Cocyclic Hadamard Matrices and Hadamard Groups Are Equivalent

D. L. Flannery

Faculty of Information Sciences and Engineering, University of Canberra, GPO Box 1, Belconnen, ACT 2616, Australia

Communicated by Walter Feit

Received August 7, 1996

In this paper, we prove that the concepts of cocyclic Hadamard matrix and Hadamard group are equivalent. A general procedure for constructing Hadamard groups and classifying such groups on the basis of isomorphism type is given. To illustrate the ideas, cocyclic Hadamard matrices over dihedral groups are constructed and the corresponding Hadamard groups classified.

1. INTRODUCTION

In [10], Ito defines the concept of Hadamard group. Such a group is necessarily a (central) extension of $\mathbb{Z}_2 = \{ -1, 1 \}$ by a group of order divisible by 4. The equivalence class of an extension $E$ of $\mathbb{Z}_2$ by a finite group $G$ corresponds uniquely to a 2-cocycle class in the second cohomology group $H^2(G, \mathbb{Z}_2)$. A 2-cocycle $\psi: G \times G \rightarrow \mathbb{Z}_2$ is naturally displayed as a cocyclic matrix, that is, a square matrix whose rows and columns are indexed by the elements of $G$ under some ordering, and whose entry in position $(g, h)$ is $\psi(g, h)$. We will show that $E$ is a Hadamard group precisely when any cocyclic matrix associated with some element in the 2-cohomology class corresponding to $E$ is Hadamard.

The connection between cohomology theory and Hadamard matrices afforded by cocyclic matrices was introduced by de Launey and Horadam in [3] (see also [7]), as a way of studying combinatorial designs. In [9] it is shown that the following concepts are equivalent: cocyclic Hadamard matrix, normal relative difference set in an extension of $\mathbb{Z}_2$, and group divisible design whose automorphism group contains an extension of $\mathbb{Z}_2$ as a regular subgroup, with $\mathbb{Z}_2$ the stabiliser of each point class (the latter two
objects have restrictions on their significant parameters). In Ito’s terminology, the extension in this equivalence is a Hadamard group, the normal relative difference set is precisely a Hadamard subset of a Hadamard group, and the group divisible design is a Hadamard design. These facts are not evident from the definitions alone, but certainly follow from the equivalence of Hadamard groups and cocyclic Hadamard matrices that we will demonstrate (see [9, Theorem 3.6]).

Hadamard groups that are split extensions (direct products) of \( Z_2 \) are used to study Menon–Hadamard difference sets in [11]; the corresponding cocyclic matrices are normalised group developed matrices, that is, are associated with coboundaries. One of the main aims of this paper is to broaden the general theory of cocyclic matrices and show how it can be applied in the construction and classification of Hadamard groups.

In Section 2 we set up some cohomological machinery, some of which is very standard. The concepts of cocyclic Hadamard matrix and Hadamard group are proved equivalent in Section 3. Section 4 focuses on two important ideas used in our study of Hadamard groups and cocyclic Hadamard matrices. First, we outline a systematic method for constructing (equivalence classes) of central extensions with given quotient and kernel. Second, we show how information about the automorphism groups of quotient and kernel, particularly about their action on the relevant second cohomology group, can be used to classify central extensions by so-called basic isomorphism type. In Section 5 we translate some results in [10] to derive nonexistence conditions for cocyclic Hadamard matrices developed over finite cyclic, dicyclic, and dihedral groups. Finally, we provide in Section 6 an application of the theory previously established. We will see in Section 6 that dihedral groups of order divisible by 4 provide a rich source of cocyclic Hadamard matrices and thus (by extension) of Hadamard groups. This work parallels independent work by Ito [12] on Hadamard groups of “type Q.”

2. COHOMOLOGICAL PRELIMINARIES

In this section we review some cohomology theory, leading up to a definition of the second cohomology group as a module for a subgroup of a direct product of two automorphism groups. This module action is especially relevant to the study of Hadamard groups and cocyclic Hadamard matrices.

Cocyclic matrices can be classified according to cohomological equivalence of the underlying 2-cocycles. Hadamard groups can be classified according to isomorphism type. A finer classification results if one regards two Hadamard groups as equivalent whenever there is an isomorphism
between them that respects the distinguished central subgroups of order 2. This is the notion of equivalence used in [14] and will be referred to in this paper as basic isomorphism. As will be shown, determining orbits in the relevant second cohomology group under the action referred to above is essentially a classification by basic isomorphism type of all Hadamard groups with specified quotient modulo distinguished $\mathbb{Z}_2$. At the end of this section, we make some comments about the inadequacy of this approach in solving the coarser classification problem.

Of course, cocyclic Hadamard matrices can be classified by Hadamard equivalence, that is, equality modulo permutation and negation of rows and columns. Determining orbits in the second cohomology group accounts for some but by no means all Hadamard equivalences. We will not consider in any detail the problem of classifying cocyclic Hadamard matrices by Hadamard equivalence type.

The material presented next is drawn mainly from [18, Sect. 4, pp. 66–71]. We begin by discussing the theory of extensions with not necessarily abelian kernel.

Let $G$ and $K$ be groups, written multiplicatively in the former case and additively in the latter, although we do not assume that $K$ is abelian. The convention is that automorphisms of $K$ act on the right and are written as superscripts. Suppose $\xi: G \to \text{Aut}(K)$ and $\psi: G \times G \to K$ are set maps satisfying

$$\psi(x, yz) + \psi(y, z) = \psi(xy, z) + \psi(x, y)^{\psi(z)}$$

(1)

and

$$\xi(x)\xi(y) = \xi(xy)\psi(x, y)$$

for all $x, y, z \in G$, where $\xi$ denotes the inner automorphism of $K$ induced by $k \in K$. For each such pair $(\xi, \psi)$ we have the associated canonical extension

$$0 \to K \overset{i}{\to} E_{(\xi, \psi)} \overset{\pi}{\to} G \to 1$$

of $K$ by $G$, where $E_{(\xi, \psi)}$ is the group consisting of all pairs $(x, k), x \in G, k \in K$, with multiplication defined by

$$(x, k)(y, l) = (xy, \psi(x, y) + k^{\psi(y)} + l).$$

The second and third maps in the short exact sequence are inclusion $i: k \to (1, k)$ and projection $\pi: (x, k) \to x$.

In general, an extension of $K$ by $G$ is a short exact sequence $0 \to K \to E \to G \to 1$ of groups; $K$ (or more properly its image in $E$) is the kernel of the extension and $G$ the quotient. The middle group $E$ is sometimes
informally referred to as an extension of $K$ by $G$. We will denote the second and third maps in the sequence by $\iota$ and $\pi$, respectively; when $E = E_{(\xi, \phi)}$ for some $(\xi, \phi)$, it is to be understood that $\iota$ and $\pi$ are defined as in the previous paragraph.

Given a pair $(\xi, \phi)$ of set maps satisfying (1), composition of $\xi$ with natural projection $\text{Aut}(K) \to \text{Out}(K)$ yields a homomorphism $\chi: G \to \text{Out}(K)$, called a coupling of $G$ to $K$. Any extension of $K$ by $G$ gives rise to a coupling of $G$ to $K$.

Suppose $\alpha \in \text{Aut}(K)$ and $\theta \in \text{Aut}(G)$. If $\psi: G \times G \to K$ is a set map, then we have set maps $\psi^\alpha$ and $\psi^\theta$ defined by

$$\psi^\alpha(g, h) = \psi(g, h)^\alpha$$

and

$$\psi^\theta(g, h) = \psi(\theta(g), \theta(h)).$$

Hence, we have a right action of $\text{Aut}(K) \times \text{Aut}(G)$ on all set maps $\psi: G \times G \to K$, defined by

$$\psi^{(\alpha, \theta)} = (\psi^\alpha)^\theta.$$

From now on, $K = U$ is a $G$-module. The $G$-module structure of $U$ is specified by a coupling $\chi: G \to \text{Out}(U) = \text{Aut}(U)$; that is, $u^\chi = u^\chi_1$ for $u \in U$ and $g \in G$. We define the abelian groups of 2-cocycles $Z^2(G, U)$, 2-coboundaries $B^2(G, U)$, and the second cohomology group $H^2(G, U) = Z^2(G, U)/B^2(G, U)$ of $G$ with coefficients in $U$, as usual. For example, $Z^2(G, U)$ consists of all set maps $\psi: G \times G \to U$ such that $\psi(1, 1) = 0$ (is normalised) and defining equation (1) modified by replacing "\(\xi(z)\)" with "\(\chi(z)\)." When $G$ and the $G$-module $U$ are clear from the context, the 2-cohomology class of $\psi$ will be denoted $[\psi]$. The canonical extension of $U$ by $G$ associated with $\psi$ is written $E_\psi$; it has coupling $\chi$. Given an extension $0 \to U \to E \to G \to 1$ with coupling $\chi$, a normalised transversal function (for the cosets of $\iota U$ in $E$) is a function $\sigma: G \to E$ satisfying $\sigma(1) = 1$ and $\pi \sigma(g) = g$ for all $g \in G$. Treating $\iota$ as inclusion, we define an element $\psi_\sigma$ of $Z^2(G, U)$ by

$$\psi_\sigma(g, h) = \sigma(gh)^{-1}\sigma(g)\sigma(h).$$

For another choice $\sigma'$ of normalised transversal function, $[\psi_\sigma] = [\psi'_{\sigma'}]$. Equivalence of extensions, as short exact sequences, is defined in the standard way. Equivalent extensions of $U$ by $G$ with coupling $\chi$ give rise to cohomologous elements of $Z^2(G, U)$. Conversely, if $[\psi] \in H^2(G, U)$ and $\sigma \in [\psi]$ then $0 \to U \xrightarrow{\iota} E_{\psi} \xrightarrow{\pi} G \to 1$ and $0 \to U \xrightarrow{\iota} E_{\sigma} \xrightarrow{\pi} G \to 1$ are
equivalent. So we have the well-known one-to-one correspondence between elements of $H^2(G, U)$ and equivalence classes of extensions of $U$ by $G$ with coupling $\chi$. Note that if $\chi$ is trivial then the extensions concerned are central, meaning that the kernel of each is a central subgroup. Also note that when $U = Z_2$, an extension of $U$ by $G$ is necessarily central.

From now on, “cocycle” means “2-cocycle” unless stated otherwise.

A compatible pair for the coupling $\chi$ is an element $(\alpha, \theta) \in \text{Aut}(U) \times \text{Aut}(G)$ such that

$$
(u^g)^\alpha = (u^\alpha)^{\theta'(g)}
$$

(3)

for all $u \in U$ and $g \in G$. The set of all compatible pairs for $\chi$ forms a subgroup $\text{Comp}(\chi)$ of $\text{Aut}(U) \times \text{Aut}(G)$. We introduced above a right action of $\text{Aut}(U) \times \text{Aut}(G)$ on set maps $G \times G \to U$. The restriction of this action to $\text{Comp}(\chi)$ leaves $Z^2(G, U)$ and $B^2(G, U)$ invariant. So there is an induced right action of $\text{Comp}(\chi)$ on $H^2(G, U)$ defined by $[\psi]^{\alpha, \theta} = [\psi^{\alpha, \theta}]$. This turns $H^2(G, U)$ into a $\text{Comp}(\chi)$-module. Note that if $G$ acts trivially on $U$ then $\text{Comp}(\chi) = \text{Aut}(U) \times \text{Aut}(G)$.

