Equivalences of $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices

V. Alvarez, F. Gudiel, M. B. Guemes, K. J. Horadam, A. Rao

August 20, 2018

Abstract

One of the most promising structural approaches to resolving the Hadamard Conjecture uses the family of cocyclic matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Two types of equivalence relations for classifying cocyclic matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$ have been found. Any cocyclic matrix equivalent by either of these relations to a Hadamard matrix will also be Hadamard.

One type, based on algebraic relations between cocycles over any finite group, has been known for some time. Recently, and independently, a second type, based on four geometric relations between diagrammatic visualisations of cocyclic matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$, has been found. Here we translate the algebraic equivalences to diagrammatic equivalences and show one of the diagrammatic equivalences cannot be obtained this way. This additional equivalence is shown to be the geometric translation of matrix transposition.

Keywords: Hadamard matrix, cocyclic matrix, shift equivalence, bundle, Williamson-type matrix.

1 Introduction

A Hadamard matrix of order m is a square matrix $[h(i,j)]$ with entries $h(i,j) = \pm 1$, $1 \leq i,j \leq m$, whose row vectors are pairwise orthogonal. A Hadamard matrix must have order 1, 2 or a multiple of 4, but no other restrictions on the order of a Hadamard matrix are known, and the century-old Hadamard Conjecture proposes that a Hadamard matrix exists for every $m \equiv 0 \pmod 4$.

About 20 years ago, the use of cocycles and cocyclic matrices was introduced by Horadam and de Launey [11] as a structural approach to resolving the Hadamard Conjecture. Its advantages led to the cocyclic Hadamard conjecture: that a cocyclic Hadamard matrix exists for every $m \equiv 0 \pmod 4$. The study and use of cocyclic matrices has expanded substantially since then, to include generalised Hadamard matrices [9, 10] and pairwise combinatorial designs [5].

If G is a group and C is an abelian group, a (2-dimensional, normalized) cocycle ψ is a mapping $\psi : G \times G \to C$ satisfying $\psi(1,1) = \psi(g,1) = \psi(1,g) =$

1, $g \in G$ and the cocycle equation:

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

The set of cocycles from G to C forms an abelian group $Z^2(G,C)$ under pointwise multiplication. The simplest cocycles are the coboundaries ∂f, defined for any function $f : G \to C$ by $\partial f(g,h) = f(g)^{-1} f(h)^{-1} f(gh)$.

A cocycle may be represented by its matrix of values

$$M_\psi = [\psi(g,h)]_{g,h \in G} \tag{2}$$

once an indexing of the elements of G has been chosen.

We set $C = \{\pm 1\} \cong \mathbb{Z}_2$ when searching for cocyclic Hadamard matrices. A cocycle ψ for which the cocyclic matrix M_ψ is Hadamard is termed *orthogonal*. It is computationally easy to check whether M_ψ is a Hadamard matrix, as we only need to check whether the dot product of the first row with each other row is 0. This computational cutdown is one motivation for using cocyclic matrices.

Most of the known constructions of Hadamard matrix families are cocyclic [9, Ch. 6]. Computationally, the most prolific indexing groups G for producing cocyclic Hadamard matrices appear to be the abelian groups $\mathbb{Z}_t \times \mathbb{Z}_2^2$ and the dihedral groups D_{4t}, where we may assume t is odd. The D_{4t} family, related to the Ito type Hadamard matrices, has been investigated by many researchers including the authors (see [9]). The $\mathbb{Z}_t \times \mathbb{Z}_2^2$ family, related to the Williamson type Hadamard matrices, has also been investigated by the authors [3, 4], and while exhaustive search often finds fewer Hadamard matrices in each order than for D_{4t}, abelian-ness makes the family computationally more tractable.

In parallel with the search for examples of Hadamard matrices in new orders, whether cocyclic or not, has been the attempt to classify them into equivalence classes. Hadamard equivalence of a $\{\pm 1\}$ matrix involves only permutation of rows or columns, and multiplication of a row or column by -1. While the transpose of a Hadamard matrix is a Hadamard matrix, transposition is not a Hadamard equivalence. The total number of Hadamard equivalence classes in small orders grows so rapidly that Orrick [14] uses a coarser Q-equivalence relation on Hadamard matrices which allows extra "switching" operations and leads to a dramatic reduction in the number of classes.

The total number of equivalence classes of cocyclic Hadamard matrices over all index groups G is studied by Ó Catháin and Röder [13] and calculated up to $m = 36$. An allied but distinct approach has been to identify equivalences of cocycles that preserve orthogonality. For the $\mathbb{Z}_t \times \mathbb{Z}_2^2$ family, two different types of equivalence of cocycles, both of which preserve orthogonality, have been discovered independently.

