Quasi-Hadamard Full Propelinear Codes

José Andrés Armario · Iván Bailera ·
Joaquim Borges · Josep Rifà

Abstract: In this paper, we give a characterization of quasi-Hadamard groups in terms of propelinear codes. We define a new class of codes that we call *quasi-Hadamard full propelinear codes*. Some structural properties of these codes are studied and examples are provided.

Keywords Cocycles · Quasi-orthogonal · Quasi-Hadamard groups · Propelinear codes

1 Introduction

The Hadamard (maximal) determinant problem asks for the largest $n \times n$ determinant with entries ± 1. This is an old question which remains unanswered in general. Throughout this paper, for convenience, when we say determinant of a matrix we mean the absolute value of the determinant. Let M be a $(-1, 1)$-matrix of order n. We call M a *D-optimal design* if the determinant of M is the maximum determinant among all $(-1, 1)$-matrices of order n, (i.e., $\det(M)$ is a solution of the Hadamard determinant problem). Hadamard showed in [8] that $n^{n/2}$ was an upper bound for the determinant of an $n \times n$ D-optimal design. This bound can be attained only if $n = 1, 2$ or n is a multiple of 4. A matrix that attains it is called a *Hadamard matrix*, and it is an outstanding conjecture that one exists for any multiple of 4. Hadamard's inequality can be improved if we restrict to matrices whose orders are not divisible by

J. A. Armario (✉)
Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n, 41012 Sevilla, Spain
e-mail: armario@us.es

I. Bailera · J. Borges · J. Rifà
Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain
e-mail: ivan.bailera@uab.cat

J. Borges
e-mail: joaquim.borges@uab.cat

J. Rifà
e-mail: josep.rifa@uab.cat

4. Indeed, if $n \equiv 2 \mod 4$ and $n \neq 2$, Ehlich [5] and independently Wojtas [17] proved that

$$\det(M) \leq (2n-2)(n-2)^{\frac{1}{2}n-1}, \tag{1.1}$$

and, moreover, there exists a $(-1, 1)$-matrix achieving equality in (1.1) if and only if there exists a $(-1, 1)$-matrix B of order n such that

$$BB^\top = B^\top B = \begin{bmatrix} L & 0 \\ 0 & L \end{bmatrix}, \tag{1.2}$$

where $L = (n-2)I + 2J$. The symbols I and J will (respectively) always denote the identity matrix and the all-ones matrix; the order of each matrix will be clear from the context in which it is used. A $(-1, 1)$-matrix of order n is called an *EW matrix* if it satisfies (1.2) (or more generally, when its determinant reaches the bound in (1.1)). Clearly Hadamard matrices and EW matrices are D-optimal designs. Note that it is known that EW matrices exist only if $2(n-1)$ is the sum of two squares, a condition which is believed to be sufficient (order 138 is the lowest for which the question has not been settled yet, [7]). The interested reader is addressed to [12] and the website [13] for further information on what is known about maximal determinants.

Example 1.1 The following matrix is a EW matrix of order 10.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1
\end{pmatrix}. \tag{1.3}$$

In the early 1990s, de Launey and Horadam discovered *cocyclic development of pairwise combinatorial designs*. This discovery opened up a new area in design theory, that emphasizes algebraic methods drawn mainly from group theory and cohomology. Cocyclic construction has been successfully used for Hadamard matrices [9] and, more recently, for EW matrices [1,2]. In this context, the notions of orthogonal (resp. quasi-orthogonal) cocycles associated to cocyclic Hadamard (resp. EW) matrices arose naturally.

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

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

is a *cocycle* (*over* G, *with coefficients in* U). We may assume that ψ is normalized, i.e., $\psi(1,1) = 1$. 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.

Example 1.2 [11, Chapter 2] Suppose that E is a finite group with normalized transversal T for a central subgroup $U = \langle -1 \rangle \cong \mathbb{Z}_2$ (i.e. $|xT \cap yU| = 1$ for any $x, y \in E$). Put $G = E/\langle -1 \rangle$ and $\sigma(t\langle -1 \rangle) = t$ for $t \in T$. The map $\psi_T : G \times G \to \langle -1 \rangle$ defined by

$$\psi_T(g,h) = \sigma(g)\sigma(h)\sigma(gh)^{-1} = \begin{cases} 1 & \sigma(g)\sigma(h) \in T, \\ -1 & \text{otherwise} \end{cases}$$

is a cocycle.

