + \alpha\, x = C \text{ for all}\, \alpha \in \mathbb{F}_q\}$. The p-kernel of C is defined as $\mathcal{K}_p(C) = \{x \in \mathbb{F}_q^n : C + x = C\}$. Note that $\mathcal{K}(C)$ is a linear subspace and $\mathcal{K}_p(C)$ is $\mathbb{F}_p$-additive. We will denote the dimension of the kernel of C by $k = \ker(C)$. 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 π and n permutations $\sigma_1, \dots, \sigma_n$ of $\mathbb{F}_q$. We denote by $\mathrm{Aut}(\mathbb{F}_q^n)$ the group of all isometries of $\mathbb{F}_q^n$:

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

where $\mathrm{Sym}\,\mathbb{F}_q$ and $\mathcal{S}_n$ denote, respectively, the symmetric group of permutations on $\mathbb{F}_q$ and on the set $\{1, \dots, n\}$.

For any $\sigma = (\sigma_1, \dots, \sigma_n)$ where $\sigma_i \in \mathrm{Sym}\,\mathbb{F}_q$, $\pi \in \mathcal{S}_n$ and $v \in \mathbb{F}_q^n$, $v = (v_1, \dots, v_n)$, we write $\sigma(v)$ and $\pi(v)$ to denote $(\sigma_1(v_1), \dots, \sigma_n(v_n))$ and $(v_{\pi^{-1}(1)}, \dots, v_{\pi^{-1}(n)})$, respectively.

The action of (σ, π) is defined as

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

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

$$(\sigma, \pi) \circ (\sigma', \pi') = ((\sigma_1 \circ \sigma'_{\pi^{-1}(1)}, \dots, \sigma_n \circ \sigma'_{\pi^{-1}(n)}), \pi \circ \pi') \text{ for all } (\sigma, \pi), (\sigma', \pi') \in \mathrm{Aut}(\mathbb{F}_q^n).$$

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 $\mathrm{Aut}(C)$ 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 automophism group of a matrix. Let K be a multiplicative group isomorphic to the additive elementary abelian group $\mathbb{F}_q$, and let $\phi : \mathbb{F}_q \to K$ be an isomorphism. *An automorphism of a matrix M* with entries in a 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 it's inverse in K, and matrix multiplication is carried out over the group ring $\mathbb{Z}[K]$. *The automorphism group* $\mathrm{Aut}(M)$ 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 $\mathrm{PAut}(M) \subset \mathrm{Aut}(M)$ comprised of all pairs of permutation matrices in $\mathrm{Aut}(M)$.

Lemma 2.1. *[6] 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 $\mathrm{Aut}(\phi(H))$ and certain isometries of C_H (elements of $\mathrm{Aut}(C_H)$). Let $(M,N) \in \mathrm{Aut}(\phi(H))$, $x = [[D_M]_{1,1}, \dots, [D_M]_{v,v}]$ and X be the $v \times v$ matrix such that each column is equal to x^T. It follows that $\phi(X+H) = D_M\phi(H)$. Likewise, if Y is a $v\times v$ matrix over $\mathbb{F}_q$ such that each row is equal to $y = [[D_N]_{1,1}, \dots, [D_N]_{v,v}]$, then $\phi(H-Y) = \phi(H)D_N^*$. So, $\phi(X+P_MHP_N^T-Y) = M\phi(H)N^* = \phi(H)$. Thus $X+P_MHP_N^T-Y = H$ and $(\sigma,\pi) \in \mathrm{Aut}(C_H)$ where $\sigma_i(u) = u + [D_N]_{ii}$ and $\pi(1,\dots,v) = (1,\dots,v)P_N$. We will say that (σ,π) is the isometry of C_H associated to the automorphism (M,N) of $\phi(H)$. Now, the following question arises naturally: Given an isometry (σ,π) of C_H, is it possible to define an automorphism (M,N) of $\phi(H)$ associated to (σ,π)? We will answer this question affirmatively in a particular case in the next section.

Definition 2.2. *[3] A q-ary code C of length n, $\mathbf{0} \in C$, is called* properlinear *if for any codeword $x \in C$ there exist $\pi_x \in \mathcal{S}_n$ and $\sigma_x = (\sigma_{x,1},\dots,\sigma_{x,n})$ with $\sigma_{x,i} \in \mathrm{Sym}\,\mathbb{F}_q$ satisfying:*

(i) for any $x \in C$ it holds $(\sigma_x,\pi_x)(C) = C$ and $(\sigma_x,\pi_x)(\mathbf{0}) = x$,

(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 the $\mathrm{Aut}(C)$ acts transitively on its codewords, i.e., the code satisfies the property (i) of the above definition.