The first of these is defined (see [9]) for any G and C by all compositions of a "shift" action and two "automorphism" actions. (If $C = \{\pm 1\}$ one of the automorphism actions is trivial.) The resulting equivalence classes, called *bundles*, are already known by other names in different contexts. For example, if f is a cryptographic function and $\psi = \partial f$ is a coboundary, the bundle corresponds to the Extended Affine (EA) equivalence class of f. Shift action is also studied

separately, for applications to the search for self-dual codes [15] and, via shift representations, to classification of pairwise combinatorial designs [6].

The second of these equivalences, independently introduced in [3], is specific to cocycles ψ in $Z^2 := Z^2(\mathbb{Z}_t \times \mathbb{Z}_2^2, \{\pm 1\})$ and arises from detailed investigation of a generating set of cocycles for Z^2. Corresponding to the decomposition of ψ as a product of generators there is a Hadamard product decomposition of M_ψ into generator matrices. Geometric actions on these generator matrices lead to a concise diagrammatic representation of cocycles and geometric equivalences which is very useful for effective computation.

This paper relates and reconciles the two types of equivalence.

The paper is organized as follows. Section 2 describes the two types of equivalence. The group acting on cocycles is determined for each type; the two groups are not isomorphic. Section 3 gives our main results, Theorems 3 and 4, translating shift action and the remaining automorphism action into diagram actions, relating the two groups of actions, and showing that the diagram action termed "complement" has no algebraic analogue. In Section 4 this diagram action is shown to be the transposing operation on M_ψ. We summarise and suggest further work.

2 Background

From now on we assume $C = \{\pm 1\}$, $G \cong \mathbb{Z}_t \times \mathbb{Z}_2^2$ with $t > 1$ odd, and $\psi \in Z^2$. Denote the group of units of the ring $\mathbb{Z}_t$ by $\mathbb{Z}_t^*$. Let G have presentation

$$G = \langle x, u, v : \ x^t = u^2 = v^2 = 1, xu = ux, xv = vx, uv = vu \rangle,$$

and ordering

$$(x^i, 1) < (x^i, u) < (x^i, v) < (x^i, uv),\ 0 \le i < t,\ (x^i, uv) < (x^{i+1}, 1),\ 0 \le i < t-1\,.$$

We describe an orthogonality-preserving algebraic action on ψ in the first subsection and an orthogonality-preserving geometric action on ψ in the second.

2.1 Bundle action on cocycles

For any $a \in G$, the *shift* $\psi \cdot a$ of ψ is the cocycle $(\psi \cdot a)(g, h) = \psi(ag, h)\psi(a, h)^{-1}$. It is orthogonal if ψ is orthogonal. For any automorphism $\theta \in \mathrm{Aut}(G)$, the cocycle $\psi \circ (\theta \times \theta)$ is orthogonal if ψ is. When the two actions are combined, the result is an action by the semidirect product $H = G \rtimes \mathrm{Aut}(G)$ called *bundle action* under which the orbit of ψ is its *bundle*

$$\mathcal{B}(\psi) = \{(\psi \cdot a) \circ (\theta \times \theta) : \ a \in G,\ \theta \in \mathrm{Aut}(G)\}. \tag{3}$$

The group H acting on Z^2 is $H = G \rtimes \mathrm{Aut}(G)$, where the semidirect product is defined for $a, b \in G,\ \theta_1, \theta_2 \in \mathrm{Aut}(G)$ by $a\theta_1 \circ b\theta_2 = a\theta_1^{-1}(b)\theta_1\theta_2$. See [9, Ch. 8] for details.

The Hadamard equivalence operations on M_ψ corresponding to shift and automorphism action can be easily described. $M_{\psi\cdot a}$ is Hadamard equivalent to M_ψ by first permuting the rows of M_ψ with respect to the row index permutation $g \mapsto g' = ag,\ g \in G$, obtaining $M' = [\psi(ag, h)]_{g,h\in G}$. The first row of M' is the a^{th} row of M_ψ. Then obtain $M_{\psi\cdot a}$ from M' by multiplying every row of M' point-wise by its first row, or, equivalently, by multiplying every column of M' by its first entry. $M_{\psi\circ(\theta\times\theta)}$ is Hadamard equivalent to M_ψ by permuting rows and columns under θ.

We complete this subsection by identifying the group $H = G \rtimes \mathrm{Aut}(G)$ which partitions cocycles into bundles (3).

