On an inequivalence criterion for cocyclic Hadamard matrices

José Andrés Armario

Abstract Given two Hadamard matrices of the same order, it can be quite difficult to decide whether or not they are equivalent. There are some criteria to determine Hadamard inequivalence. Among them, one of the most commonly used is the 4-profile criterion. In this paper, a reformulation of this criterion in the cocyclic framework is given. The improvements obtained in the computation of the 4-profile of a cocyclic Hadamard matrix are indicated.

Keywords Cocyclic Hadamard matrices · Hadamard equivalence · 4-profile criterion

1 Introduction

A Hadamard matrix of order n is an $n \times n$ matrix with every entry either 1 or -1, which satisfies $HH^T = nI$. It is known that n is necessarily 1, 2 or a multiple of 4, but there is no certainty whether such a Hadamard matrix exists for every size $4t$. This is the *Hadamard conjecture*, which remains unsolved for more than a century.

Two Hadamard matrices are called equivalent if one can be obtained from the other by some sequence of row and column permutations and negations. To identify the equivalence of two Hadamard matrices of order n, a complete search compares $(2^n n!)^2$ pairs of matrices and is known to be an NP hard problem when n increases [13]. The classification of Hadamard matrices of order $n \geq 32$ remains an open and

This work has been partially supported by the research projects FQM-296 and P07-FQM-02980 from JJAA and MTM2008-06578 from MICINN (Spain).

J. A. Armario (✉)
Department of Applied Math I, University of Seville, Avda. Reina Mercedes s/n,
41012 Seville, Spain
e-mail: armario@us.es

difficult problem and only partial results are known. What is known is that there is only one equivalence class of Hadamard matrices for each of the orders $n = 1, 2, 3, 8$ and 12. There are five equivalence classes for $n = 16$, 3 for $n = 20$, 60 for $n = 24$ and 487 for $n = 28$ [9]. For updates on the lower bounds for the number of equivalence classes for higher orders, visit this website [10]. The 4-profile criterion is a sufficient (but not necessary) condition for Hadamard inequivalence. Hadamard matrices with unequal 4-profiles are inequivalent. However, Hadamard matrices with equal 4-profiles may or may not be inequivalent.

Cooper, Milas and Wallis in [4] suggested the 4-profile criterion to investigate the equivalence of Hadamard matrices. Later Lin, Wallis and Zhu in [11] proposed some modifications of this criterion. Suppose that $H = (h_{ij})$ is a Hadamard matrix of order $4t \geq 8$. Define

$$P_{ijkl} = \left| \sum_{x=1}^{4t} h_{ix} h_{jx} h_{kx} h_{lx} \right|.$$

We shall write $\pi(m)$ for the number of sets $\{i, j, k, l\}$ of four distinct rows such that $P_{ijkl} = m$. It is well-known that $\pi(m) = 0$ unless $m \geq 0$ and $m = 4n \bmod 8$. We call $\pi(m)$ the 4-profile of H. The complexity in terms of time for the computation of this invariant is of orders $O(t^5)$. This criterion has been implemented in the Computer Algebra System, MAGMA [3].

In the early 90s, a surprising link between homological algebra and Hadamard matrices [6, 7] led to the study of cocyclic Hadamard matrices [8]. Hadamard matrices of many classes are revealed to be (equivalent to) cocyclic matrices [5, 9]. Among them, Silvester Hadamard matrices, Williamson-type Hadamard matrices and Paley Hadamard matrices. Furthermore, cocyclic construction is the most uniform construction technique for Hadamard matrices currently known, and cocyclic Hadamard matrices may consequently provide a uniform approach to the famous Hadamard conjecture.

The main purpose of this paper is to rewrite the 4-profile criterion in the cocyclic framework. It also shows that the additional internal structure in a matrix, which represents a cocycle, is sufficient to provide a substantial reduction in computational complexity of the problem of calculating this invariant. We will focus on the D_8 case.

2 Preliminaries

Assume throughtout that $G = \{g_1 = 1, g_2, \ldots, g_{4t}\}$ is a multiplicative group, not necessarily abelian. Functions $\psi : G \times G \to \langle -1 \rangle \cong \mathbf{Z}_2$ which satisfy

$$\psi(g_i, g_j)\psi(g_i g_j, g_k) = \psi(g_j, g_k)\psi(g_i, g_j g_k), \quad \forall g_i, g_j, g_k \in G \tag{1}$$

are called (binary) cocycles (over G)[12].

A cocycle ψ is naturally displayed as *a cocyclic matrix* M_ψ; that is, the entry in the (i, j)th position of the cocyclic matrix is $\psi(g_i, g_j)$), for all $1 \leq i, j \leq 4t$.