For all $x \in C$ and for all $y \in \mathbb{F}_q^n$, denote by $\star$ the binary operation such that $x \star y = (\sigma_x,\pi_x)(y)$. Then, $(C,\star)$ is a group, which is not abelian in general. This group structure is compatible with the Hamming distance, that is, such that $d(x\star u, x\star v) = d(u,v)$ where $u,v \in \mathbb{F}_q^n$.

The vector $\mathbf{0}$ is always a codeword where $\pi_{\mathbf{0}} = Id_n$ is the identity coordinate permutation and $\sigma_{\mathbf{0},i} = Id_q$ is the identity permutation on $\mathbb{F}_q$ $\forall i$. Hence, $\mathbf{0}$ is the identity element in C and $\pi_{x^{-1}} = \pi_x^{-1}$ and $\sigma_{x^{-1},i} = \sigma^{-1}_{x,\pi_x(i)}$ for all $x \in C$ and for all $i \in \{1,\dots,n\}$. We also say that $(C,\star)$ is *a propelinear code.*

Clearly, the propelinear class is more general than the linear code class.

Proposition 2.3. *Let $(C,\star) \subset \mathbb{F}_q^n$ be a group. C is propelinear code if and only if the group* $\mathrm{Aut}(C)$ *(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 $\rho_x\rho_y(z) = \rho_x(y\star z) = x\star(y\star z) = (x\star y)\star z = \rho_{x\star y}(z)$. 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, $G = \{\rho_x \mid x \in G\}$ is a subgroup of $\mathrm{Aut}(C)$, 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 $\mathrm{Aut}(C)$ contains a regular subgroup G acting transitively on C, so $|G| = |C|$. We call ρ_x the element of G such that $\rho_x(\mathbf{0}) = x$. 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 $(\sigma_x, \pi_x) \in \mathrm{Aut}(C)$ because ρ_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 $x \star \mathbf{0} = \rho_x(\mathbf{0}) = x$ for any $x \in C$. As G acts transitively on C, we have $\rho_x\rho_y = \rho_{x\star y}$ if and only if $\rho_x\rho_y(\mathbf{0}) = \rho_{x\star y}(\mathbf{0})$. Let $x, y \in C$, then $\rho_{x\star y}(\mathbf{0}) = x \star y = \rho_x(y) = \rho_x(\rho_y(\mathbf{0})) = \rho_x\rho_y(\mathbf{0})$. Thus, $(\sigma_{x\star y}, \pi_{x\star y})(z) = \rho_{x\star y}(z) = \rho_x\rho_y(z) = \rho_x((\sigma_y, \pi_y)(z)) = (\sigma_x, \pi_x) \circ (\sigma_y, \pi_y)(z)$. $\square$

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* [14] if for each codeword $x \in C$ there exists $\pi_x \in \mathcal{S}_n$ satisfying the following conditions for all $y \in C$:

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

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

Furthermore, C is called *full propelinear* [15] if the permutation π_x has not any fixed coordinate when $x \neq \mathbf{0}$, $x \neq \mathbf{1}$; and if $\mathbf{1} \in C$ then $\pi_{\mathbf{1}} = Id_n$.

Definition 2.4. *A* full propelinear code *is a propelinear code C such that for every $a \in C$, $\sigma_a(x) = a + x$ and π_a has not any fixed coordinate when $a \neq \alpha\mathbf{1}$ for $\alpha \in \mathbb{F}_q$. Otherwise, $\pi_a = Id_n$.*

A generalized Hadamard code, which is also full propelinear, is called *generalized Hadamard full propelinear code* (briefly, GHFP-code). In the binary case, we have the Hadamard full propelinear codes, they were introduced in [15] and their equivalence with Hadamard groups was proven.