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). Our principal focus in this paper is the case $U = \langle -1 \rangle \cong \mathbb{Z}_2$. We say that ψ is *orthogonal* if M_ψ is a Hadamard matrix, i.e., $M_\psi M_\psi^\top = M_\psi^\top M_\psi = nI_n$ where $n = |G|$. Similarly, for $n \equiv 2 \mod 4$ we say that ψ is *quasi-orthogonal* if M_ψ satisfies

$$\operatorname{abs}(M_\psi M_\psi^\top) = \begin{bmatrix} L & 0 \\ 0 & L \end{bmatrix} \tag{1.4}$$

up to row permutation. Where $\operatorname{abs}(M)$ denotes the matrix $[|m_{i,j}|]$ for $M = [m_{i,j}]$. By (1.2) it follows that any cocyclic EW matrix is quasi-orthogonal, but, the reciprocal does not hold (i.e., not every quasi-orthogonal cocyclic matrix is an EW matrix). Moreover, [3, Remark 6] claims that if ψ is quasi-orthogonal then $M_\psi M_\psi^\top = M_\psi^\top M_\psi$.

When $|G| = 4t + 2$ and $\psi \in Z^2(G, \langle -1 \rangle)$ is a coboundary then the identity (1.4) never holds [3, Prop 2.5.]. We say that ψ *is a quasi-orthogonal coboundary* if M_ψ satisfies

$$\operatorname{abs}(M_\psi M_\psi^\top) = L. \tag{1.5}$$

up to row permutation. As far as we are aware, quasi-orthogonal coboundaries are only known over abelian groups and the dihedral group of six elements. In this case, $M_\psi M_\psi^\top = M_\psi^\top M_\psi$.

The paper [4] describes the link between orthogonal cocyles and other combinatorial objects. For example, we can use an orthogonal cocycle to construct a relative difference set with forbidden subgroup $\mathbb{Z}_2$ in a central extension of $\mathbb{Z}_2$ by G, and vice versa. Such extensions, known as *Hadamard groups*, were studied by Ito in a series of papers beginning with [10]. Their equivalence with cocyclic Hadamard matrices was demonstrated in [6]. There is a further equivalence with class regular group divisible designs on which the Hadamard group acts as a regular group of automorphisms. Finally, in [15] a surprising characterization is given, now, in terms of a class of Hadamard propelinear codes. Techniques and results have been translated fruitfully between the different contexts.

Recently, a study of the existence, classification and combinatorics of quasi-orthogonal cocycles has been started in [3]. For instance, equivalences with quasi-Hadamard groups, relative quasi-difference sets, and certain partially balanced incomplete block designs, afforded by the analogy with orthogonal cocycles, have been found.

Keeping with the analogy, in this paper we give a characterization of quasi-orthogonal cocyles in terms of propelinear codes. Furthermore, some structural properties of these codes are studied.

2 Propelinear Codes

Let $\mathbb{F}$ be the binary field. The *Hamming distance* between two vectors $v, w \in \mathbb{F}^n$, denoted by $d(v, w)$, is the number of the coordinates in which v and w differ. The *Hamming weight* of v is given by $\mathrm{wt}(v) = d(v, e)$, where e is the all-zeros vector. A (n, M, d)*-code* is a subset, C, of $\mathbb{F}^n$ such that $|C| = M$ and $d(v, w) \geq d$ for all $v, w \in C$ with $v \neq w$. The elements of a code are called *codewords* and d is called *minimum distance*. The parameter d determines the error-correcting capability of C which is given by $\lfloor \frac{d-1}{2} \rfloor$.

Two structural properties of binary codes are the rank and dimension of the kernel. The *rank* of a binary code C, $r = rank(C)$, is the dimension of the linear span of C. The *kernel* of a binary code is the set of words which keeps the code invariant by translation, $K(C) := \{v \in \mathbb{F}^n : C + v = C\}$. Note that the kernel of a binary linear code C is not the same that the dual code of C, which is the kernel of the generator matrix of C. Assuming the zero vector is in C we have that $K(C)$ is a linear subspace. 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. When a code is linear, the rank and the dimension of the kernel are equal to the dimension of the code. In some sense, these two parameters give information about the linearity of a code.

Let $\mathcal{S}_n$ be the symmetric group of permutations of the set $\{1, \dots, n\}$. For any $\pi \in \mathcal{S}_n$ and $v \in \mathbb{F}^n$, $v = (v_1, \dots, v_n)$, we write $\pi(v)$ to denote $(v_{\pi^{-1}(1)}, \dots, v_{\pi^{-1}(n)})$.

Definition 2.1 ([14]) A binary code C of length n has a *propelinear structure* 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) $\pi_x \pi_y = \pi_{x+\pi_x(y)}$.