Theorem 1 *The group H defined by bundle action on Z^2 is $H \cong [\mathbb{Z}_t \rtimes \mathbb{Z}_t^*] \times [\mathbb{Z}_2^2 \rtimes S_3]$. Therefore the order of H is $24\,t\,\phi(t)$, where ϕ is the Euler function.*

A generating set for H is $\{x, u, v, h_r, r \in \mathbb{Z}_t^*, h_{23}, h_{243}\}$, where x, u and v are shift actions and $h_{23} : x \mapsto x, u \mapsto v, v \mapsto u$; $h_{243} : x \mapsto x, u \mapsto uv, v \mapsto u$ and $h_r : x \mapsto x^r, u \mapsto u, v \mapsto v$ are automorphism actions.

Proof. Since t is odd, $\mathrm{Aut}(\mathbb{Z}_t \times \mathbb{Z}_2^2) \cong \mathrm{Aut}(\mathbb{Z}_t) \times \mathrm{Aut}(\mathbb{Z}_2^2) \cong \mathbb{Z}_t^* \times S_3$. Under the identification $1 \leftrightarrow 1, u \leftrightarrow 2, v \leftrightarrow 3, uv \leftrightarrow 4$, $\mathrm{Aut}(\mathbb{Z}_2^2)$ is the subgroup of S_4 which fixes 1. Then $\{\mathrm{Id}\} \times \mathrm{Aut}(\mathbb{Z}_2^2)$ is generated by h_{23} and h_{243}. Thus $H = [\mathbb{Z}_t \times \mathbb{Z}_2^2] \rtimes [\mathbb{Z}_t^* \times S_3]$, with the listed generating set. Since $h_{23}(x) = h_{243}(x) = x$, $\mathbb{Z}_t$ commutes with S_3 and since $h_r(u) = u$, $h_r(v) = v$, $\mathbb{Z}_2^2$ commutes with $\mathbb{Z}_t^*$. Hence $H \cong [\mathbb{Z}_t \rtimes \mathbb{Z}_t^*] \times [\mathbb{Z}_2^2 \rtimes S_3]$. □

Remark 1 *In terms of the Coxeter presentation of S_n, if σ_i denotes the transposition $(i\ \ i+1)$, $S_n = \langle \sigma_i : \ \sigma_i^2 = (\sigma_i\sigma_{i+1})^3 = 1, 1 \le i \le n-1\rangle$ and $S_4 = \langle \sigma_1, \sigma_2, \sigma_3 : \ \sigma_i^2 = (\sigma_i\sigma_{i+1})^3 = 1, 1 \le i \le 3\rangle > \langle \sigma_2, \sigma_3\rangle \cong S_3$, so that in Theorem 1, $h_{23} = \sigma_2$ and $h_{243} = \sigma_3\sigma_2$.*

2.2 Geometric action on cocycle diagrams

The group of cocycles Z^2 has a generating set $\mathcal{Z} = \{\partial_1, \ldots, \partial_{4t}, \beta_1, \beta_2, \kappa\}$ consisting of $4t$ coboundaries $\partial_i := \partial\delta_i$, where δ_i is the Kronecker delta function of the i^{th}-element in G in the given ordering, and three representative cocycles β_1, β_2, κ, all of which are explicitly described in [1, 3]. Every 2-cocycle over G admits a (non unique) representation as a product of the generators in $\mathcal{Z}$. The identity of Z^2 is the trivial cocycle $\mathbf{1}$ for which $M_{\mathbf{1}} = J_{4t}$ is the all-ones matrix. All orthogonal cocycles known so far (cf. [4, 3]) contain the factor $\rho = \beta_1\beta_2\kappa$, where

$$M_\rho = J_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}, \tag{4}$$

and J_t denotes the $t \times t$ matrix all of 1s. It is conjectured this must always be true [9, Research Problem 37]. For the remainder of the paper, we assume that we work with cocycles of this type. That is, $\psi = {\partial_1}^{\epsilon_1} \ldots {\partial_{4t}}^{\epsilon_{4t}} \rho$, $\epsilon_i \in \{0, 1\}$.

In [3], a more concise notation to describe $\psi = \partial_{d_1} \dots \partial_{d_k} \rho$ is introduced, which allows one to determine if ψ is orthogonal much more easily. Partition the set $\{d_1, \dots, d_k\}$ according to the equivalence classes modulo 4, in the class order $2, 3, 0, 1$ and in descending order within each class. We will denote this ordered set of coboundaries

$$\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\} = \{\{d_{2+4j_2}\}, \{d_{3+4j_3}\}, \{d_{4j_4}\}, \{d_{1+4j_1}\}\}. \tag{5}$$

For example, for $t = 7$, the cocycle $\psi = \partial_4\partial_6\partial_9\partial_{10}\partial_{11}\partial_{12}\partial_{14}\partial_{20}\partial_{21}\partial_{25}\,\rho$ is orthogonal, and is represented as

$$\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\} = \{\{14, 10, 6\}, \{11\}, \{20, 12, 4\}, \{25, 21, 9\}\}. \tag{6}$$

Alternatively, we can write all the integers $1, \dots, 4t$, by equivalence classes modulo 4, in descending order, as the rows of a $4 \times t$ matrix (treated as a cylinder, i.e. left and right edges are identified) and mark out only the entries occurring in $\{d_1, \dots, d_k\}$.