Lemma 2.5. *Let $(C, \star)$ 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 $b\star\lambda\mathbf{1} = b+\pi_b(\lambda\mathbf{1}) = b+\lambda\mathbf{1} = a$ and $a\star\lambda\mathbf{1} = \lambda\mathbf{1}\star a$. On the other hand, $\pi_a(x) = a\star x - a = (b\star\lambda\mathbf{1})\star x-(b+\lambda\mathbf{1}) = (b\star x)\star\lambda\mathbf{1}-(b+\lambda\mathbf{1}) = (b\star x)+\lambda\mathbf{1}-(b+\lambda\mathbf{1}) = b\star x - b = \pi_b(x)$, for all $x\in C$. □

Lemma 2.6. *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 $x = y + \lambda\mathbf{1},\ \lambda \in \mathbb{F}_q$. Furthermore, if $x, y \in F_H$ then $x = y$.*

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

Lemma 2.7. *Let C be a* GHFP*-code, $\Pi = \{\pi_x :\ x \in C\}$ and $C_1 = \{\lambda\mathbf{1}\colon \lambda \in \mathbb{F}_q\}$. Then $C_1 \subset K(C)$ and Π is isomorphic to C/C_1.*

Proof. It is immediate that $C_1 = \{\lambda\mathbf{1}\colon u\in\mathbb{F}_q\}$. The map $x\to\pi_x$ is a group homomorphism from C to Π. 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

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 isomporphic to the additive elementary abelian group $\mathbb{F}_q$, and let $\phi:\mathbb{F}_q\to K$ be an isomorphism. Write $\phi(H) = [\phi(h_{ij})]_{1\le i,j\le n}$.

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

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

($\rho_a\in\mathrm{Aut}(C_H)$) 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 π_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 $1\le i,j\le v$ and $0\le d\le q-1$, 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 k_d.

Thus (M,N) is an automorphism of $\phi(H)$, and if $a=\lambda\mathbf{1}$ for some $\lambda\in\mathbb{F}_q$, then the corresponding automorphism is of the form $(\phi(-\lambda)I,\phi(-\lambda)I)$. This proves the following.

Theorem 3.1. *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 $(C,\star)\cong R\subseteq \mathrm{Aut}(\phi(H))$. Moreover, $(kI,kI)\in R$ for all $k\in K$, and R acts transitively on rows of $\phi(H)$.*

Remark 3.2. *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, $\mathrm{Aut}(M)\cong \mathrm{PAut}(\mathcal{E}_M)$ where $\mathcal{E}_M=[k_ik_jM]_{0\leq i,j\leq q-1}$ (this is a special case of [6, Theorem 9.6.14]). Where $\Theta:\mathrm{Aut}(M)\to\mathrm{PAut}(\mathcal{E}_M)$ is the isomorphism outlined in [6, pp. 110–111]), we note that the center of $\mathrm{Aut}(M)$ contains the group of pairs of diagonal matrices $Z=\{(kI,kI):k\in K\}$, and thus $\Theta(Z)$ is a central subgroup of $\mathrm{PAut}(\mathcal{E}_M)$. We require that $\pi_{\lambda\mathbf{1}}=Id_n$ 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 3.3. *C is a generalized Hadamard full propelinear code if and only if there is a subgroup $R\subseteq\mathrm{Aut}(\phi(H))$ with $Z\subseteq R$ such that* $\mathrm{PAut}(\mathcal{E}_{\phi(H)})$ *contains a regular subgroup $\Theta(R)$, with $\Theta(Z)\subseteq\Theta(R)$.*

Proof. Let $K=\{1=k_0,\ldots,k_{q-1}\}$ and $Z=\{z_i=(k_iI,k_iI):i\in\{0,\ldots,q-1\}\}$ and let C be a generalized Hadamard full propelinear code. Theorem 3.1 gives that $(C,\star)\cong R\subseteq\mathrm{Aut}(\phi(H))$ 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 $\mathcal{E}_{\phi(H)}$ to row $iq+j$, proving that $\Theta(R)$ is transitive on rows of $\mathcal{E}_{\phi(H)}$. By Theorem 3.1, $|R|=|(C,\star)|$ and thus $\Theta(R)$ acts regularly.