Given $\lambda \in N_{\text{Aut}(E)}(U)$, we have induced automorphisms $\lambda_U$ of $U$ and $\lambda_G$ of $G$, defined by

$$
u^\lambda = \iota^{-1}\lambda^{-1}(1, u), \quad \lambda_G(g) = \pi\lambda(g, 0).
$$

Then it may be verified that $(\lambda_U, \lambda_G) \in C_{\text{Comp}(\chi)}([\psi])$. Conversely, for each $(\alpha, \theta) \in C_{\text{Comp}(\chi)}([\psi])$ we define $\lambda_{(\alpha, \theta)} \in N_{\text{Aut}(E)}(U)$ by

$$
\lambda_{(\alpha, \theta)}(g, u) = (\theta(g), (u - \phi(g))^{-1}),
$$

where $\phi: G \to U$ is a normalised 1-cocchain giving rise to the 2-coboundary $\psi^{(\alpha, \theta)} - \psi$; that is, $\psi^{(\alpha, \theta)}(g, h) = \psi(g, h) + \phi(g)^h + \phi(h) - \phi(gh)$ for all $g, h \in G$. The proof of the following result proceeds directly from the definitions (cf. 18, (4.1)°).

**Proposition 2.1.** Let $[\psi] \in H^2(G, U)$. For $\lambda \in N_{\text{Aut}(E)}(U)$ and $(\alpha, \theta) \in C_{\text{Comp}(\chi)}([\psi])$, the set maps defined by the assignments

$$
(\lambda_U, \lambda_G)
$$

are mutually inverse, and so there is a one-to-one correspondence between $N_{\text{Aut}(E)}(U)$ and $C_{\text{Comp}(\chi)}([\psi])$.

Suppose that $0 \to U \xrightarrow{\iota_1} E_1 \xrightarrow{\pi_1} G \to 1$ and $0 \to U \xrightarrow{\iota_2} E_2 \xrightarrow{\pi_2} G \to 1$ are extensions of $U$ by $G$ with coupling $\chi$, and $\mu: E_1 \to E_2$ is an isomorphism.
We say that \( \mu \) leaves \( U \) invariant if \( \mu \) leaves \( U \) invariant. Of course, an equivalence between extensions of \( U \) by \( G \) with coupling \( \chi \) is an isomorphism which leaves \( U \) invariant.

**Theorem 2.2.** Extensions in the equivalence classes corresponding to \([\psi], [g] \in H^2(G, U)\) are isomorphic by an isomorphism leaving \( U \) invariant if and only if \([\psi] \) and \([g] \) lie in the same orbit under the action of \( \text{Comp}(\chi) \) on \( H^2(G, U) \).

**Proof.** See [5, Theorem 2.1], for example. \( \square \)

Theorem 2.2 seems to be quite well known. It forms the basis of our method of classifying Hadamard groups. Note that when the action of \( G \) on \( U \) is trivial, we may replace "\( \text{Comp}(\chi) \)" in Theorem 2.2 by "\( \text{Aut}(U) \times \text{Aut}(G) \)" in general, and by "\( \text{Aut}(G) \)" when \( U = \mathbb{Z}_2 \).

The stipulation in Theorem 2.2 that \( U \) is left invariant cannot be removed, not even in the case \( U = \mathbb{Z}_2 \) of immediate interest. For the sake of completeness, we provide an example illustrating this fact. We seek a group \( E \) with two isomorphic central subgroups \( U_1 \) and \( U_2 \) such that \( E/U_1 \cong E/U_2 \) and no element of \( \text{Aut}(E) \) maps \( U_1 \) onto \( U_2 \). Let \( \iota \) be an isomorphism of \( U_1 \) onto \( U_2 \), let \( \pi \) be the composite of natural projection \( E \to E/U_2 \) and an isomorphism of \( E/U_2 \) onto \( E/U_1 \), and set \( G = E/U_1 \).

Then \( 0 \to U_1 \to E \to G \to 1 \) and \( 0 \to U_1 \to E \xrightarrow{\pi} G \to 1 \) are inequivalent, and the cocycle classes corresponding to their equivalence classes lie in distinct \( (\text{Aut}(U_1) \times \text{Aut}(G)) \)-orbits by Theorem 2.2. The following example, due to L. G. Kovacs and E. A. O'Brien, is probably the smallest order central extension of the kind that we are seeking.

**Example 2.3.** Let \( E \) be the group of nilpotency class 3 and order 128, with generators \( x, y \) and relations

\[
x^4[y, x]^2[y, y, x] = x^4[y, x, x] = y^4 = 1.
\]

(Here, \([a, b] = a^{-1}b^{-1}ab \) and \([a, b, c] = [[a, b], c] \).) Set \( U_1 = \langle [y, x, x] \rangle \) and \( U_2 = \langle [y, x, y] \rangle \). Both \( U_1 \) and \( U_2 \) are central subgroups of \( E \) of order 2. In fact, the center of \( E \) is

\[
\langle (x^{-1}y^{-1})^2 \rangle \times U_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2
\]

and so \( U_2 = \langle (x^{-1}y^{-1})^2 \rangle \) is a characteristic subgroup of \( E \). Furthermore, it may be shown that \( E/U_1 \cong E/U_2 \). So \( E, U_1, U_2 \) is a triple with the requisite properties.

Theorem 2.2 is sufficient for the purpose of classifying Hadamard groups under the fine criterion discussed at the beginning of the section.
However, Example 2.3 shows that the theorem is not sufficient to deal with the more general problem of classifying central extensions by isomorphism type. Since the omission of \( U \)-invariance in the statement of Theorem 2.2 renders the statement false, we might ask whether weaker versions of the modified statement, applicable to special classes of quotient \( G \) and/or kernel \( U \), are true. This question has apparently not been settled even in the case of finite abelian \( G \).

3. A FUNDAMENTAL CORRESPONDENCE

We say that \( \psi \in Z^2(G, \mathbb{Z}_2) \) is an orthogonal cocycle if a cocyclic matrix associated with \( \psi \) is Hadamard.

**Lemma 3.1.** Let \( G \) be a group of order \( 4t \), \( t \geq 1 \). Then \( \psi \in Z^2(G, \mathbb{Z}_2) \) is orthogonal if and only if, for each \( h \in G \setminus \{1\} \), the number of \( g \in G \) such that \( \psi(g, h) = 1 \) is \( 2t \); equivalently, if and only if, for each \( g \in G \setminus \{1\} \), the number of \( h \in G \) such that \( \psi(g, h) = 1 \) is \( 2t \).

**Proof.** A proof of this simple but vital result depends only on the cocycle defining eq. (1) and the fact that a matrix with entries \( \pm 1 \) is Hadamard if and only if its transpose is Hadamard. See [1, Lemma 2.6].

**Remark 3.2.** We emphasize that a cocycle in the same cohomology class as an orthogonal cocycle need not itself be orthogonal.

The following definitions are due to Ito [13]. A Hadamard group is a group \( E \) of order \( 8t \), \( t \geq 1 \), containing a central subgroup \( \langle e^* \rangle \equiv \mathbb{Z}_2 \) such that there is a transversal \( \mathcal{D} \) for the cosets of \( \langle e^* \rangle \) in \( E \) with

\[
|\mathcal{D} \cap \mathcal{D} x| = 2t \quad \text{for all} \quad x \in E \setminus \langle e^* \rangle.
\]

A transversal of this kind is called a Hadamard subset of \( E \). Note that a given transversal \( \mathcal{D} \) for the cosets of \( \langle e^* \rangle \) in \( E \) is a Hadamard subset of \( E \) if and only if \( \mathcal{D} y \) is a Hadamard subset of \( E \), for all \( y \in E \). In particular, we may assume that \( 1 \in \mathcal{D} \).

**Proposition 3.3.** Let \( E \) be a Hadamard group of order \( 8t \), \( t \geq 1 \), with distinguished central subgroup \( \langle e^* \rangle \equiv \mathbb{Z}_2 \). Denote the isomorphism of \( \mathbb{Z}_2 \) onto \( \langle e^* \rangle \) by \( \iota \) and write \( G = E / \langle e^* \rangle \). If \( [\psi] \in H^1(G, \mathbb{Z}_2) \) corresponds to the equivalence class of central extensions of \( \mathbb{Z}_2 \) by \( G \) containing \( 1 \to \mathbb{Z}_2 \to E \) proj. \( \to G \to 1 \), then \([\psi]\) contains an orthogonal cocycle.

**Proof.** Let \( \mathcal{D} = \{d_1, d_2, \ldots, d_{4t}\} \) be a Hadamard subset of \( E \), and define a normalised transversal function \( \sigma : G \to \mathcal{D} \) by \( \sigma : d_1, \langle e^* \rangle \to d_i \). Defining \( \psi_\sigma \in Z^2(G, \langle e^* \rangle) \) as in (2), we observe that \( \psi_\sigma(g, h) = 1 \) if and
only if \( \sigma(g) \sigma(h) \in D \). Then for fixed \( h \in G \setminus \{1\} \), and since \( \sigma \) is one-to-one, the number of \( g \in G \) such that \( \psi_\sigma(g, h) = 1 \) is \( |D \cap D \sigma(h)^{-1}| = 2t \) by (4). Therefore, \( \psi = \iota^{-1} \psi_\sigma \) is orthogonal, by Lemma 3.1.

**Proposition 3.4.** Let \( G \) be a group of order \( 4t \), \( t \geq 1 \), and suppose that \( \psi \in Z^2(G, \mathbb{Z}_2) \) is orthogonal. Then there is an extension \( 1 \to \mathbb{Z}_2 \to E \to G \to 1 \) in the equivalence class of central extensions of \( \mathbb{Z}_2 \) by \( G \) corresponding to \( [\psi] \), such that \( E \) is a Hadamard group.

*Proof.* Define \( E = E_\psi \) as in Section 2. Set \( e^* = (1, -1) \); then

\[
D = \{(g, 1) \mid g \in G\}
\]

is a transversal for the cosets of \( \langle e^* \rangle \) in \( E \). Choose \( (h, u) \in E \setminus \langle e^* \rangle \).

Since \( (g, 1)(h, u) = (gh, u \psi_\sigma(g, h)) \), the number of elements \( (g, 1) \) of \( D \) such that \( (g, 1)(h, u) \in D \) is \( 2t \), by Lemma 3.1. Hence \( |D \cap D(h, u)| = 2t \), and so \( E \) is a Hadamard group.

An extension of \( \mathbb{Z}_2 \) by \( G \) that is equivalent to a Hadamard group (as short exact sequences) is itself a Hadamard group. However, if \( E_\psi \) is a Hadamard group, then it does not necessarily follow that \( \psi \) is an orthogonal cocycle (see Remark 3.2).

By combining Propositions 3.3 and 3.4, we have the following.