For all $x \in C$ and for all $y \in \mathbb{F}^n$, denote by $\star$ the binary operation such that $x \star y = x + \pi_x(y)$. Then, $(C, \star)$ is a group, which is not abelian in general. The vector e is always a codeword and π_e is the identity permutation. Hence, e is the identity element in C and $x^{-1} = \pi_x^{-1}(x)$, for all $x \in C$. We call $(C, \star)$ a propelinear code. Let $\mathcal{G}$ be the semi-direct product $(\mathbb{F}^n, +) \wr S_n$ (i.e. an n-dimensional $\mathbb{F}$-vector space with the natural action of S_n on coordinates.) A propelinear code is a subgroup of $\mathcal{G}$ which intersects the base group $(\mathbb{F}^n, +)$ in a subgroup of order 2 (but has larger projection onto the base group), and has a transitive projection onto the top group S_n.

Definition 2.2 ([15]) A full propelinear code is a propelinear code C such that for every $a \in C$, $a \neq e$, $a \neq u$, the permutation π_a has not any fixed coordinate, $\pi_e = Id$, and if $u \in C$ then $\pi_u = Id$ where u is the all-ones vector.

The code consisting of the rows of a binary Hadamard matrix and their complements is called a Hadamard code, which has $8t$ codewords, length $4t$ and minimum distance $2t$.

A Hadamard code, which is also full propelinear, is called *Hadamard full propelinear code*. They were introduced in [15] and the equivalence with Hadamard groups was proven.

3 The Main Result

In this section we introduce the notion of quasi-Hadamard full propelinear codes and their equivalence with quasi-Hadamard groups is studied.

A $(-1, 1)$-matrix is said to be normalized if all entries in its first row and column are equal to 1.

Definition 3.1 A quasi-Hadamard matrix is a normalized square $(-1, 1)$-matrix M of order $4t+2$ with the property such that

$$\mathrm{abs}(MM^\top) = \mathrm{abs}(M^\top M) = \begin{bmatrix} L & 0 \\ 0 & L \end{bmatrix} \tag{3.1}$$

up to row and column permutation, where $L = 4tI + 2J$.

Clearly, EW matrices are quasi-Hadamard matrices but not every quasi-Hadamard matrix is a D-optimal design. In Definition 3.1, M is said to be an *extremal* quasi-Hadamard matrix when $\mathrm{abs}(MM^\top) = \mathrm{abs}(M^\top M) = L$, where $L = 4tI + 2J$.

The matrix obtained from a quasi-Hadamard matrix, by replacing all 1's by 0's and all -1's by 1s, is called *binary quasi-Hadamard matrix*. The binary code consisting of the rows of a binary quasi-Hadamard matrix and their complements is called a *quasi-Hadamard* code, which is of length $4t + 2$ and with $8t + 4$ codewords. Since M is normalized e (the all-zeros vector) and u (the all-ones vector) are always codewords.

Proposition 3.2 *The minimum distance of a quasi-Hadamard code C of length $4t + 2$ is $2t$.*

Proof By (1.4), the inner product $x \cdot y$ is 0 or ± 2, where x, y are different rows of M (a binary quasi-Hadamard matrix associated to C). If $x \cdot y = 0$ then $d(x, y) = 2t + 1$, if $x \cdot y = 2$ then $d(x, y) = 2t$, and if $x \cdot y = -2$ then $d(x, y) = 2t + 2$. As $d(x, y) = 4t + 2 - d(x, y + u)$, then $d(x, y) \in \{2t, 2t + 1, 2t + 2, 4t + 2\}$ for any $x \neq y \in C$. □

The set of distances in a quasi-Hadamard code of length $4t+2$ is the same as in a Hadamard code of length $4t+4$ after puncturing two coordinates. The number of codewords in the above codes is $8t+4$ and $8t+8$, respectively. Hence, from an error-correction point of view it is slightly better the 2-punctured Hadamard code. However, quasi-Hadamard codes can be seen as a good alternative to 2-punctured Hadamard codes in that cases when we do not know about the existence of a Hadamard code of length $4t+4$.