A cocycle is a coboundary $\partial\phi$ if it is derived from a set mapping $\phi\colon G \to \langle -1\rangle$ by $\partial\phi(a,b) = \phi(a)\phi(b)\phi(ab)^{-1}$. For instance, the function ∂_d which is constructed from the characteristic set map $\delta_d\colon G \to \{-1, 1\}$ associated to an element $g_d \in G$, so that

$$\partial_d(g_i, g_j) = \delta_d(g_i)\delta_d(g_j)\delta_d(g_ig_j) \quad \text{for} \quad \delta_d(g_i) = \begin{cases} -1 & g_d = g_i \\ 1 & g_d \neq g_i, \end{cases} \tag{2}$$

is so-called *an elementary coboundary*. Although the elementary coboundaries generate the set of all coboundaries, they might not be linearly independent (see [2] for details).

A cocycle ψ is *normalized* if $\psi(1, g_j) = \psi(g_i, 1) = 1$ for all $g_i, g_j \in G$. The cocyclic matrix coming from a normalized cocycle is called *normalized* cocylic matrix. Note that M_{∂_d} is normalized if $d > 1$.

If a cocyclic matrix M_ψ is Hadamard, we say that the cocycle involved, ψ, is orthogonal and M_ψ is *a cocyclic Hadamard matrix*. The cocyclic Hadamard test asserts that a normalized cocyclic matrix is Hadamard if and only if the summation of each row (but the first) is zero [8].

The *generalized coboundary matrix* $\overline{M}_{\partial_j}$ related to an elementary coboundary ∂_j consists of negating the *jth*-row of the matrix M_{∂_j}. Note that negating a row or a column of a matrix does not change its Hadamard character. As it is pointed out in [1], every generalized coboundary matrix $\overline{M}_{\partial_j}$ contains exactly two negative entries in each row $s \neq 1$, which are located at positions (s, i) and (s, e), for $g_e = g_s^{-1}g_i$.

In the following lemma, we study the distribution of -1 by columns in the generalized coboundary matrices.

Lemma 1 *Every column $j \neq l$ in $\overline{M}_{\partial_l}$ contains precisely only one -1 which is located in the position (i, j) for $g_i = g_l g_j^{-1}$. Furthermore, the lth column is formed by -1s, except in the position $(1, l)$.*

Proof The proof follows from particularizing (2) to the cocycle ∂_l. □

Let us observe that fixed l, then $g_i = g_l g_j^{-1}$ reaches all the values of $G = \{g_1, \ldots, g_{4t}\}$ when g_j is taking values from g_1 until g_{4t}. Hence, for every generalized coboundary matrix $\overline{M}_{\partial_l}$ there exists a $4t \times 4t$ permutation matrix P_l such that

$$\overline{M}_{\partial_l} = AP_l,$$

where

$$A = \left(\begin{array}{c|ccc} + & + & \cdots & + \\ \hline - & - & & \\ \vdots & & \ddots & \\ - & & & - \end{array}\right)_{4t\times 4t.}$$

Another relevant property of these generalized coboundary matrices is given in the following lemma.

Lemma 2 *No two generalized coboundary matrices share a column in the same position. Hence, every column j of A appears in a different position in two generalized coboundary matrices.*

Proof Given $\overline{M}_{\partial_{l_1}}$ and $\overline{M}_{\partial_{l_2}}$ where $1 \leq l_1 < l_2 \leq 4t$. Obviously, the l_1th column in $\overline{M}_{\partial_{l_1}}$ is different from the l_1th column in $\overline{M}_{\partial_{l_2}}$ (the same follows for the l_2th column).

On the other hand, since $l_1 \neq l_2$ then $g_{l_1} \neq g_{l_2}$ and $g_{l_1} g_j^{-1} \neq g_{l_2} g_j^{-1}$ for all $1 \leq j \leq 4$. If $j \neq l_1, l_2$ then the jth column of $\overline{M}_{\partial_{l_1}}$ has its only non null entry in the position $g_{l_1} g_j^{-1}$ and the jth column of $\overline{M}_{\partial_{l_2}}$ has its only non null entry in the position $g_{l_2} g_j^{-1}$. Therefore, both jth columns are different. □

3 The 4-profile criterion for cocyclic Hadamard matrices

Let M_ψ be a cocyclic Hadamard matrix over G. In this section, we deal with the problem of computing the 4-profile for M_ψ. To this end, we have to compute the absolute value of the generalized inner product of rows i, j, k and l,

$$P_{ijkl} = \left| \sum_{x=1}^{4t} \psi(g_i, g_x)\psi(g_j, g_x)\psi(g_k, g_x)\psi(g_l, g_x) \right|$$

for every set $\{i, j, k, l\}$ of four distinct rows (i.e., four distinct integers of $\{1, \ldots, 4t\}$). Working in a similar way to [9, Lemma 6.6] and using the identity (1), we get

$$P_{ijkl} = \left| \sum_{x=1}^{4t} \psi(g_i g_j^{-1}, g_x)\psi(g_k g_l^{-1}, g_l g_j^{-1} g_x) \right|. \tag{3}$$

It seems to be a first reduction in the formula, but it presents a problem because the factor $g_l g_j^{-1}$ produces a permutation in the elements of the $g_k g_l^{-1}$th row.