**Theorem 3.5.** There is a one-to-one correspondence between the set of elements of \( H^2(G, \mathbb{Z}_2) \) containing orthogonal cocycles, and the set of equivalence classes of central extensions of \( \mathbb{Z}_2 \) by \( G \) containing Hadamard groups.

Proposition 3.3 provides one way in which a Hadamard matrix can be obtained from a Hadamard group. Another way of doing this is given in [10]. We describe next the relationship between the Hadamard matrices obtained by both methods.

Let \( D = \{d_1 = 1, d_2, \ldots, d_{4t}\} \) be a Hadamard subset of a Hadamard group \( E \) and define the cocycle \( \psi \) as in the proof of Proposition 3.3. Then a cocyclic Hadamard matrix \( M = (m_{i,j}) \) associated with \( \psi \) has rows and columns indexed \( d_1 \langle e^* \rangle, \ldots, d_{4t} \langle e^* \rangle \), where

\[
m_{i,j} = \begin{cases} 
 1 & \text{if } d_id_j \in D, \\ 
 -1 & \text{if } d_id_j \in De^*. 
\end{cases}
\]

In [10, Sect. 4], a Hadamard matrix \( H(E) = (h_{i,j}) \) is defined as follows:

\[
h_{i,j} = \begin{cases} 
 1 & \text{if } d_id_j^{-1} \in D, \\ 
 -1 & \text{if } d_id_j^{-1} \in De^*. 
\end{cases}
\]
For a given \( j \), either \( d_{-1} = d_k \) or \( d_{-1} = d_k e^n \) for some \( d_k \in D \). In the former case, interchanging the \( j \)th and \( k \)th columns of \( H(E)^T \) produces a matrix with the same \( j \)th and \( k \)th columns as \( M \). In the latter case, interchanging the \( j \)th and \( k \)th columns of \( H(E)^T \) after multiplication of those columns by \(-1\) produces a matrix with the same \( j \)th and \( k \)th columns as \( M \). These observations imply the following result.

**Proposition 3.6.** In the notation above, \( H(E)^T \) is Hadamard equivalent to \( M \).

Proposition 3.6 reflects a certain duality of matching definitions in the combinatorial design theory associated with cocyclic Hadamard matrices and Hadamard groups. This is described fully in [9].

We now note some other constructions and results in [10] that can be expressed efficiently in terms of cocyclic matrices.

Suppose \( G_1 \) and \( G_2 \) are groups acting trivially on \( U \), the latter now being written multiplicatively. If \( \psi \in \mathbb{Z}^2(G_1, U) \) and \( \varphi \in \mathbb{Z}^2(G_2, U) \) then \( \psi \otimes \varphi \in \mathbb{Z}^2(G_1 \times G_2, U) \) is defined by

\[
\psi \otimes \varphi((g_1, g_2), (h_1, h_2)) = \psi(g_1, h_1) \varphi(g_2, h_2).
\]

The use of notation here is suggestive: a cocyclic matrix associated with \( \psi \) is the tensor (Kronecker) product of cocyclic matrices associated with \( \psi \) and \( \varphi \). The assignment

\[
((g_1, u), (g_2, v)) \mapsto ((g_1, g_2), uv)
\]

defines an epimorphism of \( E\psi \times E\varphi \) onto \( E_{\psi \otimes \varphi} \). When \( U = \langle -1 \rangle \), the kernel \( K \) of this epimorphism is \( \langle ((1, -1), (1, -1)) \rangle \cong \mathbb{Z}_2 \). If \( \psi \) and \( \varphi \) are orthogonal then the tensor product of their associated cocyclic matrices is Hadamard; thus \( \psi \otimes \varphi \) is orthogonal and \( E_{\psi \otimes \varphi} \) is a Hadamard group. This implies that \( (E\psi \times E\varphi)/K \), as an isomorphic copy of \( E_{\psi \otimes \varphi} \), is a Hadamard group. Its distinguished central subgroup of order 2 and a Hadamard subset may be written down after applying the (inverse of the) above isomorphism to the corresponding subgroup and subset of \( E_{\psi \otimes \varphi} \). This gives Proposition 3 of [10].

A Hadamard group \( E \) splits over its distinguished central subgroup of order 2 if and only if an associated cocyclic matrix is Hadamard equivalent to a group developed matrix. A matrix of the latter type is regular (it has the same number of occurrences of 1 in every row), and consequently has side a perfect square. This yields Proposition 5 of [10]. The order restriction in Proposition 2 of [10] could be deduced from an associated cocyclic matrix; as is very well known, a Hadamard matrix has side 1, 2, or a
multiple of 4. This restriction has been incorporated into the definitions of Hadamard group and cocyclic Hadamard matrix, where the trivial cases have been ignored for convenience.

Propositions 6 and 7 of [10] place restrictions on the type of Sylow 2-subgroup that a Hadamard group can have. Consequences of the restrictions for cocyclic Hadamard matrices have been previously observed; we examine these in Section 5.

4. CONSTRUCTION OF HADAMARD GROUPS

By the correspondence established in Theorem 3.5, we may consider that a Hadamard group is known once a corresponding cocyclic Hadamard matrix has been determined. Throughout this paper, “construction” of Hadamard groups will be interpreted in this sense. Certainly, it is not difficult to write down a presentation for a central extension from presentations of its kernel and quotient, if we have a cocyclic matrix associated with an element in the corresponding 2-cohomology class.

Let $G$ be a finite group. As remarked earlier, basic isomorphism between central extensions of $\mathbb{Z}_2$ by $G$ defines a natural equivalence relation on the set of all Hadamard groups with specified quotient $G$ modulo $\mathbb{Z}_2$. In this section we give a procedure for constructing a representative from each basic isomorphism class.

Suppose that $G$ acts trivially on the finitely generated abelian group $U$. An explicit universal coefficient theorem decomposition of $H^2(G, U)$ is described in [4]. This decomposition is dependent on the choice of a presentation $F/R$ of $G$, and consequent choices of “Schur complement” $S/\left[R \cap F, F\right]$ of $R \cap F'/\left[R, F\right]$ in $R/\left[R, F\right]$ and Schur covering group $F/S$ of $G$. The central subgroup $R/S$ of $F/S$ is isomorphic to the Schur multiplier $H_2(G)$ of $G$, an invariant of $G$. Denote by $\left[\mu\right]$ the element of $H^2(F/R, R/S)$ corresponding to the equivalence class of

$$1 \to R/S \to F/S \to F/R \to 1.$$ 

Transgression is the homomorphism $\tau_S \colon \text{Hom}(R/S, U) \to H^2(F/R, U)$ defined by

$$\tau_S(\phi) = [\phi \circ \mu].$$

If $A$ is an abelian group acting trivially on $U$, then $\psi \in Z^2(A, U)$ is symmetric if $\psi(a, b) = \psi(b, a)$ for all $a, b \in A$ (the corresponding central extensions of $U$ by $A$ are abelian). Then $\text{Ext}(A, U)$ denotes the subgroup $\{[\psi] \in H^2(A, U) \mid \psi \text{ is symmetric}\}$ of $H^2(A, U)$. The inflation homomor-
Hadamard Matrices and Groups 759

\( \varphi\) inf: \( \text{Ext}(G/G', U) \rightarrow H^2(G, U) \) is defined by \( \inf[\psi] = [\inf \psi] \), where 
\( \inf \psi(g, h) = \psi(gG', hG') \) for all \( g, h \in G \). Having made the necessary definitions, we now state our universal coefficient theorem decomposition:

\[
H^2(G, U) = \text{im}(\inf) \oplus \text{im}(\tau_3),
\]

(5)

where \( G \) is identified with \( F/R \). Note that any Schur covering group of \( G \) (central extension with kernel \( H_2(G) \) and quotient \( G \), whose derived subgroup contains the kernel) may be used to define transgression \( \text{Hom}(H_2(G), U) \rightarrow H^2(G, U) \), and then \( \tau_3 \) may be replaced by this transgression in (5).

Next, we describe the action of \( \text{Ext}(G/G', U) \rightarrow H^2(G, U) \) in terms of cocyclic matrices. If \( [\psi] \in \text{Ext}(G/G', U) \), then a cocyclic matrix associated with the representative \( \psi \) of \( \text{Ext}(\psi) \) is obtained as the tensor product of a cocyclic matrix associated with \( \psi \) and the \( |G'| \times |G'| \) all 1s matrix. To obtain a cocyclic matrix associated with \( \psi \), first write \( G/G' = C_1 \times \cdots \times C_n \), where the \( C_i \) are cyclic groups. Then the required cocyclic matrix is the tensor product of representative cocyclic matrices associated with elements of the \( \text{Ext}(C_i, U) = H^2(C_i, U) \), as \( i \) ranges from 1 to \( n \). This is an advantageous reduction, because the cohomology of a finite cyclic group is calculable as sections of the coefficient module. For example, the single nontrivial element of \( H^2(\mathbb{Z}_2, \mathbb{Z}_2) \), \( k \geq 1 \), has representative with associated cocyclic matrix the back negacyclic matrix

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 & 1 \\
1 & 1 & \cdots & 1 & -1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 1 & \cdots & -1 & -1 \\
1 & -1 & \cdots & -1 & -1
\end{pmatrix}
\]

of side \( 2^k \).

Practically, the determination of elements of \( \text{im}(\tau_3) \) depends upon calculating a presentation for a Schur covering group of \( G \) and recognising the copy of \( H_2(G) \) as a subgroup. An algorithm for carrying out this calculation, given a polycyclic group of reasonably small order as input, is described in [17]. Then a corresponding element \( \mu \) of \( Z^2(G, H_2(G)) \) may be written down from first principles. In all applications to cocyclic matrices so far studied, \( \mu \) has been derived by hand. Given this, the method for determining elements of \( \text{im}(\inf) \) discussed above, and (5), we are able to calculate a full set of representative cocyclic matrices for the elements of \( H^2(G, U) \).

A problem which then naturally arises is classifying, by isomorphism type, the central extensions of \( U \) by \( G \) so constructed. That is, we seek to
determine when \( E_\psi \cong E_\phi \) for distinct elements \([\psi],[\phi]\) of \( H^2(G,U)\) (this is sufficient, since any central extension of \( U \) by \( G \) in the equivalence class corresponding to \([\psi]\) is isomorphic to \( E_\psi \)). Theorem 2.2 may be used to account for all isomorphisms which leave \( U \) invariant without actually constructing extensions, by listing representatives of each orbit in \( H^2(G,U) \) under the action of \( \text{Aut}(U) \times \text{Aut}(G) \). As indicated in the discussion framing Example 2.3, there is no comparably straightforward method for determining isomorphisms which do not leave \( U \) invariant.