Definition 1 *[3] The* diagram *of $\psi = \partial_{d_1} \dots \partial_{d_k} \rho$ is a $4 \times t$ matrix A, such that $a_{ij} = \times$ if $4t - 4(j-1) - 3 + i \mod 4t \in \{d_1, \dots, d_k\}$ and $a_{ij} = -$ elsewhere.*

The diagram for the example in (6) above is

$$A = \begin{vmatrix} - & - & - & \times & \times & \times & - \\ - & - & - & - & \times & - & - \\ - & - & \times & - & \times & - & \times \\ \times & \times & - & - & \times & - & - \end{vmatrix} \tag{7}$$

We now list the four types of orthogonality-preserving operations on ψ described in [3]. We adopt the notation $[m]_n$ for $m \mod n$ for brevity.

Definition 2 *Let $\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\}$ be a set of coboundaries. Denote the columns of its diagram A by $(\mathcal{C}_{t-1}, \cdots, \mathcal{C}_0)$. Let $\mathbf{c_j} + \mathbf{k}$ denote the set of coboundaries obtained by adding k to each element of $\mathbf{c_j}$ modulo $4t$.*

1. *The* complement $\mathrm{C}_2(\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\})$ *of this set is the set $\{\overline{\mathbf{c_2}}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\}$ where $\overline{\mathbf{c_2}}$ is complement of $\mathbf{c_2}$ in the equivalence class 2 modulo 4.*

2. *Six elementary* swapping *operations are possible on this set: s_{12}, s_{13}, s_{14} (see [3]) and*

   - $s_{23}(\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\}) = \{\mathbf{c_3 - 1}, \mathbf{c_2 + 1}, \mathbf{c_4}, \mathbf{c_1}\}$.
   - $s_{24}(\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\}) = \{\mathbf{c_4 - 2}, \mathbf{c_3}, \mathbf{c_2 + 2}, \mathbf{c_1}\}$.
   - $s_{34}(\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\}) = \{\mathbf{c_2}, \mathbf{c_4 - 1}, \mathbf{c_3 + 1}, \mathbf{c_1}\}$.

3. *The i-*rotation $\mathrm{T}_i(\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\})$, $0 \le i \le t-1$, *of this set is the set*

$$\{\mathbf{c_2 - 4i}, \mathbf{c_3 - 4i}, \mathbf{c_4 - 4i}, \mathbf{c_1 - 4i}\}.$$

4. *The* r-th dilatation $\mathrm{V}_r(\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\})$, *for* $r \in \mathbb{Z}_t^*$, *is the set with diagram* $\mathrm{V}_r(A)$, *where* $\mathrm{V}_r(\mathcal{C}_j) = \mathcal{C}_{[jr]_t},\ 0 \le j \le t-1$.

Clearly the order of C_2 is 2 and $\langle \mathrm{C}_2 \rangle \cong \mathbb{Z}_2$. The swappings each have order 2 and generate a group $\cong S_4$ which, in terms of a Coxeter presentation (Remark 1), is generated by $\sigma_1 = s_{23},\ \sigma_2 = s_{34}$ and $\sigma_3 = s_{14}$. The rotations are generated by T_1 so $\langle \mathrm{T}_1 \rangle \cong \mathbb{Z}_t$; and $\langle \mathrm{V}_r, r \in \mathbb{Z}_t^* \rangle \cong \mathbb{Z}_t^*$.

In terms of diagrams, C_2 complements the first row of A; s_{ij} swaps rows corresponding to $\mathbf{c_i}$ and $\mathbf{c_j}$; T_i cyclically shifts columns i places to the right; and V_r permutes columns according to multiplication of column index by the invertible element r (so $\mathcal{C}_0$ is always fixed).