To solve this problem, we use the distribution of -1 by columns in the generalized coboundary matrices pointed out in Lemma 1 and consider the following permutation matrix P:

- The 1st column of P has its unique non null entry in the same position where the jth column of $\overline{M}_{\delta_l}$ has its unique negative entry.
- The rest of the columns of P can be computed from the first one and the multiplication table of the group.

Lemma 3 *Fixed y, g_j and $g_l \in G$ and taking the permutation matrix P described above*

$$\psi(y, g_l g_j^{-1} x) = \psi(y, x) \cdot P, \quad \forall x \in G.$$

Proof Let us observe that the jth column of $\overline{M}_{\delta_l}$ has its unique negative entry in the position k where $g_k = g_l g_j^{-1}$. □

Example 1 If $G = D_{4t} = \langle a, b : a^{2t} = b^2 = (ab)^2 = 1\rangle$ the dihedral group with ordering

$$\{1, a, a^2, \ldots, a^{2t-1}, b, ab, \ldots, a^{2t-1}b\}$$

indexed as $\{1, \ldots, 4t\}$, and we know that the 1st column of P has its unique non null entry in position k then the permutation matrix P has the form:

For $1 \leq k \leq 2t$,

$$\left(\begin{array}{cc|cc} & I_{k-1} & & \\ I_{2t-k+1} & & & \\ \hline & & & I_{k-1} \\ & & I_{2t-k+1} & \end{array}\right)$$

where I_n is the $n \times n$ identity matrix.

For $2t + 1 \leq k \leq 4t$,

$$\left(\begin{array}{cc|cc} & & \hat{I}_{k-2t} & \\ & & & \hat{I}_{4t-k} \\ \hline \hat{I}_{k-2t} & & & \\ & \hat{I}_{4t-k} & & \end{array}\right)$$

where $\hat{I}_n$ is the $n \times n$ back diagonal matrix where its non null entries are in positions (i, j) satisfying $i + j = n + 1$ and these entries are all 1 s.

On the other hand, the number of sets $\{i, j, k, l\}$ of four distinct rows for M_ψ is $\binom{4t}{4}$. Actually, this is mainly responsible for the computational cost in computing for the 4-profile. In the sequel, we will define an equivalence relation for the sets $\{i, j, k, l\}$ of four distinct rows, and we will be able to compute the 4-profile of M_ψ from a representatives element of at most $\binom{4t}{4}/t$ classes.

Definition 1 Let $X = \{x_1, x_2, x_3, x_4\}$ and $Y = \{y_1, y_2, y_3, y_4\}$ be subsets of four distinct integers of $\{1, \ldots, 4t\}$. X and Y are called *equivalent* (or *G-equivalent*) if these following identities hold:

$$g_{x_1} g_{x_2}^{-1} = g_{y_1} g_{y_2}^{-1}, \quad g_{x_3} g_{x_4}^{-1} = g_{y_3} g_{y_4}^{-1}, \text{ and } g_{x_4} g_{x_2}^{-1} = g_{y_4} g_{y_2}^{-1}. \tag{4}$$

Remark 1 For a given group G of $4t$ elements with a fixed ordering, the relation of G-equivalence is an equivalence relation. Therefore, one can study the equivalence classes and define representative for each class. $[\{x_1, x_2, x_3, x_4\}]$ denotes the class defined by the element $\{x_1, x_2, x_3, x_4\}$.

Definition 2 The *size of* $[\{x_1, x_2, x_3, x_4\}]$, denoted by $\sharp[\{x_1, x_2, x_3, x_4\}]$, is the number of "different" elements $Y = \{y_1, y_2, y_3, y_4\}$ equivalent to $X = \{x_1, x_2, x_3, x_4\}$. If Y and $\alpha(Y) = \{y_{\alpha(1)}, y_{\alpha(2)}, y_{\alpha(3)}, y_{\alpha(4)}\}$ are G-equivalent to X for a permutation α of the integers $\{1, 2, 3, 4\}$, then Y and $\alpha(Y)$ are considered to be the same to this end.