From a Hadamard code we can always obtain a quasi-Hadamard code by puncturing twice. Let say M is a normalized Hadamard matrix of length n and fix any two different columns (also different from the first one). It is well known the design structure of M and so, in this case, the projection of the row vectors of M over these two fixed coordinates gives exactly $n/4$ times each one of the vectors $(1,1)$, $(-1,-1)$, $(-1,1)$, $(1,-1)$. Puncturing these fixed two columns and removing any pair of rows such that its projection over the two punctured coordinates give two orthogonal vectors, we obtain a quasi-Hadamard matrix. However, the reciprocal is not true. It is easy to see that the quasi-Hadamard matrix in Eq. (1.3) could not be extended to a Hadamard matrix. Indeed, adding two columns to that matrix the two coordinates added to the second row should be $(1,1)$ to have this row orthogonal to the first one; also the two coordinates added to the third row should be $(1,1)$ to have this row orthogonal to the first one; but now the new second and third rows are not orthogonal.

An interesting bound which Hadamard codes fit is the so called Grey-Rankin bound, applicable only to self-complementary codes to check its optimality. The quasi-Hadamard codes do not attain this bound. For a (n,M,d)-code the bound states that

$$M \leq \frac{8d(n-d)}{n-(n-2d)^2}$$

and in the case of the quasi-Hadamard code, we have a $(4t+2, 8t+4, 2t)$-code which is almost optimal taking into account the Grey-Rankin bound as it is easy to see. The left part of the inequality is $M = 8t+4$ and the right part is $8t+4+(8+\frac{12}{2t-1})$.

A quasi-Hadamard code, which is also full propelinear, is called *quasi-Hadamard full propelinear code*. Now we present the analogous of a result which is proven for Hadamard codes in [16, Lemma 3.11]. We note that the same proof is valid for quasi-Hadamard codes.

Lemma 3.3 *Let C be a quasi-Hadamard code of length $4t+2$. The rank r of C fulfills $r \leq \frac{8t+4}{2^k}+k-1$, where k is the dimension of the kernel.*

Henceforth, we will assume that E is a finite (multiplicatively written) group of order $2n$ with identity e and normalized transversal T for a central subgroup $\langle u\rangle \cong \mathbb{Z}_2$. We recall that this implies in particular that:

- T and uT are disjoints and $T \cup uT = E$.
- aT and $\{b, bu\}$ intersect exactly in one element, for any $a, b \in E$.

Now, we state a technical result that we will need later.

Lemma 3.4 *Let $a, b \in E$ and $A = [T \backslash (a(T \cup bT) \cap T)] \cup [a(T \cap bT) \cap T]$. Then,*

1. *$x \in T \cap bT \Rightarrow$ either $ax \in A$ or $axu \in A$.*
2. *$x \in A \Rightarrow$ either $a^{-1}x \in T \cap bT$ or $a^{-1}xu \in T \cap bT$.*

As a consequence, we have $|T \cap bT| = |A|$.

Proof 1. $x \in T \cap bT \Rightarrow ax \in a(T \cap bT)$. Now, we have to possibilities:

1.1. if $ax \in T$ then $ax \in a(T \cap bT) \cap T$. Thus, $ax \in A$.
1.2. if $ax \notin T$ then $axu \in T$. Taking into account that $ax \in aT \wedge ax \in abT$ and T is a transversal (the second property above), we have $axu \notin aT \cup abT$. Thus, $axu \in T \backslash (a(T \cup bT) \cap T)$. Hence, $axu \in A$.

2. Follows by a similar argument.

□

For a fixed order in $T = \{t_1 = e, t_2, \ldots, t_n\}$ and given an element $a \in E$, we can define a n-vector $v_a \in \mathbb{F}^n$ in the following manner:

$$[v_a]_k = \begin{cases} 0 & a^{-1}t_k \in T, \\ 1 & \text{otherwise} \end{cases}$$

where $[v_a]_k$ denotes the k-th coordinate of v_a and $C_E = \{v_a \in \mathbb{F}^n : a \in E\}$. Let us point out that v_e is the all-zeros vector and v_u is the all-ones vector.

The next result follows immediately.

Lemma 3.5 *Let $b \in E$, the set of positions where the vector v_b has a* 0 *entry is given by $T \cap bT$ (i.e., $t_k \in T \cap bT \Leftrightarrow [v_b]_k = 0$).*

In the sequel our main goal will be to endow C_E with a propeline structure using the transversal T, the central subgroup $\langle u \rangle$ and the law group of E. The first step consists of finding a suitable permutation $\pi_{v_a} \in \mathcal{S}_n$ associated to an element $a \in E$. For any $b \in E$ define $\pi_{v_a}(v_b) = v_a + v_{ab}$ where $+$ is the componentwise addition in $\mathbb{F}^n$. At this moment, it is not obvious that $\pi_{v_a}(v_b)$ has the same weight as v_b and even if it did, this might not define a unique permutation. Before trying to clarify this point, we will point out that if $\pi_{v_a} \in \mathcal{S}_n$ for any $a \in E$ then $(C_E, \star)$ with $v_a \star v_b = v_a + \pi_{v_a}(v_b)$ is isomorphic to E as a group since $v_a \star v_b = v_{ab}$ by the definition of π_{v_a}. Furthermore,