For instance, if A is the diagram in (7),

$$\mathrm{C}_2(A) = \left|\begin{array}{ccccccc} \times & \times & \times & - & - & - & \times \\ - & - & - & - & \times & - & - \\ - & - & \times & - & \times & - & \times \\ \times & \times & - & - & \times & - & - \end{array}\right|, \quad \mathrm{T}_2(A) = \left|\begin{array}{ccccccc} \times & - & - & - & - & \times & \times \\ - & - & - & - & - & - & \times \\ - & \times & - & - & \times & - & \times \\ - & - & \times & \times & - & - & \times \end{array}\right|,$$

$$s_{23}(A) = \left|\begin{array}{ccccccc} - & - & - & - & \times & - & - \\ - & - & - & \times & \times & \times & - \\ - & - & \times & - & \times & - & \times \\ \times & \times & - & - & \times & - & - \end{array}\right|, \quad \mathrm{V}_2(A) = \left|\begin{array}{ccccccc} \times & - & \times & - & \times & - & - \\ - & - & \times & - & - & - & - \\ - & - & \times & - & - & \times & \times \\ - & \times & \times & \times & - & - & - \end{array}\right|.$$

It is possible to identify the action of C_2 on coboundaries directly.

Lemma 1 $\mathrm{C}_2(\partial_{d_1} \dots \partial_{d_k}) = \partial_{d_1} \dots \partial_{d_k} \prod_{i=0}^{t-1} \partial_{2+4i}$.

Proof. If $\psi = \mathbf{1}$ is the trivial coboundary in Z^2, with $M_{\mathbf{1}} = J_{4t}$ the all-ones matrix, then it has $\{\mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_1}\} = \{\emptyset, \emptyset, \emptyset, \emptyset\}$ so $\mathrm{C}_2(\mathbf{1}) = \prod_{i=0}^{t-1} \partial_{2+4i}$. By simple inspection, it may be checked that

$$\mathrm{C}_2(J_{4t}) = \prod_{i=0}^{t-1} M_{\partial_{2+4i}} = J_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{8}$$

The result follows immediately. □

We complete this subsection by identifying the group H' generated by the diagrammatic operations above.

Theorem 2 *The group* H' *defined by diagrammatic action on* Z^2 *is* $H' \cong [\mathbb{Z}_t \rtimes \mathbb{Z}_t^*] \times S_4 \times \mathbb{Z}_2$. *Therefore the order of* H' *is* $48\, t\, \phi(t)$. *A generating set for* H' *is* $\{\mathrm{T}_1, \mathrm{V}_r, r \in \mathbb{Z}_t^*,\ s_{14}, s_{23}, s_{34}, \mathrm{C}_2\}$.

Proof. It is shown in [3] that the complement and swapping operations commute with each other and with rotations and dilatations, but that rotation and dilatation do not commute. The composition $\mathrm{V}_r^{-1}\mathrm{T}_1\mathrm{V}_r$ acts on column $[j]_t$

of A to give column $[(jr-1)r^{-1}]_t = [j-r^{-1}]_t$, so $\mathrm{V}_r^{-1}\mathrm{T}_1\mathrm{V}_r = \mathrm{T}_{r^{-1}}$. Define a homomorphism $\mu : \mathbb{Z}_t^* \to \mathrm{Aut}(\mathbb{Z}_t)$ by $\mu(\mathrm{V}_r)(\mathrm{T}_1) = \mathrm{T}_{r^{-1}}$. Consequently, $\langle \mathrm{T}_1, \mathrm{V}_r, r \in \mathbb{Z}_t^* \rangle \cong \mathbb{Z}_t \rtimes_\mu Z_t^*$.

Swapping permutes rows while rotations and dilatations permute columns, so swapping is not in the subgroup of H' generated by rotations and dilatations. All combinations of swapping, rotation and dilatation preserve the total number of coboundaries but complementation does not, so complementation is not in the subgroup of H' generated by rotations, swappings and dilatations. □

3 Bundle actions as Diagram actions

In this section we express the bundle actions on Z^2 in terms of the diagrammatic operations and identify the role of the diagrammatic action C_2. Subsection 3.1 is given to proving the following theorem.

Theorem 3 *1. The shift actions by x, u and v, respectively, on ψ, are the diagrammatic actions T_1, $s_{12}s_{34}$ and $s_{13}s_{24}$, respectively.*

2. The automorphism actions by h_r, h_{23} and h_{243}, respectively, on ψ, are the diagrammatic actions $\mathrm{V}_{r^{-1}}$, $\mathrm{C}_2 s_{23}$ and $s_{234} := s_{23}s_{24}$, respectively.

From Theorem 3 we obtain our main result.

Theorem 4 *Bundle action by H on $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic matrices corresponds to diagrammatic action by the subgroup*

$$H^* = \langle \mathrm{T}_1,\ \mathrm{V}_{r^{-1}},\ s_{12}s_{34},\ s_{13}s_{24},\ \mathrm{C}_2 s_{23},\ s_{23}s_{24} \rangle \cong (\mathbb{Z}_t \rtimes \mathbb{Z}_t^*) \times S_4$$

of index 2 in H'. The operation C_2 is not in H^*.