Lemma 4 *Let α be a permutation of the integers $\{1, 2, 3, 4\}$. If $X = \{x_1, x_2, x_3, x_4\}$ and $Y = \{y_1, y_2, y_3, y_4\}$ are G-equivalent. Then $\alpha(X) = \{x_{\alpha(1)}, x_{\alpha(2)}, x_{\alpha(3)}, x_{\alpha(4)}\}$ and $\alpha(Y) = \{y_{\alpha(1)}, y_{\alpha(2)}, y_{\alpha(3)}, y_{\alpha(4)}\}$ are G-equivalent too.*

Proof Assume $1 \leq i, j \leq 4$ and $i \neq j$. We are going to prove that $g_{x_i} g_{x_j}^{-1} = g_{y_i} g_{y_j}^{-1}$. Firstly, for being X equivalent to Y, we have

$$g_{x_1} g_{x_2}^{-1} = g_{y_1} g_{y_2}^{-1}, \quad g_{x_3} g_{x_4}^{-1} = g_{y_3} g_{y_4}^{-1}, \text{ and } g_{x_4} g_{x_2}^{-1} = g_{y_4} g_{y_2}^{-1}.$$

Now, we check that the desired identity holds for:

$$\begin{aligned} g_{x_2} g_{x_3}^{-1} = g_{x_2} g_{x_4}^{-1} g_{x_4} g_{x_3}^{-1} = g_{x_2} g_{x_4}^{-1} (g_{x_3} g_{x_4}^{-1})^{-1} = g_{y_2} g_{y_4}^{-1} (g_{y_3} g_{y_4}^{-1})^{-1} \\ = g_{y_2} g_{y_4}^{-1} g_{y_4} g_{y_3}^{-1} = g_{y_2} g_{y_3}^{-1}. \\ g_{x_1} g_{x_3}^{-1} = g_{x_1} g_{x_2}^{-1} g_{x_2} g_{x_3}^{-1} = g_{y_1} g_{y_2}^{-1} g_{y_2} g_{y_3}^{-1} = g_{y_1} g_{y_3}^{-1}. \end{aligned}$$

The rest of the identities follow in a similar manner. □

Corollary 1 *Given two different equivalent classes* $[X]$ *and* $[Y]$*. If* Z *is equivalent to* X *and* $\alpha(Z)$ *is equivalent to* Y *for a permutation* α *of the integers* $\{1, 2, 3, 4\}$*, then these two classes* $[\alpha(X)]$ *and* $[Y]$ *are the same.*

Definition 3 A set $\{[X_1], \ldots, [X_n]\}$ of different equivalence classes is not *proper* if there exists two classes, $[X_i]$ and $[X_j]$, and a permutation α of the integers $\{1, 2, 3, 4\}$ such that $[X_i] = [\alpha(X_j)]$. Otherwise, we say that $\{[X_1], \ldots, [X_n]\}$ is *a set of proper equivalence classes*.

Definition 4 We will say that a set $\Omega = \{[X_1], \ldots, [X_n]\}$ is a *distribution of proper equivalence classes*, if Ω is a set of proper equivalence classes and $\Omega \cup [Y]$ is not proper for any equivalent class $[Y]$.

Fixed a group G, we outline a procedure to construct a distribution of proper equivalent classes and to evaluate the size of every class.

Algorithm 1 Searching for a distribution of proper G-equivalent classes.

Input: a multiplicative group G of $4t$ elements.
Output: a distribution of proper equivalent classes and the size of every class.

$\Omega \leftarrow \emptyset$

$\mathcal{S} \leftarrow$ all $\binom{4t}{4}$ subsets of four distinct elements of $\{1, 2, \ldots, 4t\}$
while $\mathcal{S}$ is not empty {

1. Choose a set X in $\mathcal{S}$.
2. $\mathcal{S} \leftarrow \mathcal{S} \setminus \{X\}$.
3. Check whether either X or a permutation of its components is equivalent to one element of Ω. If no, go to 5; otherwise go to 4.

4. $\sharp[Y] \leftarrow \sharp[Y] + 1$ where $[Y]$ is the unique element of Ω satisfying that either X or a permutation of its components is equivalent to Y. Go to 1.
5. $\Omega \leftarrow \Omega \cup [X]$ and $\sharp[X] \leftarrow 1$.

}
$\Omega = \{[X_1], \ldots, [X_n]\}$ and $\Omega^\sharp = \{\sharp[X_1], \sharp[X_2], \ldots, \sharp[X_n]\}$

Correctness: Corollary 1 guarantees the uniqueness of $[Y]$ in the Step 4. By construction, Ω is a set of proper equivalence classes and $\Omega \cup [Z]$ is not proper for any equivalence class $[Z]$. Furthermore, $\Omega^\sharp$ gives the size of every class.

The following result can be seen as an immediate consequence of the procedure described above.

Proposition 1 *Assuming that $\Omega = \{[X_1], \ldots, [X_n]\}$ is a distribution of proper equivalence classes. We have:*

- *Given a set $\{i, j, k, l\}$ of four distinct integers of $\{1, 2, \ldots, 4t\}$. There is one and only one class in Ω, $[X_m]$, such that either $\{i, j, k, l\}$ or a permutation of its components is equivalent to X_m.*
- $\displaystyle\sum_{i=1}^{n} \sharp[X_i] = \binom{4t}{4}$.