Lemma 3.6 *Let $a, b \in E$ then $\pi_{v_a}\pi_{v_b} = \pi_{v_a \star v_b}$.*

Proof For any $c \in E$, we have

$$\begin{aligned} \pi_{v_a \star v_b}(v_c) &= \pi_{v_{ab}}(v_c) = v_{ab} + v_{(ab)c} = v_a + \pi_{v_a}(v_b) + v_{a(bc)} \\ &= v_a + \pi_{v_a}(v_b) + v_a + \pi_{v_a}(v_{bc}) = \pi_{v_a}(v_b + v_{bc}) = \pi_{v_a}\pi_{v_b}(c) \end{aligned}$$

□

By abuse of notation, from now on we will use the same symbol a to denote v_a. Similarly, for the underlying set of the group E and C_E. The meaning of a (resp. E) will be clear from the context in which it is used.

In the sequel, for any $a, b \in E$ some properties of the map $\pi_a(b)$ (defined above) are studied.

Lemma 3.7 *Let a, b and A as in Lemma 3.4. Then,* $[\pi_a(b)]_k = \begin{cases} 1 & t_k \notin A, \\ 0 & t_k \in A. \end{cases}$

Proof To check the value of the k-th coordinate of $\pi_a(b)$, we have to compute $[a]_k + [ab]_k \mod 2$. Therefore, $[\pi_a(b)]_k = 0$ if and only if $[a]_k = [ab]_k$. Now, applying the definition of $[a]_k$ and Lemma 3.4, we conclude with the desired result. □

Taking into account $|A| = |T \cap bT|$ and Lemmas 3.5 and 3.7, it is proved that $\pi_a(b)$ has the same weight as b. Moreover, the following result guarantees the π_a is a permutation depending only on a.

Proposition 3.8 *The map π_a is an element of $\mathcal{S}_n$. Specifically, for any b, π_a moves the k-th coordinate of b to the h-th coordinate where*

$$t_h = \begin{cases} at_k & at_k \in T, \\ at_k u & \textit{otherwise}. \end{cases}$$

Proof We have that $[\pi_a(b)]_h = [a]_h + [ab]_h \mod 2$. It is straightforward to check that $[\pi_a(b)]_h = [b]_k$. □

Remark 3.9 Let us observe that $at_k = t_h$ if $a = e$ and $at_k u = t_h$ if $a = u$. Hence, the permutation π_a does not fix any coordinate for all $a \in E \backslash \{e, u\}$ and $\pi_e = \pi_u = Id$.

We can always assume without loss of generality that the elements of T are ordered in such a way so, $\pi_{t_k}(e_k) = e_1$ where e_k is the unitary vector with only one nonzero coordinate at the position k-th. A justification of the fact that $\pi_a(e_k) \neq \pi_b(e_k)$ for all $a, b \in T$ with $a \neq b$ is given in the proof of Theorem 3.13.

It is known [16] that if E is a Hadamard group then the permutations of Proposition 3.8 yields a full propeline structure on the Hadamard code C_E. From now on, we will deal with the case E being a quasi-Hadamard group and we will obtain the analog result.

Definition 3.10 ([3]) Let E be a group of order $8t+4 \geq 12$ with central subgroup $Z = \langle u \rangle \cong \mathbb{Z}_2$. We say that E is a quasi-Hadamard group if there exists a transversal T for Z in E of size $4t+2$ containing a subset $S \subset T \backslash Z$ of size $2t+1$ such that

$$|T \cap xT| = \begin{cases} 2t+1 & x \in S, \\ 2t \text{ or } 2t+2 & x \in T \backslash (S \cup Z). \end{cases} \tag{3.2}$$

The transversal T is called a *quasi-Hadamard subset* of E. It may be assumed that $e \in T$.

Armario and Flannery [3, Thm 3.2] shows that quasi-orthogonal cocycle and quasi-Hadamard group are essentially the same concept.

Let Q_{8t+4} denote the dicyclic group with presentation

$\langle a, b \mid a^{2t+1} = b^2,\ b^4 = e,\ b^{-1}ab = a^{-1} \rangle$

This family provides good candidates for quasi-Hadamard groups. For instance, $T = \{e, a, a^2, b, ab, a^2b\}$ is a quasi-Hadamard subset of Q_{12}. Furthermore, in [3] it has been conjectured that Q_{8t+4} is always a quasi-Hadamard group. It can be seen as the analog of Ito's conjecture for Hadamard groups.