Now let us specialise to the task of constructing and classifying by basic isomorphism type all Hadamard groups with quotient \( G \) modulo \( \mathbb{Z}_2 \). A procedure for carrying out this task begins with determination of a set of representatives for the elements of \( H^2(G,\mathbb{Z}_2) \). Then representatives for the \( \text{Aut}(G) \)-orbits in \( H^2(G,\mathbb{Z}_2) \) are found. (\( \text{Aut}(G) \)-action translates to Hadamard equivalence operations on associated cocyclic matrices.) After completion of this step, all potential basic isomorphism classes of Hadamard groups with quotient \( G \) modulo \( \mathbb{Z}_2 \) have been found. The final step is to test cocycles in each \( \text{Aut}(G) \)-orbit representative for orthogonality. The task of orthogonality-testing is relegated to a computer; note that the number of cocycles is exponential in \(|G|\). There is no way of knowing \emph{a priori} which elements of \( H^2(G,\mathbb{Z}_2) \) contain orthogonal cocycles. Neither is it sufficient to test a single representative from each cohomology class for orthogonality, since (by Remark 3.2) this property is not respected by cohomological equivalence. However, for a given \( \text{Aut}(G) \)-orbit representative, testing of elements in that cocycle class can stop as soon as an orthogonal cocycle has been found. The outlined procedure determines all Hadamard groups with quotient \( G \) modulo distinguished central subgroup \( \mathbb{Z}_2 \), up to basic isomorphism.

For the example studied in Section 6, it will be seen that the action of \( \text{Aut}(U) \times \text{Aut}(G) \) on \( H^2(G,U) \) accounts for \emph{all} isomorphism between the corresponding central extensions of \( U \) by \( G \). Some results used in proving this claim are given below. For the rest of this section, \( \text{inf} \) denotes inflation \( \text{Ext}(G/U,G) \rightarrow H^2(G,U) \).

Denote the centre of a group \( K \) by \( \zeta(K) \). Clearly, if \([\psi] \in H^2(G,U)\) then

\[
\zeta(E_\psi) = \{(z,u) \in E_\psi | u \in U, z \in \zeta(G), \psi(z,g) = \psi(g,z) \forall g \in G\}.
\]

(6)

If \([\psi] \in \text{im}(\text{inf})\) then \( \psi(g,h) = \psi(h,g) \) for all \( g, h \in G \) such that \([g,h] = 1\). In this case, by (6), \( \zeta(E_\psi) \) is as large as possible: \(|\zeta(E_\psi)| = |\zeta(G)||U|\).

(In Example 2.3, \(|\zeta(E)| = |\zeta(E/U)| = 8\), so that the equivalence class of \( E \) does not correspond to an inflation cocycle class in \( H^2(E/U,U)\).)
**Lemma 4.1.** Choose a presentation $F/R$ of $G$ and Schur complement $S/[R,F]$. Denote by $Z$ the complete inverse image in $F$ of $\zeta(F/R)$ under natural projection. If $\phi \in \text{Hom}(R/S,U)$ and $E$ is a central extension of $U$ by $G$ whose corresponding cocycle class has $\text{im}(\tau_3)$-component $\tau_3(\phi)$, then

$$\zeta(E) = \{(zR,u) \in E | u \in U, z \in Z, \phi([z,f]S) = 1 \forall f \in F\}.$$ 

**Proof.** Proceeding from (6), the method of proof is similar to that of Lemma 4.1 in [4].

Now $\theta \in \text{Aut}(G) = N_{\text{Aut}(G)}(G')$ induces $\theta_{G'/G} \in \text{Aut}(G'/G')$, and it is readily checked that $(\text{inf } \varrho)^{(\alpha, \theta)} = \text{inf } \varrho^{(\alpha, \theta)}$ for $\varrho \in Z^2(G'/G',U)$ and $(\alpha, \theta) \in \text{Aut}(U) \times \text{Aut}(G)$. Thus $\text{im}($inf$)$ is invariant under the action of $\text{Aut}(U) \times \text{Aut}(G)$. In fact, more is true, as (i) of the next lemma shows.

**Lemma 4.2.** (i) If $[\psi] \in \text{im}($inf$)$, $[\varrho] \in H^2(G,U)$ and $E_\psi \cong E_\varrho$, then $[\varrho] \in \text{im}($inf$)$.

(ii) If $[\psi],[\varrho] \in \text{Ext}(G'/G',U)$ and $E_{\text{inf } \psi} \cong E_{\text{inf } \varrho}$ then $E_\psi \cong E_\varrho$.

**Proof.** Both parts depend on the observation that

$$\text{im}($inf$)$ = $[\psi] \in H^2(G,U) | E_\psi = G' \times 1,$$

for which see [15, 2.17, p. 24]. (In other words, elements of $\text{im}($inf$)$ are characterised by the fact that central extensions in their corresponding equivalence classes have derived subgroup as small as possible.) Then (i) is clear. For any $[\psi] \in \text{Ext}(G'/G',U)$ we have $E_{\text{inf } \psi} / E_{\text{inf } \varrho} \cong E_\psi$, so that (ii) also follows easily.

Since $\text{Aut}(U) \times \text{Aut}(G)$ leaves $\text{im}($inf$)$ invariant, $\text{Aut}(U) \times \text{Aut}(G)$ is intransitive on $H^2(G,U)$ when $\tau_3$ is nontrivial. In the next section we will see that $\text{Aut}(U) \times \text{Aut}(G)$ leaves $\text{im}(\tau_3)$ invariant for $G$ dihedral and a certain choice of $S$: this will be established by the results below. In general, $\text{Aut}(U) \times \text{Aut}(G)$ does not leave $\text{im}(\tau_3)$ invariant. However, note that $\text{Aut}(U)$ leaves $\text{im}(\tau_3)$ invariant, and that $E_{\psi^\mu}$ is a Schur covering group of $G$ for each $\theta \in \text{Aut}(G)$ and $\mu \in Z^2(G,H_3(G))$ corresponding to a Schur covering group of $G$. From this we deduce that $\text{Aut}(U) \times \text{Aut}(G)$ maps $\text{im}(\tau_3)$ onto the image of a transgression defined according to another choice of Schur cover (rather than another choice of Schur complement).

The next result is a restatement of Proposition 2.1.

**Proposition 4.3.** Choose a presentation $F/R$ of $G$ and Schur complement $S/[R,F]$. Denote by $[\mu]$ the element of $H^2(F/R, R/S)$ corresponding
to the equivalence class of
\[ 1 \to R/S \to F/S \to F/R \to 1. \]

Then \( [\mu]^{(\alpha, \theta)} = [\mu] \) for \((\alpha, \theta) \in \text{Aut}(R/S) \times \text{Aut}(F/R)\) if and only if there exists \( \lambda \in N_{\text{Aut}(F/R)(R/S)} \) such that
\[
\lambda_{R/S} = \alpha, \quad \lambda_{F/R} = \theta.
\]

**Corollary 4.4.** Choose a presentation \( F/R \) of \( G \) and Schur complement \( S/[R, F] \). If for each \( \theta \in \text{Aut}(F/R) \) there exists \( \lambda \in N_{\text{Aut}(F/R)(R/S)} \) such that \( \lambda_{F/R} = \theta \), then \( \text{Aut}(U) \times \text{Aut}(G) \) leaves \( \text{im}(\tau) \) invariant.

## 5. Existence of Cocyclic Hadamard Matrices Developed over Abelian, Dicyclic, and Dihedral Groups

Let \( \psi \in \mathbb{Z}^2(G, \mathbb{Z}_2) \) be an orthogonal cocycle. In this section we derive restrictions on \( \psi \) for particular types of \( G \). Specifically, we will show that if \( G \) is cyclic or a dicyclic group then \( \psi \) is necessarily a coboundary (and so the corresponding Hadamard groups are direct products). We will also exclude certain classes in \( H^2(G, \mathbb{Z}_2) \) as sources of orthogonal cocycles, for \( G \) dicyclic or abelian of type \( \mathbb{Z}_2^2 \times \mathbb{Z}_t \), \( t > 1 \). The case of dihedral \( G \) will be treated at length both in this section and the next, as an application of the procedure discussed in Section 4 for constructing and classifying Hadamard groups.

If there is a cocyclic Hadamard matrix \( M \) developed over \( G \) then there is a cocyclic Hadamard matrix developed over \( G \times \mathbb{Z}_2 \), obtained as the tensor product of \( M \) with the \( 2 \times 2 \) back negacyclic matrix. Hence, the atomic cases to consider in development over abelian groups are \( G = \mathbb{Z}_2 \times \mathbb{Z}_t \), \( t \geq 1 \) odd, and \( G \) cyclic of order divisible by 4. The former case is studied in [1]. Here, we begin with a simple argument concerning development over cyclic groups.

Let
\[
G = \langle a, b | a^t = b^4 = [a, b] = 1 \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_t,
\]
where \( t > 1 \) is odd, and set \( N = \langle a \rangle \). Certainly \( H^i(\mathbb{Z}_i, \mathbb{Z}_2) = 0 \) for all \( i \geq 1 \) and so by [16, Corollary 10.3 p. 354], inf: \( H^2(G/N, \mathbb{Z}_2) \to H^2(G, \mathbb{Z}_2) \) is an isomorphism. Consequently \( H^2(G, \mathbb{Z}_2) \cong H^2(\mathbb{Z}_4, \mathbb{Z}_2) \approx \mathbb{Z}_2 \). The single nontrivial cocycle class in \( H^2(G, \mathbb{Z}_2) \) has representative cocyclic matrix the tensor product of the \( 4 \times 4 \) back negacyclic matrix with the \( t \times t \) all 1s matrix. Thus an element of the nontrivial class in \( H^2(G, \mathbb{Z}_2) \) has cocyclic matrix
\[
\begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1
\end{pmatrix}
\]
HADAMARD MATRICES AND GROUPS 763

matrix Hadamard equivalent to a matrix of the form

\[
\begin{pmatrix}
X_1 & X_2 & \cdots & X_t \\
X_2 & X_3 & \cdots & X_1 \\
\vdots & \vdots & \ddots & \vdots \\
X_t & X_1 & \cdots & X_{t-1}
\end{pmatrix}
\]

where each $4 \times 4$ block $X_i$ is the entrywise product of a back circulant with a back negacyclic matrix. This matrix is Hadamard if and only if

(i) $\sum_{i=1}^t X_i^2 = 4t I_4$,
(ii) $\sum_{i=1}^t X_i X_{i+k+i} = 0$, $1 \leq k < t$,

where $\mid \cdot \mid_t$ denotes remainder mod $t$. These conditions imply that

\[
\left( \sum_{i=1}^t X_i \right)^2 = 4t I_4.
\]

Write the first row of $X_j$ as $x_1, x_2, x_3, x_4$. Now $\sum_{i=1}^t X_i$ is of the same form as the blocks $X_i$, with first row $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, where $\lambda_j = \sum_{i=1}^t x_{i,j}$. Note that $\lambda_j$ is odd. Then $(\sum_{i=1}^t X_i)^2 = 4t I_4$ is equivalent to the conditions

\[
\sum_{j=1}^4 \lambda_j^2 = 4t, \quad \lambda_1 \lambda_2 + \lambda_2 \lambda_3 + \lambda_3 \lambda_4 - \lambda_4 \lambda_1 = 0.
\]

Setting $\lambda_4 = 2m + 1$, $\lambda_2 = 2n + 1$, we see that the second of these identities may be rewritten as $\lambda_4(m - n) = \lambda_2(m + n + 1)$. But this contradicts the fact that precisely one of $m - n$ or $m + n + 1$ is even. Hence orthogonal cocycles developed over $\mathbb{Z}_4 \times \mathbb{Z}_t$ are coboundaries and possibly exist only for square $t$.