Now we study the connection between the 4-profile of M_ψ and the relation of G-equivalence.

Proposition 2 *Given two sets $\{i, j, k, l\}$ and $\{i', j', k', l'\}$ of four distinct rows of M_ψ (i.e., sets of four distinct integers of $\{1, \ldots, 4t\}$). If $\{i, j, k, l\}$ is equivalent to $\{i', j', k', l'\}$ then $P_{ijkl} = P_{i'j'k'l'}$.*

Proof It follows from Eqs. 3 and 4. □

We now describe a method to evaluate the 4-profile for a cocyclic Hadamard matrix over G. Let us observe that Step 1 of this method depends only on G.

Algorithm 2 Computing the 4-profile of M_ψ.

Inputs: a multiplicative group G of $4t$ elements and a cocyclic Hadamard matrix M_ψ over G

Output: the 4-profile of M_ψ

Step 1. Calculate Ω and $\Omega^\sharp$.
Step 2. Calculate $\mathcal{I} = \{P_{X_1}, P_{X_2}, \ldots, P_{X_n}\}$.
Step 3. For each $m \in \mathcal{I}$, $\pi(m) = \displaystyle\sum_{[X_i] \in \Omega / P_{X_i} = m} \sharp[X_i]$

In the remaining part of this section, we will tackle the problem of determining the size of every equivalent class. To this end, we fix a set $\{i, j, k, l\}$ of four distinct rows of M_ψ. Any solution $\{i', j', k', l'\}$ of the following equations system

$$\begin{cases} g_i g_j^{-1} = g_{i'} g_{j'}^{-1} \\ g_k g_l^{-1} = g_{k'} g_{l'}^{-1} \\ g_l g_j^{-1} = g_{l'} g_{j'}^{-1}, \end{cases} \tag{5}$$

is G-equivalent to $\{i, j, k, l\}$ and vice versa. Therefore, the size of $[\{i, j, k, l\}]$ is the number of different solutions of Eq. 5.

In the following lemma we study the number of different solutions for one equation.

Lemma 5 *Given a set $\{i, j\}$ of two distinct rows of M_ψ. If λ denotes the number of different pairs $\{i', j'\}$ such that*

$$g_i g_j^{-1} = g_{i'} g_{j'}^{-1}. \tag{6}$$

Then, $2t \leq \lambda \leq 4t$.

Proof By Lemma 1, $g_i g_j^{-1}$ indicates the position of the unique -1 entry of the jst column of $\overline{M}_{\partial_i}$.

Let c_j^i be the $4t \times 1$ vector of ones except in the position $g_i g_j^{-1}$ with entry -1. By Lemma 2, c_j^i appears only one time in every generalized coboundary as a column, but always in a different position. Thus, there is a permutation α of the integers $\{1, \ldots, 4t\}$ such that the first column of $\overline{M}_{\partial_{\alpha(1)}}$ coincides with c_j^i, the second column of $\overline{M}_{\partial_{\alpha(2)}}$ coincides with c_j^i and so on. Therefore, any element of $\{g_{\alpha(1)} g_1^{-1}, \ldots, g_{\alpha(4t)} g_{4t}^{-1}\}$ is a solution of Eq. 6 and obviously, these are all the solutions. We point out that some of the following identities could hold

$$g_{\alpha(1)} g_1^{-1} = g_1 g_{\alpha(1)}^{-1},\ g_{\alpha(2)} g_2^{-1} = g_2 g_{\alpha(2)}^{-1}, \ldots, g_{\alpha(4t)} g_{4t}^{-1} = g_{4t} g_{\alpha(4t)}^{-1}.$$

Since the sets $\{i, \alpha(i)\}$ and $\{\alpha(i), i\}$ of two distinct rows are the same, it follows the desired result. □

Remark 2 To solve Eq. 6 is equivalent to localizing a determinate column in each generalized coboundary matrix.

Lemma 6 *If κ denotes the number of different sets $\{i', j', k', l'\}$ of four distinct rows which are solutions of Eq. 5. Then,*

$$t \leq \kappa \leq 4t.$$

Proof To solve Eq. 5, we start by taking one solution, $g_{x_1} g_{x_2}^{-1}$, from the third equation. It determines the second and the fourth component for the solution of Eq. 5

$$\{-, x_2, -, x_1\}.$$

Now, we have to look for the solution of the second equation of type $g_{y_1} g_{x_1}^{-1}$. Thus, we have the third component

$$\{-, x_2, y_1, x_1\}.$$

Finally, we have to look for the solution of the first equation of type $g_{z_1} g_{x_2}^{-1}$. Thus,

$$\{z_1, x_2, y_1, x_1\}$$

is a solution of the system (5). So, every solution of the third equation generates a unique solution of the system. Furthermore, we could have started by taking one solution from either the first or the second equation and, in a similar manner, we would have obtained the unique solution of the system from this input.