Proof. Define a homomorphism $\alpha : H \rightarrowtail H'$ by $x \mapsto \mathrm{T}_1, h_r \mapsto \mathrm{V}_{r^{-1}}, u \mapsto s_{12}s_{34}, v \mapsto s_{13}s_{24}, h_u \mapsto \mathrm{C}_2 s_{23}$ and $h_v \mapsto s_{23}s_{24}$. By Theorem 2 and Theorem 3, $\alpha(\langle x, h_r, r \in \mathbb{Z}_t^* \rangle) = \langle \mathrm{T}_1, \mathrm{V}_{r^{-1}}, r \in \mathbb{Z}_t^* \rangle \cong \mathbb{Z}_t \rtimes \mathbb{Z}_t^*$ is an isomorphism.

Let CS_4 be the subgroup of H' isomorphic to S_4 which is generated by the 6 order-2 elements $\mathrm{C}_2 s_{ij}$ (i.e. compose every transposition s_{ij} with the complement C_2; they commute so order doesn't matter). Products corresponding to even permutations in S_4 will appear unchanged, while those corresponding to odd permutations in S_4 will be multiplied by C_2. Then, from Theorem 1 and Theorem 3, $\alpha(\mathbb{Z}_2^2 \rtimes S_3)$ is generated by $\mathrm{C}_2 s_{12} \mathrm{C}_2 s_{34} = s_{12}s_{34}$ and $\mathrm{C}_2 s_{13} \mathrm{C}_2 s_{24} = s_{13}s_{24}$ (shift action, isomorphic to $\mathbb{Z}_2^2$), and $\mathrm{C}_2 s_{23}$ and $\mathrm{C}_2 s_{23} \mathrm{C}_2 s_{24} = s_{23}s_{24}$ (automorphism action, isomorphic to S_3). Direct calculation shows that α maps $\mathbb{Z}_2^2 \rtimes S_3$ onto CS_4, so α is an isomorphism. Thus $H^* \cong (\mathbb{Z}_t \rtimes \mathbb{Z}_t^*) \times S_4$, and $\alpha(H)$ does not contain C_2. □

3.1 Proof of Theorem 3

Every cocyclic matrix M_ψ admits a decomposition as the Hadamard (pointwise) product of the cocyclic matrices corresponding to the generators. That is, $M_\psi = M_{\partial_1}^{\epsilon_1} \dots M_{\partial_{4t}}^{\epsilon_{4t}} M_\rho$, $\epsilon_i \in \{0,1\}$.

Each matrix M_{∂_i} is symmetric. Without loss of generality we negate the i^{th} row and i^{th} column of M_{∂_i}. These Hadamard equivalent matrices, denoted M_i, have a very particular form (see [1] for details). Each M_i is a 4×4-block back diagonal square matrix of order $4t$. The first block row has a 4×4 matrix $A_{[i]_4}$ as the $\lceil \frac{i}{4} \rceil^{th}$ block and 4×4 all-1s blocks in the other $t-1$ positions. The remaining block rows are obtained by successively back-cycling the first.

The 4×4-blocks $A_{[i]_4}$ depend on the equivalence class of i modulo 4, as follows. Let $R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $D = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ so $DR = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$. Then, adopting the notation blank for 1 and $-$ for -1, for brevity, $A_0 = \begin{pmatrix} & DR \\ DR & \end{pmatrix}, A_1 = \begin{pmatrix} D & \\ & D \end{pmatrix}, A_2 = \begin{pmatrix} DR & \\ & DR \end{pmatrix}, A_3 = \begin{pmatrix} & D \\ D & \end{pmatrix}$.

It may be checked without difficulty that bundle action by each of x, u, v, h_r and h_{243} leaves M_ρ invariant. Only action by h_{23} alters M_ρ. In terms of identifying diagram actions, it does not matter whether we work with M_{∂_i} or M_i so we use the latter. We determine each bundle action on M_i in the subsections below, concluding with the action of h_{23} on M_ρ.

3.1.1 Shift action of x

First, we change the order of the elements in the group to $g' = xg$, obtaining

$$(x,1) < (x,u) < \dots < (x^{t-1}, uv) < (1,1) < \dots < (1, uv)$$

that is, we put the first block of 4 elements at the end of the list.

For an individual coboundary ∂_i, the reordering takes the first four rows to the last four, moving the other rows upwards. Now the blocks $A_{[i]_4}$ start from the $\lceil \frac{i}{4} \rceil - 4^{th}$-column, the negated row is the $i - 4^{th}$ row, and the negated column is still the i^{th} column. Next we perform the pointwise product of the first row and the others. This first row (the former 5^{th}) has two negative entries, at positions i and $i-4$, so we have to negate these columns, getting the coboundary ∂_{i-4}.