**Proposition 5.1.** If $t > 1$ is odd, existence of a cocyclic Hadamard matrix over $\mathbb{Z}_4 \times \mathbb{Z}_t$ is equivalent to the existence of a (back) circulant Hadamard matrix of side $4t^2$.

Proposition 5.1 is true for $t = 1$. In fact, this is the only value of $t$ for which circulant Hadamard matrices are known. The circulant Hadamard conjecture is that there are no circulant Hadamard matrices of side greater than 4. It has been verified for all sides $4t^2$, $1 < t < 57$ (see [2, Remark 24.15, p. 371]). This dissuades us from searching for cocyclic Hadamard matrices developed over cyclic groups.

Proposition 5.1 is a special case of the more powerful Proposition 7 in [10]. The latter result, together with Proposition 6 of [10], suggest that the
Sylow 2-subgroup of an extension of \( Z_2 \) is significant in determining whether the extension is a Hadamard group. In the rest of this section we explore this idea.

Let \( G \) be a finite group with Sylow 2-subgroup \( P \) and denote by \( \text{res} \) the restriction homomorphism \( H^2(G, \mathbb{Z}_2) \to H^2(P, \mathbb{Z}_2) \). Clearly, if \( [\psi] \in H^2(G, \mathbb{Z}_2) \) then a Sylow 2-subgroup of \( E_\psi \) is \( E_{\text{reg}\psi} \).

**Lemma 5.2.** Suppose \( G \) is a group with cyclic Sylow 2-subgroups. If there is a cocyclic Hadamard matrix developed over \( G \) then it must be associated with a coboundary (and so \( |G| \) is necessarily a square).

**Proof.** Let \( P \) be a Sylow 2-subgroup of \( G \). There is a normal complement of \( P \) in \( G \) (see [19, 6.2.11, p. 138]), and so via inflation we have \( H^2(G, \mathbb{Z}_2) \cong H^2(P, \mathbb{Z}_2) \cong \mathbb{Z}_2 \). If \( [\psi] \) denotes the unique nontrivial class in \( H^2(G, \mathbb{Z}_2) \), then

\[
\text{cor}(\text{res}[\psi]) = [\psi]^{[G: P]} = [\psi]
\]

(see [15, 1.5.8, p. 10]), where \( \text{cor}: H^2(P, \mathbb{Z}_2) \to H^2(G, \mathbb{Z}_2) \) is corestriction. Hence \( \text{res}[\psi] \) is the nontrivial class in \( H^2(P, \mathbb{Z}_2) \). Since a non-splitting extension of \( \mathbb{Z}_2 \) by \( P \) is cyclic, the result follows from [10, Proposition 7].

The dicyclic group of order \( 4t \) (\( t > 1 \)), denoted \( Q_{4t} \), has presentation

\[
\langle x, y \mid x^{2t} = 1, y^2 = x^t, y^{-1}xy = x^{-1} \rangle.
\]

For odd \( t \), \( Q_{4t} \) is a split extension \( \langle x^2 \rangle \rtimes \langle y \rangle \cong \mathbb{Z}_t \rtimes \mathbb{Z}_4 \). So we have the following as a direct consequence of Lemma 5.2.

**Corollary 5.3.** Let \( G \) be a cyclic group or \( Q_{4t}, t > 1 \) odd. Then a cocyclic Hadamard matrix developed over \( G \) is necessarily associated with a coboundary.

Corollary 5.3 strengthens Proposition 5.1. The reasoning which established Corollary 5.3 cannot be extended to \( Q_{4t} \) for all \( t > 1 \); an analysis such as that carried out below for dihedral \( G \) is possible (computer checks have verified the corollary for several small even values of \( t \)).

Denote by \( D_{4t} \) the dihedral group of order \( 4t, t \geq 1 \), given by the presentation

\[
\langle a, b \mid a^{2t} = b^2 = (ab)^2 = 1 \rangle.
\]

We proceed to describe explicitly representatives for the elements of \( H^2(D_{4t}, \mathbb{Z}_2) \).
First, \( \text{Ext}(D_4; D_4, \mathbb{Z}_2) = \text{Ext}(aD_4, bD_4, \mathbb{Z}_2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \). Representatives for the elements of the inflation component in a decomposition (5) of \( H^2(D_4, \mathbb{Z}_2) \) are easily obtained by the discussion following (5).

In this case, the transgression component, for a particular choice of Schur complement, is dealt with in [4, Sect. 5]. There, for the presentation \( F/R \) of \( D_4 \), where \( F \) is the free group \( a, b \) and \( R \) the normal closure in \( F \) of \( \langle a^{2t}, b^2, (ab)^2 \rangle \), it is seen that a Schur complement is

\[
S/[R, F] = \langle b^2[R, F], (ab)^2[R, F] \rangle.
\]

Consequently \( R/S = \langle a^{2t} \rangle = \langle [a', b]S \rangle \cong \mathbb{Z}_2 \) and a presentation of the Schur cover \( F/S \) is

\[
\langle aS, bS | (aS)^{4t} = 1, (bS)^2 = 1, (bS)^{-1}aSb = (aS)^{-1} \rangle.
\]

A normalised transversal function \( \sigma : F/R \to F/S \) is defined by

\[
\sigma : a^{i}b^{k}R \mapsto a^{i}b^{k}S,
\]

for \( 0 \leq i \leq 2t - 1 \) and \( 0 \leq k \leq 1 \), and we define \( \mu \in \mathbb{Z}^2(F/R, R/S) \) accordingly. More detail can be found in [4, Sect. 5]. In summary, a representative \( \psi \) of \( [\psi] \in H^2(D_4, \mathbb{Z}_2) \cong \mathbb{Z}_2(3) \) is written interchangeably as a triple \( (A, B, K) \), where \( A \) and \( B \) are the inflation variables and \( K \) is the transgression variable; all variables take values \( \pm 1 \). Explicitly,

\[
\psi(a', a^{i}b^{k}) = \begin{cases} A^{ij}, & i + j < 2t, \\ A^{i}K, & i + j \geq 2t, \end{cases}
\]

\[
\psi(a'b, a^{i}b^{k}) = \begin{cases} A^{i}B^{k}, & i \geq j, \\ A^{i}B^{k}K, & i < j. \end{cases}
\] (8)

Let \( U \) be a finitely generated abelian group and let \( \tau_3 : \text{Hom}(R/S, U) \to H^2(D_4, U) \) be transgression defined for the choice of \( S \) made above. Before a complete description of \( (\text{Aut}(U) \times \text{Aut}(D_4)) \)-action on \( H^2(D_4, U) \) in the case \( U = \mathbb{Z}_2 \) is given, we show that \( \text{im}(\tau_3) \) is invariant under this action.

Assume \( t > 1 \) and choose \( \theta \in \text{Aut}(F/R) \); note then that \( \theta(aR) = a^{k}R \) for some \( k \) coprime to \( 2t \), and \( \theta(bR) = a^{i}b^{k}R \) for some \( i, 0 \leq i \leq 2t - 1 \). Define

\[
\lambda : aS \mapsto \sigma \theta(aR), \quad bS \mapsto \sigma \theta(bR).
\]

Clearly \( (\lambda(aS))^{4t} = 1 \). If \( \phi \in \text{Hom}(R/S, \mathbb{Z}_2) \) is nontrivial then \( \phi \circ \mu \) is the cocycle defined in (8) for \( (A, B, K) = (1, 1, -1) \), so that \( (\lambda(bS))^{2} = \)
\( \mu(\theta(bR), \theta(bR)) = 1 \) by (8). Also, since \( a'bS \) acts invertingly on \( \langle aS \rangle \), we have \( \lambda(aS)^{a'bS} = \lambda(aS)^{-1} \). Thus \( \lambda \) is an endomorphism of \( F/S \). Since \( k \) is odd, \( \lambda(a^{2k}S) = a^{2k}S = a^{2}S \); that is, \( \lambda_{R/S} = \text{id}_{R/S} \). Furthermore, by definition, \( \lambda_{F/R}(aR) = \theta(aR) \) and \( \lambda_{F/R}(bR) = \theta(bR) \), so that \( \lambda_{F/R} = \theta \). By the five lemma, \( \lambda \) is an automorphism of \( F/S \). Together with Corollary 4.4, all of this implies the following.

**Proposition 5.4.** For \( G = D_{1}, t > 1 \), with presentation (7) and \( S \) chosen as above, \( \text{im}(\tau_{S})^{(\alpha, \theta)} = \text{im}(\tau_{S}) \) for all \( (\alpha, \theta) \in \text{Aut}(U) \times \text{Aut}(G) \).

In Proposition 5.7 we will see that Proposition 5.4 is false for \( t = 1 \). A full set of generators of \( \text{Aut}(D_{1}) \) is required, and this is stated next.

**Lemma 5.5.** Suppose \( G = D_{1}, t > 1 \), with presentation (7). Then \( \text{Aut}(G) \) is generated (not necessarily minimally) by

\[ \theta: \quad a \mapsto a, \quad b \mapsto ab \]

of order \( 2t \) and, for each \( k \) coprime to \( 2t \),

\[ \eta_{k}: \quad a \mapsto a^{k}, \quad b \mapsto b. \]

One further preliminary lemma is needed before we can give the orbit partition of \( H^{2}(D_{1}, \mathbb{Z}/2) \) under the action of \( \text{Aut}(D_{1}) \).

**Lemma 5.6.** If \( \psi \in Z^{2}(D_{1}, \mathbb{Z}/2) \) is defined as in (8) then, for each \( q \in [\psi] \),

(i) \( B = q(b, b) \),

(ii) \( A = q(a, b)q(ab, a) \).

**Proof.** Suppose \( \varphi \in B^{2}(D_{1}, \mathbb{Z}/2) \) arises from the normalised 1-cochain \( \phi: D_{1} \to \mathbb{Z}/2 \). Then \( \varphi(b, b) = \varphi(b)\varphi(b) = 1 \). Similarly \( \varphi(a, b)\varphi(ab, a) = 1 \). So (i) and (ii) follow from (8). \( \square \)

**Proposition 5.7.** For \( t > 1 \), the \( \text{Aut}(D_{1}) \)-orbit partition of \( H^{2}(D_{1}, \mathbb{Z}/2) \) is

\[ \{(1, 1, 1), (1, 1, -1), (1, 1, 1), (1, 1, -1)\}, \]
\[ \{(-1, 1, 1), (-1, 1, 1), (-1, 1, -1), (-1, 1, -1)\}. \]

For \( t = 1 \), the partition is

\[ \{(1, 1, 1), (1, -1, -1)\}, \]
\[ \{(1, 1, -1), (1, -1, -1), (-1, 1, -1), (-1, 1, -1)\}, \]
\[ \{(-1, 1, 1), (1, -1, 1), (-1, -1, 1)\}. \]
Proof. Choose an arbitrary element of $H^2(D_{4t}, \mathbb{Z}_2)$, whose representative $\psi$ is written $(A, B, K)$ and is defined by (8). For $\nu \in \text{Aut}(D_{4t})$, denote the triple representing $[\psi]^{\nu}$ by $(A', B', K')$. By Proposition 5.4, $K' = K$. If $\nu = \theta$ as in Lemma 5.5, then Lemma 5.6(ii) and (8) imply that

$$A' = \psi^{\theta}(a, b) \psi^{\theta}(ab, a)$$
$$= \psi(a, ab) \psi(a^2b, a)$$
$$= A.$$ 

If $\nu = \eta_k$ for some $k$ coprime to $2t$ as in Lemma 5.5, then $A' = \psi(a^k, b) \psi(a^kB, a^k) = A^k$ by (8). Thus $A' = A$ for all $\nu \in \text{Aut}(D_{4t})$.