On the one hand, the most favorable case takes place when every solution $g_{x_1} g_{x_2}^{-1}$ generates one "different" solution $\{z_1, x_2, y_1, x_1\}$ of the system. Since there are $4t$ solutions for an equation, we have $4t$ solutions for the system.

On the other hand, the worst scenario takes place when for every solution $X = \{x_1, x_2, x_3, x_4\}$ of the system, the cardinal of the set $\mathcal{A} = \{\alpha_j \colon \alpha_j(X) \text{ is a solution too}\}$ is maximum, where α_j denotes a permutation of the integers $\{1, 2, 3, 4\}$. Let us observe that if α_p and $\alpha_q \in \mathcal{A}$ satisfy that $\alpha_p(i) = \alpha_q(i)$ for some i, then $\alpha_p(i) = \alpha_q(i)$, $\forall i$. Hence, 4 is an upper bound for the cardinal of $\mathcal{A}$, since if the cardinal of $\mathcal{A}$ were five or more, then there would exist two permutations α_p and α_q satisfying that $\alpha_p(i) = \alpha_q(i)$ for some i. As a consequence, $4t/4$ is a lower bound of the number of different solutions for Eq. 5. □

Remark 3 Let $\Omega = \{[X_1], \ldots, [X_n]\}$ be a distribution of proper equivalence classes. On the one hand, using the identification between the size of $[X]$ and κ (the number of different solutions of Eq. 5), we have by Lemma 6 that the size of every equivalent class, $\sharp[X_i]$, is greater than or equal to t. On the other hand, by Proposition 1, this identity $\sum_{i=1}^{n} \sharp[X_i] = \binom{4t}{4}$ holds. So, the number of elements in a distribution of proper equivalence classes, n, is lesser than or equal to $\binom{4t}{4}/t$. Taking into account the step 2 of Algorithm 2, the number of sets of $\{i, j, k, l\}$ of four distinct rows to be considered for computing the 4-profile of a cocyclic Hadamard matrix over G is n instead of being $\binom{4t}{4}$.

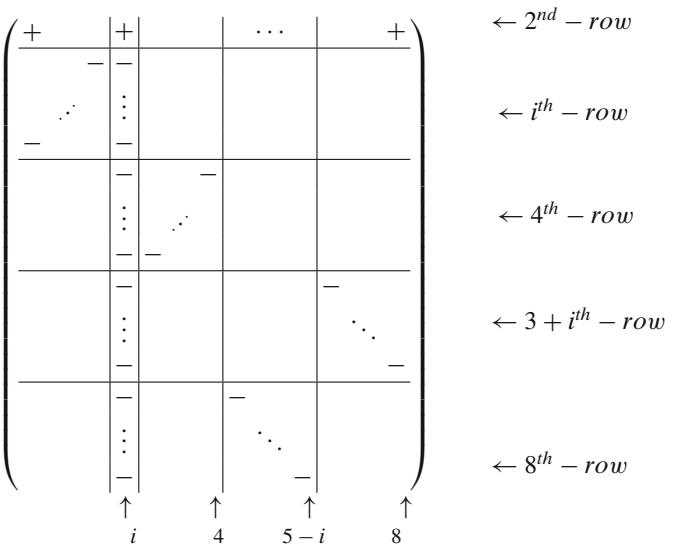
3.1 The D_8 case

In this section, we will solve Eq. 5 and will compute a distribution of proper equivalence classes being G the dihedral group of 8 elements, D_8, with presentation $\langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$, and with ordering

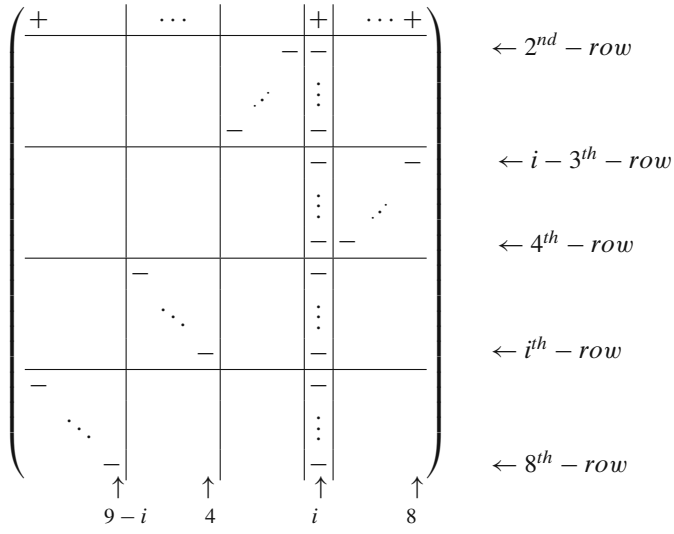
$$\{1, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

indexed as $\{1, \ldots, 8\}$.