We say that a quasi-Hadamard group E is *extremal* when in Definition 3.10 $S = \emptyset$. Quasi-orthogonal coboundary and extremal quasi-Hadamard group are also essentially the same concept.

Proposition 3.11 *Let E be a quasi-Hadamard group and $T = \{t_1 = e, t_2, \ldots, t_n\}$ be a quasi-Hadamard subset of E. Then E is a quasi-Hadamard code with*

$$[H(T)]_{i,j} = \begin{cases} 0 & t_i^{-1}t_j \in T, \\ 1 & \textit{otherwise} \end{cases}$$

as a binary quasi-Hadamard matrix (up to normalization).

Proof Let us point out that the codewords of E are the rows of the following (0, 1)-matrices $H(T)$ and $\overline{H(T)}$ where $H(T) + \overline{H(T)} = J$.

Let $\psi_T \in Z^2(E/\langle u \rangle,\ \langle -1 \rangle)$ be as in Example 1.2. By [3, Thm 3.2],

$$[M_{\psi_T}]_{i,j} = \begin{cases} 1 & t_i t_j \in T, \\ -1 & \text{otherwise} \end{cases}$$

is a quasi-orthogonal cocyclic matrix. Hence, the matrices M_{ψ_T} and $M_{\psi_T}^{\top}$ satisfies (1.4).

Now, let us observe that the binary version of M_{ψ_T} is equivalent to $H(T)$. Normalizing (i.e., taking the complement of the rows starting by 1 in $H(T)$) we get the binary version of M_{ψ_T} up to rows permutation, due to the fact that if $a \in E$ then $a \in T$ or $au \in T$ and v_a is the complement of v_{au}. Therefore, E is a quasi-Hadamard code with $H(T)$ as a binary quasi-Hadamard matrix up to normalization. □

Now, we can define a propelinear structure on E by $a \star b = a + \pi_a(b) = ab$. Finally, as an immediate consequence of the previous results above. We have,

Theorem 3.12 *Let E be a quasi-Hadamard group and $T = \{t_1 = e, t_2, \ldots, t_n\}$ be a quasi-Hadamard subset of E. Then $(E, \star)$ is a quasi-Hadamard full propelinear code.*

Proof From 3.11, we have that E is a quasi-Hadamard code. Now, let's see that E has a propelinear structure. For each $x \in E$, we define $\pi_x(y) = x + xy$ for any $y \in E$. From 3.8, $\pi_x \in S_n$ for every $x \in E$. For any $x, y \in E$, $x + \pi_x(y) = x + x + xy = xy \in E$, and by 3.6 $\pi_x \pi_y = \pi_{xy} = \pi_{x+\pi_x(y)}$. Thus $(C, \star)$ is a propelinear code, which is full by 3.9. □

In the next result, we will show that the converse statement holds. An analogous version for Hadamard full propelinear codes appears in [15].

Theorem 3.13 *Let E be a quasi-Hadamard full propelinear code of length $4t+2$. Then E is a quasi-Hadamard group of order $8t+4$.*

Proof Define T_1 to be the subset of E consisting of codewords with first coordinate equal to zero. It is easy to check that

- $T_1 \cap uT_1 = \emptyset$ and $T_1 \cup uT_1 = E$.
- aT_1 and $\{b, bu\}$ intersect exactly in one element, for any $a, b \in E$.
- $\langle u \rangle \cong \mathbb{Z}_2$ is a central subgroup of E.

We associate to each codeword in $x \in T_1$, the integer k_x such that $\pi_x^{-1}(e_1) = e_{k_x}$. Let us point out that if $x, y \in T_1$ and $x \neq y$ then $k_x \neq k_y$. Indeed, if $k_x = k_y$ then $e_1 = \pi_x \pi_y^{-1}(e_1) = \pi_x \pi_{y^{-1}}(e_1) = \pi_{xy^{-1}}(e_1)$. Now, taking into account that E is full then $xy^{-1} = e$ or $xy^{-1} = u$. Hence, $x = y$ or $\{x, y\}$ is not a subset of T_1. As a consequence, k_x ranges over all the integers between 1 and $4t+2$ when x moves in T_1.