Conversely, assuming that H is generalized Hadamard over $\mathbb{F}_q$ and that there is a subgroup $R\subseteq\mathrm{Aut}(\phi(H))$ with $Z\subseteq R$ such that $\Theta(R)\subseteq\mathrm{PAut}(\mathcal{E}_{\phi(H)})$ is regular and $\Theta(Z)\subseteq\Theta(R)$. Label the rows of $\mathcal{E}_{\phi(H)}$ 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 $\mathcal{E}_{\phi(H)}$ are the entries in the codeword labelling the row. For any $x\in C_H$ there is $(M_xN_x)\in\Theta(R)$ such that M_x sends row x to row 0. In the preimage of Θ, N_x corresponds to a monomial matrix $D_{-x}Q_x$. For each x, let π_x be coordinate the 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., π_x and σ_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, where $\lambda \in \mathbb{F}_q$, it follows that $(M_{\lambda \mathbf{1}}, N_{\lambda \mathbf{1}}) \in \Theta(Z)$, where $\pi_{\lambda \mathbf{1}} = Id_n$. Because $R \subseteq \mathrm{Aut}(\phi(H))$, 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 $z = (\sigma_z, \pi_z)(\mathbf{0}) = (\sigma_x, \pi_x)(\sigma_y, \pi_y)(\mathbf{0}) = (\sigma_x, \pi_x)(y)$ 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_ψ denote the canonical central extension of K by G obtained from ψ. The following is a special case of [6, Theorem 14.6.4].

Theorem 3.4. *A generalized Hadamard matrix H over K is cocyclic with cocycle ψ if and only if there exists a centrally regular embedding of E_ψ into $\mathrm{PAut}(\mathcal{E}_H)$.*

Corollary 3.5. *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 ψ, with extension group $E_\psi \cong R \cong (C_H, \star)$ where R is a regular subgroup of $\mathrm{PAut}(\mathcal{E}_H)$.*

Remark 3.6. *We observe that a generalized Hadamard matrix H may be cocyclic over several distinct cocycles ψ, and that the extension groups E_ψ 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_ψ and $(C_H, \star)$.

Assuming $\psi \in Z^2(G, K)$. For a fixed order 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 isomporphic to the additive elementary abelian group $\mathbb{F}_q$), we can define the following map:

$$\Phi \colon E_\psi \to K^v$$

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

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

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

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

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

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

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

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

Proposition 3.7. *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 $\pi_x \in \mathcal{S}_v$ where $\pi_x(y) = x \star y - x$. We know that every codeword has to be a multiple of a row of M_ψ. 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

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

Putting together,

$$\begin{aligned}
[\pi_x(y)]_j &= [x\star y]_j - [x]_j \\
&= \mu\psi(g^{-1},g)\psi(h^{-1},h)\left(\psi(g^{-1},h^{-1})\psi((hg)^{-1},hg)\right)^{-1}\psi(hg,g_j)(\psi(g,g_j))^{-1} \\
&= \mu\psi(h,gg_j).
\end{aligned}$$

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

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

Hence, the map π_x is an element of $\mathcal{S}_v$. Specifically, for any y, π_x moves the l-th coordinate of y to 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 π_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 it, let z be an element of C then

$$\begin{aligned} \pi_{x\star y}(z) &= (x \star y) \star z - x \star y \\ &= x \star (y \star z) - x \star y \\ &= x + \pi_x(y \star z) - \pi_x(y) - x \\ &= \pi_x(y \star z - y) = \pi_x(\pi_y(z)). \end{aligned}$$

□

Let H be a normalized Hadamard matrix $\mathrm{GH}(q, v/q)$ 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. $D_j = \cup_{\alpha \in \mathbb{F}_q} \{f + (-\alpha)\mathbf{1} : \ f \in F_H \ \wedge \ [f]_j = \alpha\}$.
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 $\mathrm{GH}(q, v/q)$ (over $\mathbb{F}_q$) too [11, Lemma 4.10]. Thus, the number of entries equal to α in the j-th column of H is v/q, for all $\alpha \in \mathbb{F}_q$.
4. $|D_j| = v$ and $C = \cup_{i \geq 1} D_i$.

Proposition 3.8. *Let* $(C, \star)$ *be a* GHFP*-code of length* v *over* $\mathbb{F}_q$ *coming from* H *a* $\mathrm{GH}(q, v/q)$*. Then* $F_H = D_1$ *is a (central) relative* $(v, q, v, v/q)$*-difference set in* C *relative to the normal subgroup* $C_1 = \{\alpha\mathbf{1} : \alpha \in \mathbb{F}_q\} \cong \mathbb{F}_q$.