By Lemma 5.6(i), obviously $B' = B$ for $\nu = \eta_k$. For $\nu = \theta$ we have $B' = \psi(ab, ab) = AB$ by (8). Hence, for $t > 1$, $\text{Aut}(D_{4t})$ fixes each element of $H^2(D_{4t}, \mathbb{Z}_2)$ represented by a triple $(1, B, K)$, and partitions the remaining four elements into two orbits of length 2 each.

When $t = 1$, $\text{Aut}(D_{4t}) \cong S_3$ is generated by the involution $\theta$, acting as before, and the 3-cycle $\eta = (a, b, ab)$. Under $\eta$, $B' = AB$ as before, but now $A' = BK$. Thus $(1, -1, -1)$ is a fixed point. The elements represented by $(1, 1, -1), (-1, 1, -1), (1, -1, -1)$, and $(1, -1, 1, 1)$ all lie in the same $\eta$-orbit, hence constitute a full $\text{Aut}(D_{4t})$-orbit. The same statement applies to $(1, -1, 1), (-1, 1, 1)$, and $(1, 1, 1, -1)$.

Write $t = 2s$, where $s$ is odd. A Sylow 2-subgroup $P$ of $D_{4t}$ is $\langle a^s, b \rangle \cong D_{2^{s+1}}$. Select an element of $H^2(D_{4t}, \mathbb{Z}_2)$ and write its representative $\psi$ as $(A, B, K)$ in the usual fashion. Let $\text{res}$ be restriction to $P$. Then in $E_{\text{res} \psi}$ we have the following relations:

$$(a^s, 1)^{2^{s+1}} = \begin{cases} (1, AK), & r = 0, \\ (1, K), & r \geq 1, \end{cases}$$

$$(b, 1)^2 = (1, B),$$

$$(a^s, 1)_{(b, 1)} = (a^s, 1)^{-1}(1, A),$$

together with those identifying $(1, -1)$ as a central involution of $E_{\text{res} \psi}$. It is straightforward to determine a presentation and isomorphism type of $E_{\text{res} \psi}$ for $[\psi]$ in each of the $\text{Aut}(D_{4t})$-orbits found in Proposition 5.7. We list the isomorphism types in Table 1. Here, $SD_{2^n}$ denotes the semidihedral group $\langle x, y | x^{2^{n+1}} = 1, y^2 = 1, x^y = x^{2^{n-1}-1} \rangle$ of order $2^n$. Presentations of $E_{\text{res} \psi}$ for $\psi = (1, -1, 1)$ and $\psi = (-1, 1, 1)$ are

$$\langle x, y | x^{2^{s+1}} = 1, y^4 = 1, x^y = x^{-1} \rangle$$
and

\[ \langle x, y, z | x^{2r+1} = 1, y^2 = 1, z^2 = 1, x^r = x^{-1}z, z^r = z^r = z \rangle, \quad r \geq 1, \]

respectively.

**Proposition 5.8.** If \([\psi] \in H^2(D_4, \mathbb{Z}_2)\) represented by \((A, B, K)\) contains an orthogonal cocycle, then

(i) \((A, B, K) \neq (1, 1, -1)\) for \(t\) even;

(ii) \((A, B, K) \neq (1, 1, -1)\) and \((A, B, K) \neq (-1, -1, -1)\) and \((A, B, K) \neq (-1, 1, -1)\) for \(t\) odd.

**Proof.** By Proposition 6 of [10], \(E_{res} \psi\) cannot be dihedral. The claim then follows from inspection of Table 1 and with reference to Proposition 5.7.

In the next section, we will exhibit orthogonal cocycles over \(D_4\) in the classes represented by \((A, B, K) = (1, -1, 1)\) for all allowable values of \(t\) in the range \(1 \leq t \leq 8\), and \((A, B, K) = (1, -1, -1)\) for \(1 \leq t \leq 11\). In turn, as we will see, this implies that \(Q_{4t}\) for \(1 \leq t \leq 11\) is a Hadamard group. However, no orthogonal cocycles over \(D_4\) have been found in the classes represented by \((A, B, K) = (1, 1, 1)\) or \((-1, 1, 1)\) for \(t > 1\) (when \(t = 1\), there is a single orthogonal cocycle in each of these classes). In fact, for \(t\) odd, existence of orthogonal cocycles in these classes is possible only when \(t\) is the sum of two squares (see Proposition 6.6).

We conclude this section with some remarks about development over

\[ G = \langle a, b | a^{2t} = b^2 = [a, b] = 1 \rangle \cong \mathbb{Z}_2^t \times \mathbb{Z}_t, \quad t \text{ odd}. \]
Cocyclic Hadamard matrices developed over $G$ are described in [1]. We classify by isomorphism type the extensions of $\mathbb{Z}_2$ by $G$, and use this information to show that certain elements of $H^2(G, \mathbb{Z}_2)$ cannot contain orthogonal cocycles.

Set $N = \langle a^2 \rangle$. Then $\inf: H^2(G/N, \mathbb{Z}_2) \to H^2(G, \mathbb{Z}_2)$ is an isomorphism. Moreover, if $\psi \in Z^2(G/N, \mathbb{Z}_2)$ then $E_{\inf, \psi} \equiv E_\psi \times \mathbb{Z}_2$. Hence $E_{\inf, \psi} \equiv E_{\inf, \psi}$ if and only if $E_\psi \equiv E_\psi$, and the isomorphism classes of extensions of $\mathbb{Z}_2$ by $G$ are in one-to-one correspondence with the isomorphism classes of extensions of $Z_2$ by $\mathbb{Z}_2^{(1)}$. The latter classes are essentially determined in Proposition 5.7, and the isomorphism types for each class are given in Table 1. Representing $\inf[\psi] \in H^2(G, \mathbb{Z}_2)$ by the same triple used to represent $[\psi] \in H^2(G/N, \mathbb{Z}_2)$, we list the isomorphism types of central extensions of $\mathbb{Z}_2$ by $G$ in Table 2.

**Proposition 5.9.** Let $t$ be odd. If $[\varphi] \in H^2(\mathbb{Z}_2^{(1)} \times \mathbb{Z}_2)$ represented by $(A, B, -1)$ contains an orthogonal cocycle, then $A = 1$ and $B = -1$.

**Proof.** This result follows from Proposition 5.7, Table 2, and Proposition 6 of [10].

Proposition 5.9 is verified directly in [8]. Note, however, that the transgression variable $K$ used here differs from that used in [8]; this amounts essentially to different choices of Schur complement in (5).

### 6. COCYCLIC HADAMARD MATRICES DEVELOPED OVER $D_t$

In this section we continue the analysis of development over $D_t$, begun in the previous section, carrying over the notation used there. The first result shows that we have already obtained a classification by isomorphism type of the extensions of $\mathbb{Z}_2$ by $D_t$.

**Theorem 6.1.** Let $[\psi], [\varphi] \in H^2(D_t, \mathbb{Z}_2)$. Then $E_\psi \equiv E_\varphi$ if and only if $[\psi]$ and $[\varphi]$ lie in the same orbit under the action of $\text{Aut}(D_t)$.

**Table 2**

<table>
<thead>
<tr>
<th>$(A, B, K)$</th>
<th>$E_{(A, B, K)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1, 1, 1)$</td>
<td>$\mathbb{Z}_2^{(1)} \times \mathbb{Z}_2$</td>
</tr>
<tr>
<td>$(1, -1, -1)$</td>
<td>$Q_8 \times \mathbb{Z}_2$</td>
</tr>
<tr>
<td>$(1, 1, -1)$</td>
<td>$D_4 \times \mathbb{Z}_2$</td>
</tr>
<tr>
<td>$(-1, 1, 1)$</td>
<td>$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2$</td>
</tr>
</tbody>
</table>
One possible approach involves determining presentations for $E_{\phi}$ as $\psi$ ranges over representatives $(A, B, K)$, one chosen from a single element in each of the $\text{Aut}(D_8)$-orbits listed in Proposition 5.7. However, presentations for Sylow 2-subgroups of such extensions have already been determined, and we prefer to use these and less explicit arguments.

By Lemma 4.2(i), if $E_{(A, B, K)} \cong E_{(A', B', K')}$, then $K = K'$. Suppose that $K = K' = 1$. Choose the presentation $F/R$ of $D_8$ and Schur complement $S/[R, F]$ as in the discussion following (7). If $\phi \in \text{Hom}(R/S, \mathbb{Z}_2)$ is nontrivial then $\phi(\langle a', b \rangle) \neq 1$ and so $\zeta(E_{(A, B, -1)}) = \langle (1, -1) \rangle$ by Lemma 4.1. This means that any isomorphism between $E_{(A, B, -1)}$ and $E_{(A', B', -1)}$ leaves $\langle (1, -1) \rangle$ invariant and so arises from $\text{Aut}(D_8)$-action on $H^2(D_8, \mathbb{Z}_2)$. Consequently, we restrict attention henceforth to the case $K = K' = 1$.

Suppose that $t$ is odd. From Table 1, we cannot have $E_{(1, 1, 1)} \cong E_{(1, -1, 1)}$, since the two extensions have nonisomorphic Sylow 2-subgroups; similarly, $E_{(1, 1, 1)} \not\cong E_{(-1, 1, 1)}$. By (6) and (8), $\zeta(E_{(1, 1, 1)}) = \langle (a', 1) \rangle \cong \mathbb{Z}_4$, whereas $\zeta(E_{(-1, 1, 1)}) = \langle (a', 1), (1, -1) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so that $E_{(-1, 1, 1)} \not\cong E_{(1, -1, 1)}$.

Now suppose that $t$ is even. We cannot have $E_{(-1, 1, 1)} \cong E_{(1, -1, 1)}$, since these two extensions have nonisomorphic Sylow 2-subgroups. For in the first extension, a Sylow 2-subgroup has derived quotient $\mathbb{Z}_2 \times \mathbb{Z}_4$, but in the second that quotient is $\mathbb{Z}_2^{(3)}$, as we may see from the presentations given after Table 1. Finally, $E_{(1, 1, 1)} \cong E_{(-1, 1, 1)}$ and $E_{(1, 1, 1)} \not\cong E_{(-1, -1, 1)}$ by Lemma 4.2(ii): (1, 1, 1) is inflated from a cocycle giving rise to an extension with isomorphism type $\mathbb{Z}_2^{(3)}$, whereas both $(-1, 1, 1)$ and $(1, 1, 1)$ are inflated from cocycles giving rise to extensions with isomorphism type $\mathbb{Z}_2 \times \mathbb{Z}_4$.