Let H be the binary quasi-Hadamard matrix associate to E where the k_x-th row of H corresponds with the codeword x. It is straightforward to check that

$$[H]_{k_x, k_y} = 0 \quad \text{if and only if} \quad y \star x \in T_1.$$

As a consequence,

$$|T_1 \cap T_1\, x| = \text{number of zeros of the } k_x\text{-th row of } H.$$

$$|T_1 \cap x\, T_1| = \text{number of zeros of the } k_x\text{-th colum of } H.$$

Let S be the set of columns of H where their number of zeros is equal to $2t+1$.

Since the $(-1, 1)$ version of H satisfies (1.4), then

- $|T_1 \cap x\, T_1| = \begin{cases} 2t+1 & x \in S, \\ 2t \text{ or } 2t+2 & x \in T \backslash (S \cup \langle u \rangle). \end{cases}$
- $|S| = 2t+1$.

Obviously, $S = \emptyset$ when H is extremal. □

Finally, we have studied the allowable values for the rank and for the dimension of the kernel of these codes.

Proposition 3.14 *Let E be a quasi-Hadamard full propelinear code of length $4t+2$. Then*

- $\dim(K(E)) = k \leq 2$.
- *If $k = 1$, then $K(E) = \langle u \rangle$, and $r \leq 4t+2$.*
- *If $k = 2$, then $K(E) = \langle u, s \rangle$, with $\mathrm{wt}(s) = 2t+1$, $s^2 \in \langle u \rangle$, and $r \leq 2t+2$.*

Proof It is trivial that $u \in K(E)$. Let $s \neq u$ be a codeword in $K(E)$, then $s + x \in E$ for any $x \in E$. Suppose that $\mathrm{wt}(s)$ is equal to $2t$ or $2t+2$, then for each $x \in E$ with $\mathrm{wt}(x) = 2t+1$, we have that $\mathrm{wt}(s+x) = 2t+1$.

Note that we have an odd amount of rows of H (the quasi-Hadamard matrix associated to E) with weight equal to $2t+1$ because the $(-1, 1)$ version of H satisfies (3.1). Thus we have $4t+2$ codewords with weight equal to $2t+1$. As $u \in K(E)$, we need to distribute the codewords with weight equal to $2t+1$ in sets of four elements, $\{x, x+s, x+u, x+s+u\}$, then there is a contradiction. Thus $\mathrm{wt}(s) = 2t+1$ for each codeword in $K(E)\backslash\langle u \rangle$.

Let s_1, s_2 be two different codewords in $K(E)$ and $s_1 \neq s_2 + u$, as $K(E)$ is a linear subspace, then $s_1 + s_2 \in K(E)$, but $\mathrm{wt}(s_1 + s_2)$ is $2t$ or $2t+2$. Then $K(E)$ is at most $\langle u, s \rangle$ where s is a codeword with $\mathrm{wt}(s) = 2t+1$. Also $s^2 = s + \pi_s(s) \in K(E)$, but the unique possibility is that s^2 is u or e.

The bounds for the rank are immediately from 3.3. □

4 Examples

In this section, we provide some examples of quasi-Hadamard full propelinear codes (briefly, QHFP-codes) coming from quasi-Hadamard groups.

Example 4.1 Let $Q_{12} = \langle a, b \mid a^3 = b^2, b^4 = e, b^3ab = a^5 \rangle$ be a dicyclic group of order 12. We have that $Q_{12} = \{e, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$. Let $T = \{e, a, a^2, b, ab, a^2b\}$ be a transversal, $Z = \langle a^3 \rangle$, where $a^3 = b^2$ is an involution, and $S = \{b, ab, a^2b\}$. Therefore, the quasi-Hadamard matrix associated to T is

$$H(T) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Thus, the generators of the QHFP-code are $a = (1, 0, 0, 1, 0, 0)$, $b = (1, 0, 0, 0, 1, 1)$, and the permutations are $\pi_a = (1, 2, 3)(4, 5, 6)$ and $\pi_b = (1, 4)(2, 6)(3, 5)$. Note that $a^3 = b^2 = u$. With these values, the relation $b^3ab = a^5$ is fulfilled. The rank of this code is 4 and the dimension of the kernel is 2, $K(Q_{12}) = \langle u, a^2b \rangle$.

Example 4.2 Let $E = \{a, b \mid a^6 = b^2 = e, ab = ba\} \simeq \mathbb{Z}_6 \times \mathbb{Z}_2$. Let $T = \{e, a, a^2, b, a^4b, a^5b\}$ be a transversal, $Z = \langle a^3 \rangle$ where a^3 is an involution, and $S = \emptyset$. Therefore, the quasi-Hadamard matrix associated to T is

$$H(T) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Thus, the generators of the QHFP-code are $a = (1, 0, 0, 0, 1, 0)$ and $b = (0, 1, 1, 0, 1, 1)$, and the permutations are $\pi_a = (1, 2, 3)(4, 5, 6)$ and $\pi_b = (1, 4)(2, 5)(3, 6)$. Note that $a^3 = u$. The rank of this code is 5 and the dimension of the kernel is 1, $K(E) = \langle u \rangle$.