An explicit description of every generalized coboundary matrix is:
For $1 \leq i \leq 4$, the matrices $\overline{M}_{\partial_i}$ have the form:



For $5 \leq i \leq 8$, the matrices $\overline{M}_{\partial_i}$ have the form:



Let ψ be a cocycle over D_8. In the sequel, $[n]_m$ denotes n mod m where we will use m as a representative for his class. Fixed a set $\{i, j\}$ of two different rows of M_ψ, we have the following lemma:

Lemma 7 *The pairs* $\{i', j'\}$ *solutions of* $\mathbf{g_i g_j^{-1}} = g_{i'} g_{j'}^{-1}$ *are:*

- *If* $1 \leq i, j \leq 4$ *or* $5 \leq i, j \leq 8$ *then,*

$$\{[\mathbf{i}]_4, [\mathbf{j}]_4\}, \{[i+1]_4, [j+1]_4\}, \{[i+2]_4, [j+2]_4\}, \{[i+3]_4, [j+3]_4\}, \{[i]_4+4, [j]_4+4\}$$
$$\{[i+1]_4+4, [j+1]_4+4\}, \{[i+2]_4+4, [j+2]_4+4\}, \{[i+3]_4+4, [j+3]_4+4\}.$$

- *If* $1 \leq i \leq 4$ *and* $5 \leq j \leq 8$, *or,* $5 \leq i \leq 8$ *and* $1 \leq j \leq 4$ *then,*

$$\{[\mathbf{i}]_4, [\mathbf{j}]_4 + \mathbf{4}\}, \{[i+1]_4, [j-1]_4+4\}, \{[i+2]_4, [j-2]_4+4\}, \{[i+3]_4, [j-3]_4+4\},$$
$$\{[i]_4+4, [j]_4\}, [i+1]_4+4, [j-1]_4\}, \{[i+2]_4+4, [j-2]_4\}, \{[i+3]_4+4, [j-3]_4\}.$$

Proof It follows from Lemma 5 and the form of the matrices $\overline{M}_{\partial_i}$. □

Example 2 Fixed the set $\{5, 2\}$ of two rows. We have

$$\mathbf{g_5 g_2^{-1}} = g_6 g_1^{-1} = g_7 g_4^{-1} = g_8 g_3^{-1} = g_1 g_6^{-1} = g_2 g_5^{-1} = g_3 g_8^{-1} = g_4 g_7^{-1}.$$

The following proposition gives an explicit description of every solution for Eq. 5 being $G = D_8$.

Proposition 3 *Fixed a set* $R = \{i, j, k, l\}$ *of four distinct rows of* M_ψ, *we define* $R_1 = \{r \in R : r < 5\}$ *and* $R_2 = \{r \in R : r > 4\}$. *Let S be the following matrix*

$$S = \begin{pmatrix} i & j & k & l \\ c(i) & c(j) & c(k) & c(l) \\ c^2(i) & c^2(j) & c^2(k) & c^2(l) \\ c^3(i) & c^3(j) & c^3(k) & c^3(l) \end{pmatrix}$$

where $c(r) = \begin{cases} [r-1]_4 & r \in R_1 \\ [r+1]_4 + 4 & r \in R_2 \end{cases}$ *and* $c^n(r) = c^{n-1}(c(r))$. *Every row of S is a solution of Eq. 5. Now, by adding* 4 *to every entry of C less than or equal to* 4, *and subtracting* 4 *from every entry of C greater than or equal to* 5, *we have a new matrix* S' *where every row is a solution of Eq. 5 too.*

$$S' = \begin{pmatrix} i \pm 4 & j \pm 4 & k \pm 4 & l \pm 4 \\ c(i) \pm 4 & c(j) \pm 4 & c(k) \pm 4 & c(l) \pm 4 \\ c^2(i) \pm 4 & c^2(j) \pm 4 & c^2(k) \pm 4 & c^2(l) \pm 4 \\ c^3(i) \pm 4 & c^3(j) \pm 4 & c^3(k) \pm 4 & c^3(l) \pm 4 \end{pmatrix}$$

Proof Using Lemma 7, it is easy to check that these rows are the solutions of Eq. 5. □

The following example illustrates the way the former proposition generates the solutions for Eq. 5 in a concrete case.