Proof. C_1 is a central subgroup. We have to prove:

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

- 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 $x = \mathbf{0}$. 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 $[x + \alpha_0\mathbf{1}]_j = 0$. Since $(x + \alpha_0\mathbf{1}) \star f \in D_j$ for all $f \in F_H$ and $|y \star F_H| = v$ for all $y \in C_H$ then $(x + \alpha_0\mathbf{1}) \star F_H = D_j$. As a consequence,

$$x \star F_H = D_j - \alpha_0\mathbf{1}.$$

  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 conclude the proof.

□

Corollary 3.9. *Let $(C, \star)$ be a* GHFP*-code of length v over $\mathbb{F}_q$ coming from H a* $\mathrm{GH}(q, v/q)$*. Let $G = C/C_1$ and $\sigma(f \star C_1) = f$ for $f \in F_H$. The map $\psi_{F_H} \colon G \times G \to K$ defined by*

$$\psi_{F_H}(g, h) = k, \quad \textit{if} \sigma(g) \star \sigma(h) \in k\mathbf{1} \star F_H$$

is an orthogonal cocycle, i.e. $M_{\psi_{F_H}}$ is a $\mathrm{GH}(w, v/w)$*. Furthermore, $(C, \star) \cong E_{\psi_{F_H}}$ where $F_H^\star = \{(1, g) \colon g \in G\}$ is the isomorphic image of F_H.*

Proof. It is a consequence of [12, Theorem 3.1] and Proposition 3.8. □

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 [7] the study of the rank and dimension of the kernel of codes coming from generalized Hadamard matrices was initiated. We begin with a definition of an infinite family of cocyclic generalized Hadamard matrices.

Definition 4.1. [6, Section 9.2] Let $q = p^m$ be a prime power and denote the k-dimensional vector space over $\mathbb{F}_q$ by V. Then

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

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

It is well known that the generalized Sylvester matrices are cocyclic, see [11, p.122] for example. They were analyzed in terms of their cocyclic development in [8]. 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 $\mathrm{AGL}_{k+1}(V)$. Hence the matrix $H = D_{(p,m,k)}$ of order q^k is cocyclic with multiple cocycles ψ and has multiple non-isomorphic extension groups E_ψ of order q^{k+1}. As such, for each ψ 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 4.2. *If $G = U = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1\rangle \cong \mathbf{Z}_2^2$ (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, $\mathrm{GH}(4,1)$, 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 Π of permutations*

$$\pi_x = \begin{cases} I & x \in C_1 \\ (1,2)(3,4) & x \in C_2 \\ (1,3)(2,4) & x \in C_3 \\ (1,4)(2,3) & x \in C_4 \end{cases}$$

That is, $x \star y = x + \pi_x(y)$ where $(C, \star) \cong \mathbf{Z}_4^2$ and $\Pi \cong \mathbf{Z}_2^2$. The rank and the dimension of the kernel of this code are 2.

Example 4.3. *If $G = \mathbf{Z}_3^2$ 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 $\mathbf{Z}_3$*

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{pmatrix}$$

is a generalized Hadamard matrix (of Sylvester type), GH(3, 3)*, with entries in* $\mathbf{F}_3$*. The generalized Hadamard code over* G

$$C = C_1 \cup C_2 \cup \ldots \cup C_9$$

can be endowed with a **full propelinear structure** *with the following group* Π *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 $C \cong \mathbf{Z}_3^3$ *and* $\Pi \cong \mathbf{Z}_3^2$*. The rank and the dimension of the kernel of this code are 3.*

Example 4.4. *Let* $G = U = \mathbf{Z}_2^3$ *be with indexing* $\{0, 1, x, x^2, x^3, x^4, x^5, x^6\}$ *where*

$+$	*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		*0*	x^3	x^6	x	x^5	x^4	x^2
x			*0*	x^4	1	x^2	x^6	x^5
x^2				*0*	x^5	x	x^3	1
x^3					*0*	x^6	x^2	x^4
x^4						*0*	1	x^3
x^5							0	x
x^5								0

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, 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 **full propelinear structure** *with the following group* Π *of permutations*

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

We have $(C,\star) \cong \mathbf{Z}_4^3$ *and* $\Pi \cong \mathbf{Z}_2^3$*. The rank and the dimension of the kernel of this code are 2.*

Example 4.5. *Let* $G = U = \mathbf{Z}_3^4$ *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 1.2. Then the* G*-cocyclic matrix over* U

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

is a generalized Hadamard matrix, 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* Π *of permutations and the matrix* $[H]_{g,h}$ *can be downloaded from the following website (ddd.uab.cat/record/204295).*

We have that $(C,\star) \cong \mathbf{Z}_3^8$ *and* $\Pi \cong \mathbf{Z}_3^4$*. The rank of this 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 1.2. 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, fixed 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 were true, we would have an affirmative answer. For instance, for $a = 7$ we have two (cocyclic) 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.