Example 4.3 Let $E = \{a \mid a^{12} = e\} \simeq \mathbb{Z}_{12}$. Let $T = \{e, a, a^2, a^9, a^{10}, a^5\}$ be a transversal, $Z = \langle a^6 \rangle$ where a^6 is an involution and $S = \{a, a^9, a^5\}$. Therefore, the quasi-Hadamard matrix associated to T is

$$H(T) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Thus, the generator of the QHFP-code is $a = (1, 0, 0, 1, 0, 1)$, and the permutation is $\pi_a = (1, 2, 3, 4, 5, 6)$. Note that $a^6 = u$. The rank of this code is 6 and the dimension of the kernel is 1, $K(E) = \langle u \rangle$.

We note that the values of the rank and the dimension of the kernel obtained in the above examples tell us that the codes are nonlinear. In the case of Hadamard full propelinear codes with length 4 and 8 do not appear nonlinear codes. When the length is 4 the HFP-codes have rank and dimension of the kernel equal to 3, and in the case of length 8 the rank and the dimension of the kernel are 4.

Acknowledgements The authors wish to thank the anonymous referee for his valuable comments that improved the paper. 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 rest of authors were partially supported by the Spanish Grant TIN2016-77918-P (AEI/FEDER, UE).

References

1. Álvarez, V., Armario, J.A., Frau, M.D., Gudiel, F.: The maximal determinant of cocyclic $(-1, 1)$-matrices over D_{2t}. Linear Algebra Appl. **436**, 858–873 (2012)
2. Álvarez, V., Armario, J.A., Frau, M.D., Gudiel, F.: Determinants of $(-1, 1)$-matrices of the skew-symmetric type: a cocyclic approach. Open Math. **13**, 16–25 (2015)
3. Armario, J.A., Flannery, D.L.: On quasi-orthogonal cocycles. J. Comb. Des. **26**, 401–411 (2018)
4. de Launey, W., Flannery, D.L., Horadam, K.J.: Cocyclic Hadamard matrices and difference sets. Discrete Appl. Math. **102**, 47–62 (2000)
5. Ehlich, H.: Determiantenabschätzungen für binäre Matrizen. Math. Z. **83**, 123–132 (1964)
6. Flannery, D.L.: Cocyclic Hadamard matrices and Hadamard groups are equivalent. J. Algebra **192**, 749–779 (1997)
7. Fletcher, R.J., Koukouvinos, C., Seberry, J.: New skew-Hadamard matrices of order $4 \cdot 59$ and new D-optimal designs of order $2 \cdot 59$. Discrete Math. **286**, 252–253 (2004)
8. Hadamard, J.: Résolution d'une question relative aux déterminants. Bull. Sci. Math. (2) **17**, 240–246 (1893)
9. Horadam, K.J.: Hadamard Matrices And Their Applications. Princeton University Press, Princeton (2007)
10. Ito, N.: On Hadamard groups. J. Algebra **168**, 981–987 (1994)
11. Karpilovsky, G.: Projective Representations of Finite Groups. Marcel Dekker, New York (1985)
12. Kharaghani, H., Orrick, W.: D-optimal matrices. In: Colbourn, C.J., Dinitz, J. (eds.) The CRC Handbook of Combinatorial Designs, 2nd edn, pp. 296–298. CRC Press, Boca Raton (2006)
13. Orrick, W., Solomon, O.: The Hadamard Maximal Determinant Problem (website), http://www.indiana.edu/~maxdet/. Accessed 3 Oct 2017
14. Rifà, J., Basart, J.M., Huguet, L.: On completely regular propelinear codes. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. LNCS, vol. 357. Springer, pp. 341–355 (1989)
15. Rifà, J., Suárez, E.: About a class of Hadamard propelinear codes. Electron. Notes Discrete Math. **46**, 289–296 (2014)
16. Rifà, J., Suárez, E.: Hadamard full propelinear codes of type Q. Rank and kernel. Des. Codes Cryptogr. **00**, 1–17 (2017). https://doi.org/10.1007/s10623-017-0429-2. arXiv:1709.02465 [math.CO]
17. Wojtas, W.: On Hadamard's inequallity for the determinants of order non-divisible by 4. Colloq. Math. **12**, 73–83 (1964)