We have shown that $E_{\phi} \cong E_{\psi}$, only if $[\phi]$ and $[\psi]$ lie in the same orbit under the action of $\text{Aut}(D_8)$, for any $[\phi], [\psi] \in H^2(D_8, \mathbb{Z}_2)$. This proves the theorem.

Recall the procedure discussed in Section 4 for classifying Hadamard groups with quotient $D_8$ modulo distinguished central $\mathbb{Z}_2$. After Propositions 5.7 and 5.8, the next step in such a classification is to search for orthogonal cocycles in the classes represented by $(A, B, K) = (1, 1, 1), (1, -1, 1), (1, -1, 1), (-1, 1, 1),$ and $(-1, -1, 1)$ (this last class applicable only for even $t$). A full classification entails testing all cocycles in each of the stated classes until an orthogonal one is found. For a given value of $t$, the corresponding Hadamard groups of this kind are classified according to isomorphism, by Theorem 6.1.

We will not attempt a full classification here. Instead, we search for orthogonal cocycles in classes for which the associated cocyclic matrices have a comparatively simple block structure.
Now the Hadamard groups of order 8 have been classified (see [10, Example 2], for instance). Of course, such a group is a central extension of $\mathbb{Z}_2$ by $\mathbb{Z}_4$, or of $\mathbb{Z}_2$ by $\mathbb{Z}_2^{(2)}$. By Corollary 5.3, the only elements of $\mathbb{Z}^2(\mathbb{Z}_4, \mathbb{Z}_2)$ which are possibly orthogonal are coboundaries. Indeed, precisely two of the four elements of $B^2(\mathbb{Z}_4, \mathbb{Z}_2)$ are orthogonal, and both give rise to extensions $\mathbb{Z}_2 \times \mathbb{Z}_4$. Classes in $H^2(\mathbb{Z}_2^{(2)}, \mathbb{Z}_2)$ have size 2. In the notation of Table 2, there is a single orthogonal cocycle in the classes represented by $(1, 1, 1)$ and $(-1, 1, 1)$, as remarked after Proposition 5.8. Both cocycles in the class represented by $(1, -1, -1)$ are orthogonal.

We assume that $t > 1$ in the sequel.

First, a general form for a cocyclic matrix associated with an element of $B^2(D_4, \mathbb{Z}_2)$ will be found. Such a matrix is Hadamard equivalent to one which is group developed, the latter being derived from the multiplication table for $D_4$, by assigning each element of $D_4$ value 1 or $-1$ and then replacing each entry in the table accordingly. If we index rows and columns according to the ordering

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

of elements of $D_4$, then a group developed matrix over $D_4$ has block form

$$\begin{pmatrix}
M & N \\
NC_{2t} & MC_{2t}
\end{pmatrix},$$

where $M$ and $N$ are $2t \times 2t$ back circulant matrices and $C_{2t}$ is the back circulant $2t \times 2t$ permutation matrix with first row

$$1 \ 0 \ 0 \ 0 \ \cdots \ 0.$$

That is, postmultiplication of an $n \times n$ matrix by $C_n$ fixes its first column and reverses the order of its columns 2 through $2t$.

A back circulant matrix is symmetric (hence $C_n$ is self-inverse, since permutation matrices are orthogonal); however, a forward circulant matrix is not necessarily symmetric.

**Lemma 6.2.** (i) Forward circulant matrices commute.

(ii) The product of two forward circulant matrices is forward circulant, and the product of two back circulant matrices is forward circulant.

**Proof.** (i) This is well known. See [20, pp. 153–154]: an $n \times n$ forward circulant matrix is a polynomial in $C_n$, the matrix of multiplicative order $n$ obtained by reversing the order of the columns of $C_n$. Therefore two matrices of this type commute.
(ii) The product of two polynomials in $C_n$ is also a polynomial in $C_n$, hence forward circulant. Premultiplication or postmultiplication of an $n \times n$ back circulant matrix by $C_n$ produces a forward circulant matrix. Thus, if $X$ and $Y$ are back circulant then $XY = XC_nC_nY$ is forward circulant.

**Corollary 6.3.** For $M$ and $N$ as in (9), $MC_{2t}N = NC_{2t}M$.

**Proof.** Both $MC_{2t}$ and $NC_{2t}$ are forward circulant by Lemma 6.2(ii). Hence they commute by (i) of the lemma, and this implies the result.

**Lemma 6.4.** Let $X_n$ be the $n \times n$ matrix obtained by writing the rows of the $n \times n$ back negacyclic matrix in reverse order. An $n \times n$ matrix which is the entrywise product of a forward circulant matrix and $X_n$ commutes with any other matrix of this form.

**Proof.** Compare the proof of Lemma 6.2(i): a matrix of the stated form is a polynomial in the matrix obtained by negating the last column of $C_n$.

**Proposition 6.5.** (i) There is a cocyclic Hadamard matrix developed over $D_{4t}$, associated with a cocycle in the class represented by $(A, B, K) = (1, 1, 1)$ if and only if there are $2t \times 2t$ back circulant matrices $M$ and $N$ such that

$$M^2 + N^2 = 4tI_{2t} \quad \text{and} \quad MC_{2t}N = 0_{2t}.$$  

Existence in this case implies existence in the case $(A, B, K) = (1, -1, 1)$, for which only the first of the stated conditions is necessary and sufficient.

(ii) There is a cocyclic Hadamard matrix developed over $D_{4t}$, associated with a cocycle in the class represented by $(A, B, K) = (1, -1, -1)$ if and only if there are $2t \times 2t$ matrices $M$ and $N$, each of which is the entrywise product of a back circulant and back negacyclic matrix, such that

$$M^2 + N^2 = 4tI_{2t}.$$  

**Proof.** (i) A matrix associated with a cocycle in the class represented by $(A, B, K) = (1, 1, 1)$ is Hadamard equivalent to a matrix of the form (9) (we use the same indexing of rows and columns as that laid down before (9)). Since $M$, $N$, and $C_{2t}$ are symmetric, this matrix is Hadamard if and only if $M^2 + N^2 = 4tI_{2t}$ and $MC_{2t}N + MC_{2t}M = 0_{2t}$. By Corollary 6.3, this gives the first assertion in (i).
A matrix associated with a cocycle in the class represented by \((A, B, K) = (1, -1, 1)\) is Hadamard equivalent to a matrix of the form
\[
\begin{pmatrix}
M & N \\
NC_{2t} & -MC_{2t}
\end{pmatrix},
\]
as we see from (8) and (9). Now the second assertion in (i) is evident by Corollary 6.3.

(ii) In this case, the matrices of interest have the form
\[
\begin{pmatrix}
M & N \\
ND & -MD
\end{pmatrix},
\]
where \(M\) and \(N\) are each the entrywise product of a back circulant and back negacyclic matrix (hence are symmetric), and \(D\) is the \(2t \times 2t\) matrix obtained by negating every noninitial column of \(C_{2t}\). Then \(MD\) and \(ND\) are each the entrywise product of a forward circulant matrix and \(X_{2t}\), where \(X_{2t}\) is defined as in Lemma 6.4. Since \(MDND = NDMD\) by that lemma, the claim is proved.

In two cases, the restrictions on the block structure of cocyclic Hadamard matrices over \(D_4, t\) odd, imply the existence of a weighing matrix. This in turn restricts \(t\), as shown in the next result.

**Proposition 6.6.** Let \(t\) be odd. If there is a cocyclic Hadamard matrix developed over \(D_4\) associated with a cocycle in the class represented by \((A, B, K) = (1, 1, 1)\) or in the class represented by \((A, B, K) = (-1, 1, 1)\), then \(t\) is the sum of two squares.

**Proof.** Suppose first that there are \(2t \times 2t\) back circulant matrices \(M\) and \(N\) satisfying the conditions of Proposition 6.5(i). Then \(\frac{1}{2}(M + NC_{2t})\) is a weighing matrix of weight \(t\) and order \(2t\) (see [6, Definition 2.1, p. 7]). One claim then follows from [6, Corollary 2.11(b), p. 13]. The proof of the other claim is the same, after replacing \(M\) by the entrywise product of \(M\) and the \(2t \times 2t\) matrix
\[
\begin{pmatrix}
1 & 1 & 1 & 1 & \cdots & 1 \\
1 & -1 & 1 & -1 & \cdots & -1 \\
1 & 1 & 1 & 1 & \cdots & 1 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & -1 & 1 & -1 & \cdots & -1
\end{pmatrix},
\]
and replacing \(N\) similarly. \(\square\)
By Proposition 5.7, 5.8, and 6.5, an existence search for cocyclic Hadamard matrices over \( D_4 \) may be restricted to the cases \((A, B, K) = (1, -1, 1), (1, -1, -1), (-1, 1, 1), \) and \((-1, 1, -1)\), excluding the last case when \( t \) is odd. The matrices for \((A, B, K) = (1, -1, 1)\) and \((1, -1, -1)\) possess the most tractable block structure, and we deal with these cases only from now on.

The search space for matrices \( M \) and \( N \) as in Proposition 6.5 increases exponentially in size with \( t \). However, some further simple matrix algebra may be used to reduce the number of tests which need to be applied to a pair of candidates chosen from the search space. We devote the rest of this section to recasting the search problems in this way.

First suppose that \((A, B, K) = (1, -1, 1)\). By Proposition 6.5(i), we seek for \( t \geq 1 \) two back circulant matrices \( M \) and \( N \) such that \( M^2 + N^2 = 4I_{2t} \).

Write the first row of \( M \) as \( \bar{m} \). Then the \( i \)th row of \( M \) is \( \bar{m}P^i \), where \( P \) is the \( 2t \times 2t \) permutation matrix which upon postmultiplication of a compatible matrix cycles its columns once to the left. That is, \( P \) is forward circulant, with first row

\[
\begin{bmatrix}
0 & 0 & \cdots & 0 & 1
\end{bmatrix}.
\]

For \( 2 \leq i \leq t \), the \((t - i + 2)\)th entry in the first row of \( M^2 \) is

\[
\bar{m}(\bar{m}P^{t-i+1})^T = \bar{m}\bar{m}^T \bar{m}P^{t-i-1}m^T = (\bar{m}\bar{m}^T)^T \bar{m}P^{t-i-1}m^T = \bar{m}P^{t-i-1}P^{-2i}\bar{m}^T = \bar{m}P^{1-i}m^T = \bar{m}(\bar{m}P^{1-i})^T,
\]

which is the \((t + i)\)th entry in the first row of \( M^2 \). This shows that each of the forward circulant matrices \( M^2 \) and \( N^2 \) is completely determined by the first \( t + 1 \) entries in its first row. Our requirement has therefore been modified to:

For each \( t \leq 2 \), find a pair of \( 2t \)-tuples \( \bar{m} \) and \( \bar{n} \) with entries \( \pm 1 \) such that \( \bar{m}(\bar{m}P^i)^T = -\bar{n}(\bar{n}P^i)^T \) for \( 1 \leq i \leq t \).