Example 3 Given $R = \{1, 2, 3, 5\}$, we have that $R_1 = \{1, 2, 3\}$ and $R_2 = \{5\}$. We establish the 4×4 matrix where every row is a solution.

$$S = \begin{pmatrix} 1\,2\,3\,5 \\ 4\,1\,2\,6 \\ 3\,4\,1\,7 \\ 2\,3\,4\,8 \end{pmatrix}$$

and now, by adding 4 to every entry less than or equal to 4, and subtracting 4 from every entry greater than or equal to 5 in the above array, we have a new array where every row is a solution too.

$$S' = \begin{pmatrix} 5\,6\,7\,1 \\ 8\,5\,6\,2 \\ 7\,8\,5\,3 \\ 6\,5\,8\,4 \end{pmatrix}$$

Hence, the class with representative element $\{1, 2, 3, 5\}$ is formed by the eight rows.

In the following proposition, we describe a distribution of proper classes for the G-equivalence being $G = D_8$ and we will give the size for each class.

Proposition 4 *This is a distribution of proper equivalent classes for D_8:*

- *There are three classes with size 2. These are representative elements for each class:*

$$\{1, 2, 3, 4\}, \quad \{1, 3, 6, 8\}, \quad \{1, 3, 5, 7\}.$$

- *There are four classes with size 4. These are representative elements for each class:*

$$\{1, 2, 5, 6\}, \quad \{1, 2, 6, 7\}, \quad \{1, 2, 7, 8\}, \quad \{1, 2, 8, 5\}.$$

- *There are six classes with size 8. These are representative elements for each class:*

$$\{1, 2, 5, 7\}, \quad \{1, 2, 6, 8\}, \quad \{1, 2, 3, 5\}, \quad \{1, 2, 3, 6\}, \quad \{1, 2, 3, 7\}, \quad \{1, 2, 3, 8\}.$$

Proof This is seen by inspection and left to the reader. □

To sum up, we have proved that for computing the 4-profile of a cocyclic Hadamard matrix over D_8, it is sufficient to consider only 13 sets of four distinct rows of M_ψ (see Algorithm 2 and Proposition 4). These 13 sets of four distinct rows are explicitly given in Proposition 4. In general, for H a Hadamard matrix of order 8, it is necessary to consider 70.

4 Conclusion and further work

In this article, we presented some improvements in the computation of the 4-profile for a cocyclic Hadamard matrix over G.

- Firstly, we have reduced P_{ijkl} to compute the absolute value of the inner product of two rows.
- Secondly, we give an important reduction in the number of sets $\{i, j, k, l\}$ of four distinct rows to consider.

Our next goal is to give a distribution of proper equivalent classes when G is the dihedral group of $4t$ elements, D_{4t}. Actually, the analogous results to Lemma 7 and Proposition 3 applied to D_{4t} follow from the form of the generalized coboundary matrix over D_{4t} (see [1]). In addition, we conjecture that the size of the classes for the G-equivalence being $G = D_4$ is necessarily t, $2t$ or $4t$.

Acknowledgements The author would like to thank Kristeen Cheng for her reading of this article. The author would also like to thank the anonymous reviewers for their comments that helped improve the presentation of this paper.

References

1. Alvarez, V., Armario, J.A., Frau, M.D., Real, P.: A system of equations for describing cocyclic Hadamard matrices. J. Comb. Des. **16**(4), 276–290 (2008)
2. Alvarez, V., Armario, J.A., Frau, M.D., Real, P.: The homological reduction method for computing cocyclic Hadamard matrices. J. Symb. Comput. **44**, 558–570 (2009)
3. Bosma, W., Cannon, J.: Handbook of Magma Functions, ver. 2.9. Sydney (2002)
4. Cooper, J., Milas, J., Wallis, W.D.: Hadamard equivalence, In: Combinatorial Mathematics, Lecture Notes in Mathematics, vol. 686, pp. 126–135. Springer-Verlag, Berlin, Heidelberg, New York (1978)
5. de Launey, W., Horadam, K.J.: A weak difference set construction for higher dimensional designs. Des. Codes Cryptogr. **3**, 75–87 (1993)
6. Horadam, K.J., de Launey, W.: Cocyclic development of designs. J. Algebr. Comb. **2**(3), 267–290 (1993)
7. Horadam, K.J., de Launey, W.: Erratum: Cocyclic development of designs. J. Algebr. Comb. **3**(1), 129 (1994)
8. Horadam, K.J., de Launey, W.: Generation of Cocyclic Hadamard matrices, In: Computational Algebra and Number Theory. Math. Appl., pp. 279–290. Kluwer Acad. Publ, Dordrecht (1995)
9. Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ (2007)
10. Koukouvinos, C.: Website http://math.ntua.gr/∼ckoukouv/
11. Lin, C., Wallis, W., Zhu, L.: Generalized 4-profiles of Hadamard matrices. J. Comb. Inf. Syst. Sci. **18**, 397–400 (1993)
12. Mac Lane, S.: Homology. Classics in Mathematics Springer-Verlang, Berlin (1995). Reprint of the 1975 edition
13. McKay, B.D.: Hadamard equivalence via graph isomorphism. Discrete Math. **27**, 213–214 (1979)