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 1.2.

$b\backslash a$	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)

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 MAGMA [4]. We prove in Corollary 5.6 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 $\mathrm{GH}(3^a, 1)$ matrix as in Example 1.2. 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* [16] is a standard method to construct GH matrices from other GH matrices. That is, if $H = (h_{i,j})$ is any $\mathrm{GH}(w, v/w)$ matrix over U and $B_1,\ B_2, \ldots,\ B_v$ are any $\mathrm{GH}(w, v'/w)$ matrices over U then the matrix

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

is a $\mathrm{GH}(w, vv'/w)$ 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

$$(\psi \otimes \psi')((g,g'),(h,h')) = \psi(g,h)\psi(g',h'),$$

and $M_{\psi\otimes\psi'} = M_\psi \oplus M_{\psi'}$.

Let S_q be the normalized $\mathrm{GH}(q,1)$ matrix given by the multiplicative table of $\mathbb{F}_q$. We can recursively define S^t as a $\mathrm{GH}(q, q^{t-1})$ matrix, constructed as

$S^t = S_q \oplus S^{t-1}$ for $t > 1$, (this is an alternative definition for the generalized Sylvester Hadamard matrices). It is well-known that S_q is cocyclic (see [11, p. 122]) and $\mathrm{rank}(C_{S_q}) = \ker(C_{S_q}) = 2$.

Lemma 5.1. *[7, Lemma 3] Let H_1 and H_2 be two* GH *matrices over $\mathbb{F}_q$ and $H = H_1 \oplus H_2$. Then* $\mathrm{rank}(C_H) = \mathrm{rank}(C_{H_1}) + \mathrm{rank}(C_{H_2}) - 1$ *and* $\ker(C_H) = \ker(C_{H_1}) + \ker(C_{H_2}) - 1$.

Immediate consequences of the result above are that $\mathrm{rank}(C_{S^l}) = \ker(C_{S^l}) = l+1$. 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 5.2. *[7, Corollary 28] Let H be a* $\mathrm{GH}(q, q^{h-1})$ *matrix over $\mathbb{F}_q$, with $q > 3$ and $h \geq 1$, or $q = 3$ and $h \geq 2$. Then* $\mathrm{rank}(C_H) \in \{h+1, \dots, \lfloor q^h/2 \rfloor\}$.

Lemma 5.3. *[7, Proposition 9] Let H be a* $\mathrm{GH}(q, \lambda)$ *over $\mathbb{F}_q$, where $q = p^e$ and p prime. Let $v = q\lambda = p^t s$ such that* $\gcd(p, s) = 1$. *Then* $1 \leq \ker(C_H) \leq \ker_p(C_H) \leq 1 + t/e$.

Lemma 5.4. *Let C be a generalized full propelinear code. Then $\mathcal{K}(C)$ is a subgroup of C.*

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

Proposition 5.5. *Let H be a* $\mathrm{GH}(3^a, 1)$ *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* $\mathrm{rank}(C_H) \geq 2$.

Proof. From Lemma 5.3, we have that $\ker(C_H) \in \{1, 2\}$. We suppose that $\mathcal{K}(C_H) = \langle \mathbf{1}, x \rangle$, for some $x \in C_H$ with $x \neq \alpha \mathbf{1}$ for any $\alpha \in \mathbb{F}_{3^a}$. As the kernel is a linear subspace of C_H, we have that $\mathcal{K}(C_H) = \{\alpha \mathbf{1} + \beta x : \alpha, \beta \in \mathbb{F}_{3^a}\}$. Thus, $|\mathcal{K}(C_H)| = 3^{2a} = |C_H|$. Therefore $C_H = \mathcal{K}(C_H)$ and so C_H is linear.

From Lemma 5.2, we have that $\mathrm{rank}(C_H) \geq 2$ if $a > 1$. □

Corollary 5.6. *Let $H = M_{\partial \phi_{(a,b)}}$ be as in Example 1.2 then* $\ker(C_H) = 1$.