A procedure written in the algebraic computer system MAGMA has been used to search for such pairs of \( 2t \)-tuples. The procedure breaks as soon as a suitable pair is found; otherwise a message is printed that no cocyclic Hadamard matrices of this kind exist. Results for \( 2 \leq t \leq 8 \) are given in Table 3.
TABLE 3
Examples of Cocyclic Hadamard Matrices over $D_{4t}$ with $(A, B, K) = (1, -1, 1)$

<table>
<thead>
<tr>
<th>$t$</th>
<th>First row of $M$</th>
<th>First row of $N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$(1, 1, 1, -1)$</td>
<td>$(1, 1, 1, -1)$</td>
</tr>
<tr>
<td>4</td>
<td>$(1, 1, 1, -1, -1, -1, -1, -1)$</td>
<td>$(1, 1, 1, -1, 1, -1, 1, -1)$</td>
</tr>
<tr>
<td>5</td>
<td>$(1, 1, 1, -1, -1, -1, -1, 1)$</td>
<td>$(1, 1, 1, -1, 1, -1, -1, 1)$</td>
</tr>
<tr>
<td>8</td>
<td>$(1, 1, 1, -1, -1, -1, -1, 1)$</td>
<td>$-1, -1, 1, -1, -1, -1, -1, -1)$</td>
</tr>
</tbody>
</table>

In the search, the values $t = 3, 6$ and 7 were ignored by virtue of the next result (cf. Proposition 6.6).

**Proposition 6.7.** If there is a cocyclic Hadamard matrix developed over $D_{4t}$ associated with a cocycle in the class represented by $(A, B, K) = (1, -1, 1)$, then $t$ is the sum of two squares.

**Proof.** Suppose $M$ and $N$ are back circulant $2t \times 2t$ matrices such that $M^2 + N^2 = 4tI_{2t}$. Denote the $j$th rows of $M$ and $N$ by $\bar{m}_j$ and $\bar{n}_j$, and denote the $j$th entry of each by $m_{i,j}$ and $n_{i,j}$, respectively. The condition $M^2 + N^2 = 4tI_{2t}$ is equivalent to the conditions $\bar{m}_j \bar{m}_j^T + \bar{n}_j \bar{n}_j^T = 4t$ and $\bar{m}_j \bar{m}_j^T + \bar{n}_j \bar{n}_j^T = 0$ for $2 \leq i \leq 2t$. Thus

$$4t = \sum_{i=1}^{2t} \bar{m}_i \bar{m}_i^T + \sum_{i=1}^{2t} \bar{n}_i \bar{n}_i^T$$

$$= \bar{m}_1^T \left( \sum_{i=1}^{2t} \bar{m}_i \right) + \bar{n}_1^T \left( \sum_{i=1}^{2t} \bar{n}_i \right)$$

$$= \left( \sum_{i=1}^{2t} m_{1,i} \right) \bar{m}_1 (1, 1, \ldots, 1)^T + \left( \sum_{i=1}^{2t} n_{1,i} \right) \bar{n}_1 (1, 1, \ldots, 1)^T$$

$$= \left( \sum_{i=1}^{2t} m_{1,i} \right)^2 + \left( \sum_{i=1}^{2t} n_{1,i} \right)^2.$$

Hence $4t$ is the sum of two even squares, so that $t$ is the sum of two squares.

The analysis in the case $(A, B, K) = (1, -1, -1)$ is slightly more complicated. From now on, $M$ and $N$ are $2t \times 2t$ matrices of the type specified in Proposition 6.5(ii). For $1 \leq i \leq 2t$, let $W_i$ be the $2t \times 2t$
diagonal matrix whose main diagonal is

\[
\begin{pmatrix}
1 & 1 & \cdots & 1 & -1 & \cdots & -1
\end{pmatrix},
\]

where the last entry 1 occurs in position \(2t-i\). If the first row of \(M\) is \(\vec{m}_1\), then, for \(i \geq 2\), the \(i\)th row \(\vec{m}_i\) of \(M\) is \(\vec{m}_1 P^{i-1} W_{t-1}\). Note that premultiplication by the permutation matrix \(P\) defined earlier cycles rows of a compatible matrix downward once; thus, if \(X\) is a diagonal matrix then \(PX^T\) is the diagonal matrix obtained from \(X\) by cycling the entries on the main diagonal forward once. In particular, \(PW_i P^T = -W_{2t-1} W_{t-1}\), and hence

\[
PW_i = -W_{2t-1} W_{t-1} P. \tag{10}
\]

**Lemma 6.8.** \(W_i P^j = P^j W_i W_{i+j}\).

**Proof.** By (10), \(PW_{i+1} = -W_{2t-1} W_i P\), so that

\[
W_i P = -W_{2t-1} P W_{i+1} = PW_1 W_{i+1},
\]

and the assertion is true for \(j = 1\). Assume the assertion is true for some \(j \geq 1\); then

\[
W_i P^{j+1} = P^j W_i W_{i+j} P = P^j W_i PW_{i+j+1} = P^j PW_{i+j+1} W_{i-j+1} = P^{j+1} W_{i+j+1} W_{i-j+1},
\]

and the assertion is proved by induction.

**Proposition 6.9.** In the notation above,

(i) \(\vec{m}_i \vec{m}_{i+1}^T = -\vec{m}_i \vec{m}_{i+1+2}^T, \ 2 \leq i \leq t\);
(ii) \(\vec{m}_i \vec{m}_j^T = \vec{m}_{i+1} \vec{m}_{j+1}^T, \ 2 \leq i, j \leq t\).

**Proof.** We have

\[
\vec{m}_i \vec{m}_{i+1}^T = \vec{m}_1 \left( P^{i+1} W_{i+1+1} \right)^T = \vec{m}_1 W_{i+1+1} P^{i+1} \vec{m}_1^T = \vec{m}_1 P^{i+1} W_{i+1+1} W_{i+1+1} \vec{m}_1^T = -\vec{m}_1 P^{i+1} W_{i+1+1} W_{i+1+1} \vec{m}_1^T.
\]
where in moving from the second to the third line we employed Lemma 6.8. This proves (i). The proof of (ii) proceeds similarly.

In view of Proposition 6.9(ii), $M^2 + N^2 = 4tI_2$, if and only if $\tilde{m}_i\tilde{m}_i^T = -\tilde{n}_i\tilde{n}_i^T$ for all $i$, $2 \leq i \leq t$. Then by Proposition 6.9(i)—note in particular that $\tilde{m}_1\tilde{m}_1^T, 1 = 0$—our requirement may be modified to:

For each $t \geq 2$, find a pair of $2t$-tuples $\tilde{m}$ and $\tilde{n}$ with entries $\pm 1$ such that $\tilde{m}(\tilde{m}^TP^W)^T = -\tilde{n}(\tilde{n}^P)^T$ for $1 \leq i \leq t - 1$.

A computer search for such pairs may be carried out by using a slightly amended version of the MAGMA procedure mentioned above. Since $(M, N)$ is a pair of matrices of the required type satisfying $M^2 + N^2 = 4tI_2$, if and only if $(\pm M, \pm N)$ is also, the search space for $\tilde{m}$ and $\tilde{n}$ may be reduced from size $2^{2t}$ to $2^{2t-1}$ ($2t$-tuples with first entry 1).

Table 4 provides examples of cocyclic Hadamard matrices in this case. For each value of $t$, the full matrix $M$ or $N$ is obtained by writing down the back circulant matrix specified by the stated first row, and then forming the entrywise product of this with the $2t \times 2t$ back negacyclic matrix.

<table>
<thead>
<tr>
<th>$t$</th>
<th>First rows of $M$ and $N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(1, 1, 1, -1)</td>
</tr>
<tr>
<td></td>
<td>(1, -1, 1, -1)</td>
</tr>
<tr>
<td>3</td>
<td>(1, 1, -1, 1, 1)</td>
</tr>
<tr>
<td></td>
<td>(1, -1, -1, 1, 1)</td>
</tr>
<tr>
<td>4</td>
<td>(1, -1, -1, -1, 1, -1)</td>
</tr>
<tr>
<td></td>
<td>(1, -1, -1, -1, -1, 1)</td>
</tr>
<tr>
<td>5</td>
<td>(1, 1, 1, -1, 1, 1, -1, 1)</td>
</tr>
<tr>
<td></td>
<td>(1, 1, -1, 1, 1, -1, 1, -1)</td>
</tr>
<tr>
<td>6</td>
<td>(1, 1, -1, 1, 1, -1, 1, 1, -1)</td>
</tr>
<tr>
<td></td>
<td>(1, 1, 1, -1, 1, 1, 1, -1, 1, 1)</td>
</tr>
<tr>
<td>7</td>
<td>(1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1)</td>
</tr>
<tr>
<td></td>
<td>(1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1)</td>
</tr>
<tr>
<td>8</td>
<td>(1, 1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, -1)</td>
</tr>
<tr>
<td></td>
<td>(1, 1, -1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1, -1)</td>
</tr>
<tr>
<td>9</td>
<td>(1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1)</td>
</tr>
<tr>
<td></td>
<td>(1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1)</td>
</tr>
<tr>
<td>10</td>
<td>(1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1)</td>
</tr>
<tr>
<td></td>
<td>(1, -1, -1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1)</td>
</tr>
<tr>
<td>11</td>
<td>(1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, 1, -1, 1, -1)</td>
</tr>
<tr>
<td></td>
<td>(1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, 1, -1)</td>
</tr>
</tbody>
</table>
The computational evidence suggests that there is a greater density of cocyclic Hadamard matrices developed over $D_4$, in this case than in the previously considered case (this is not surprising, given that in the present case there are fewer linear constraints on rows in the blocks of such matrices). By the usual reasoning, one may verify that the cocycle $(A, B, K) = (1, -1, -1)$ gives rise to the central extension $G(t)$ of $\mathbb{Z}_2$ by $D_4$, with presentation

$$\langle x, y \mid x^{4t} = 1, y^2 = x^{2t}, x^y = x^{-1} \rangle.$$

In [12], Ito calls $G(t)$ a group of type $Q$ (in this paper, $G(t) = Q_{8t}$ is called dicyclic) and conjectures that, for all $t \geq 1$, $G(t)$ is a Hadamard group. In this section we have verified the conjecture for $1 \leq t \leq 11$.

Finally, it is interesting to note that a dicyclic but never a dihedral group can be a Hadamard group; whereas a dihedral but never a dicyclic group (with order 4 Sylow $\mathbb{Z}$-subgroup) can arise as the quotient modulo distinguished $\mathbb{Z}$ of a Hadamard group.

ACKNOWLEDGMENTS

The work in this paper was mostly undertaken while I was a Research Associate on the project “Cocyclic Hadamard matrix codes” funded by Australian Research Council Grant A69230619. I thank the ARC for their financial support. I also thank Professor K. J. Horadam for her guidance throughout my time on the project and for giving me the opportunity to work in this area.

I am indebted to Dr. E. A. O’Brien, who assisted enormously in the writing of computer programs which were used to determine the cocyclic Hadamard matrices catalogued in Sect. 6, and to both Dr. O’Brien and Dr. L. G. Kovács, who showed me Example 2.3.

REFERENCES