So, the action of x on the cocyclic matrix is the 1-rotation T_1 on it.

3.1.2 Shift action of u

First, we change the order of the elements in the group to $g' = ug$, obtaining

$$(x^i, u) < (x^i, 1) < (x^i, uv) < (x^i, v),\ 0 \le i < t,\ (x^i, v) < (x^{i+1}, u),\ 0 \le i < t-1,$$

that is, we reorder every block of 4 elements by means of the permutation $\sigma = (12)(34)$.

For an individual coboundary ∂_i, the reordering permutes rows in the same way. This permutation transforms the blocks $A_{[i]_4}$ in the same way, under $(A_1A_2)(A_3A_0)$, the negated row is the $\sigma(i)^{th}$ and the negated column is the i^{th}. The first row (the former 2^{nd}) has two negative entries, at positions i and $\sigma(i)$. After negating these columns, we get the coboundary $\partial_{\sigma(i)}$.

So, the action of u on the cocyclic matrix is the composition of swappings $s_{21}s_{34}$.

3.1.3 Shift action of v

First, we change the order of the elements in the group to $g' = vg$, obtaining

$$(x^i, v) < (x^i, uv) < (x^i, 1) < (x^i, u),\ 0 \le i < t,\ (x^i, u) < (x^{i+1}, v)\ 0 \le i < t-1,$$

that is, we reorder every block of 4 elements by means of the permutation $\sigma' = (13)(24)$.

For an individual coboundary ∂_i, the reordering permutes rows in the same way. This permutation transforms the blocks $A_{[i]_4}$ in the same way, under $(A_1A_3)(A_2A_0)$, the negated row is the $\sigma'(i)^{th}$ and the negated column is the i^{th}. The first row (the former 3^{rd}) has two negative entries, at positions i and $\sigma'(i)$. After negating these columns, we get the coboundary $\partial_{\sigma'(i)}$.

So, the action of v on the cocyclic matrix is the composition of swappings $s_{13}s_{24}$.

3.1.4 Automorphism action of h_r

A straightforward algebraic calculation shows that $h_r(\partial_k) = \mathrm{V}_{r^{-1}}(\partial_k)$, for each $k = x^{k_x}u^{k_u}v^{k_v}$. Set $\delta_{ij} = -1$ if $i = j$, and $\delta_{ij} = 1$ otherwise.

On one hand, $h_r(\partial_k)(x^{i_x}u^{i_u}v^{i_v},\ x^{j_x}u^{j_u}v^{j_v})$

$$\begin{aligned} &= \partial_k(x^{r\cdot i_x \bmod t}\, u^{i_u}\, v^{i_v},\ x^{r\cdot j_x \bmod t}\, u^{j_u}\, v^{j_v}) \qquad (9)\\ &= \delta_{x^{k_x}u^{k_u}v^{k_v},\ x^{[r\cdot i_x]_t}u^{i_u}v^{i_v}}\ \delta_{x^{k_x}u^{k_u}v^{k_v},x^{[r\cdot j_x]_t}u^{j_u}v^{j_v}}\\ &\quad \delta_{x^{k_x}u^{k_u}v^{k_v},\ x^{[r\cdot(i_x+j_x)]_t}u^{[i_u+j_u]_2}v^{[i_v+j_v]_2}}. \end{aligned}$$

On the other hand, $\mathrm{V}_{r^{-1}}(\partial_k)(x^{i_x}u^{i_u}v^{i_v},\ x^{j_x}u^{j_u}v^{j_v})$

$$\begin{aligned} &= \partial_{x^{[k_x\cdot r^{-1}]_t}u^{k_u}v^{k_v}}(x^{i_x}\, u^{i_u}\, v^{i_v},\ x^{j_x}\, u^{j_u}\, v^{j_v}) \qquad (10)\\ &= \delta_{x^{[k_x\cdot r^{-1}]_t}u^{k_u}v^{k_v},\ x^{i_x}u^{i_u}v^{i_v}}\ \delta_{x^{[k_x\cdot r^{-1}]_t}u^{k_u}v^{k_v},\ x^{j_x}u^{j_u}v^{j_v}}\\ &\quad \delta_{x^{[k_x\cdot r^{-1}]_t}u^{k_u}v^{k_v},\ x^{[i_x+j_x]_t}u^{[i_u+j_u]_2}v^{[i_v+j_v]_2}}. \end{aligned}$$

A careful check, using the invertibility of r in $\mathbb{Z}_t$, shows these equations are equal term by term. Consequently, $h_r = \mathrm{V}_{r^{-1}}$, for all $r \in \mathbb{Z}_t^*$.