Proof. C_H is a nonlinear GHFP-code by Remark 1.3. □

Corollary 5.7. *If $q = 3^a$ with $a > 1$, H a* GH *matrix over $\mathbb{F}_q$ where C_H is a nonlinear* GHFP*-code and $H' = S_q \oplus H$. Then* $\mathrm{rank}(C_{H'}) = \mathrm{rank}(C_H) + 1 > \ker(C_{H'}) = 2$.

Proposition 5.8. *[11, 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 ψ is orthogonal if and only if ψ_i is orthogonal, $1 \leq i \leq n$.*

Remark 5.9. *As a direct consequence of Proposition 5.8, the Sylvester generalized Hadamard matrix S^l is cocyclic.*

Proposition 5.10. *Let B_1 be a $\mathrm{GH}(w, v/w)$ matrix over U and B_2 be a $\mathrm{GH}(w, v'/w)$ 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,*

$$\pi_{a\oplus b}(x \oplus y) = \pi_a(x) \oplus \pi_b(y),$$
$$(a \oplus b) \star (x \oplus y) = (a \star x) \oplus (b \star y).$$

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 3.9, 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 fixed this ordering in G_i) with $i = 1, 2$. Now, using Proposition 5.8, 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 $\mathrm{GH}(w, vv'/w)$. Therefore, by Proposition 3.7, 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 3.7, we have $\pi_a(l) = i \Leftrightarrow g_l = gg_i$ and $\pi_b(m) = j \Leftrightarrow h_m = hh_j$, where $g_j \in G_1$ and $h_j \in G_2$. For the same reason, $\pi_{a\oplus b}((l-1)v + m) = (i-1)v + j \Leftrightarrow (g_l, h_m) = (g, h)(g_i, h_j)$. 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 $(a \oplus b) \star (x \oplus y) = (a \star x) \oplus (b \star y)$. ☐

Corollary 5.11. *Let $\partial\phi_{(a,b)}$ be as in Example 1.2 then C_H are not linear GHFP-codes where $H = S^l \oplus M_{\partial\phi_{(a,b)}}$, for $l \geq 1$, are $\mathrm{GH}(3^a, 3^{al})$ matrices with $S = S_{3^a}$. Moreover, $\ker(H) = l + 1 < \mathrm{rank}(H)$.*

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 JJAA (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**, 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. Electronic J. Combinatorics **20**, 1–14 (2013).

[4] Bosma, W., Cannon, J.J., Fieker, C., Steel, A.: Handbook of Magma functions, Edition 2.22 (2016).

[5] Coulter, R., Matthews, R.: Planar functions and planes of Lenz-Barlotti class II. Des. Codes and Cryptogr. **10**, 167–184 (1997).

[6] de Launey, W., Flannery, D.L.: Algebraic design theory. Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence, RI (2011).

[7] Dougherty, S.T., Rifà, J., Villanueva, M.: Ranks and kernels of codes from generalized Hadamard matrices. IEEE trans. Inf. Theory **62**, 687–694 (2016).

[8] Egan, R., Flannery, D.L.: Automorphisms of generalized Sylvester Hadamard matrices, Discrete Math. **340**(3), 516–523 (2017).

[9] Flannery, D.L.: Cocyclic Hadamard matrices and Hadamard groups are equivalent. J. Algebra **192**, 749–779 (1997).

[10] Horadam, K.J., Udaya, P.: A new class of ternary cocyclic Hadamard codes. Applic. Algebra En. Commun. Comp. **14**, 65–73 (2003).

[11] Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ (2007).

[12] Perera, A.A.I., Horadam, K.J.: Cocyclic generalized Hadamard matrices and central relative difference sets. Des. Codes Cryptogr. **15**, 187–200 (1998).

[13] Phelps, K. T., Rifà, J.: On binary 1-perfect additive codes: some structural properties. IEEE Trans. Inf. Theory **8**, 2587–2592 (2002).

[14] Rifà, J., Basart, J.M., Huguet, L.: On completely regular propelinear codes. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS 357, pp. 341–355. Springer, Berlin (1989).

[15] Rifà, J., Suárez, E.: Hadamard full propelinear codes of type Q. Rank and kernel. Des. Codes Cryptogr. **86**, 1905âĂŞ-1921 (2018).

[16] Shrikhande, S.S.: Generalized Hadamard matrices and orthogonal arrays of strength two. Can. J. Math. **16**, 736–740 (1964).