3.1.5 Automorphism action of h_{243}

The automorphism h_{243} shifts cyclically to the right the second, third and fourth positions of the elements in G, in each block of 4, leaving the first element

unchanged. So the action on the cocycles will be the same permutation of every second, third and fourth rows and columns in every block of four.

For an individual coboundary ∂_i, this reordering transforms the blocks $A_{[i]_4}$ in the same way, giving the permutation $(A_2A_3A_0)$, and the negated row/column remains unchanged if $[i]_4$ is 1 and is interchanged cyclically between cosets 2, 3 and 0, so we get the coboundary $s_{234}(\partial_i)$.

Hence, the action of h_{243} on any cocyclic matrix gives us the operation s_{234}.

3.1.6 Automorphism action of h_{23}

The action of the automorphism h_{23} on the cocyclic matrix will be the permutation of second and third rows and columns in every block of four.

For an individual coboundary ∂_i, this reordering transforms the blocks $A_{[i]_4}$ in the same way, giving the permutation (A_2A_3), and the negated row/column remains unchanged if $[i]_4$ is 0 or 1 and interchanged between cosets 2 and 3, so we get the coboundary $s_{23}(\partial_i)$.

The action of this reordering on matrix M_ρ applies the same permutation to its rows and columns, so the 4×4 blocks in (4) become

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

This expression coincides with the pointwise product of the 4×4 block in (4) and the block A_2 with the second row and column negated, so the action of the automorphism h_{23} on M_ρ gives us $M_\rho \cdot M_{\partial_2} \cdot M_{\partial_6} \dots M_{\partial_{4t-2}}$, the product with all coboundaries whose index is congruent to 2 modulo 4. Hence, by Lemma 1, $h_{23}(\partial_{d_1} \dots \partial_{d_k}\, \rho) = s_{23}(\partial_{d_1} \dots \partial_{d_k})\, (\prod_{i=0}^{t-1} \partial_{2+4i})\, \rho = \mathrm{C}_2(s_{23}(\partial_{d_1} \dots \partial_{d_k}))\, \rho$.

Hence, the action of h_{23} on any cocyclic matrix gives us the operation $\mathrm{C}_2 s_{23}$.

4 Complement

Next we demonstrate that complementation corresponds to matrix transposition and gives the matrix of the transpose cocycle.

Theorem 5 *The operation* C_2 *on* M_ψ *coincides with transposition:* $\mathrm{C}_2(M_\psi) = (M_\psi)^\top = M_{\psi^\top}$.

Proof. Consider $M_\psi = M_{\partial_{d_1}} \dots M_{\partial_{d_k}} M_\rho$. Since transposition commutes with pointwise products, $M_\psi^\top = M_{\partial_{d_1}} \dots M_{\partial_{d_k}} M_\rho^\top$. By (4)

$$M_\rho^\top = J_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix} = \left(J_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \right) \cdot M_\rho\,.$$

By (8), $M_\psi^\top = M_{\partial_{d_1}} \dots M_{\partial_{d_k}} \left(\prod_{i=0}^{t-1} M_{\partial_{2+4i}} \right) M_\rho = \mathrm{C}_2(M_\psi)$, as claimed. Since $G = \mathbb{Z}_t \times \mathbb{Z}_2^2$ is abelian, the transpose $\psi^\top$ of ψ, with $\psi^\top(g,h) = \psi(h,g)$, is a cocycle [9, (6.10)], and $(M_\psi)^\top = M_{\psi^\top}$. □

In summary, we have shown that the diagrammatic operations which can be implemented for effective calculation of cocyclic Hadamard matrices over $G = \mathbb{Z}_t \times \mathbb{Z}_2^2$, can all be interpreted as compositions of known algebraic equivalences, with the exception of complementation, which corresponds to matrix transposition. ÓCatháin [12] has used the algebraic equivalences together with transposition to determine classes of cocyclic matrices of order $4t$ over various G. He then checks any transposes lying in such a class to partition them into Hadamard inequivalence classes. He coins the term *strong inequivalence* for Hadamard matrices H and H' for which H' is not Hadamard equivalent to H or to $H^\top$. So, this approach using diagrammatic operations may be computationally effective.

It will also be interesting to investigate if diagrams and diagram operations can be found for cocycles over $G = D_{4t}$, and whether there are diagrammatic operations which correspond to Orrick's switching operations.

References

[1] V. Álvarez, J. A. Armario, M. D. Frau and P. Real, "A system of equations for describing cocyclic Hadamard matrices", *J. Comb. Des.*, vol. 16, pp. 276–290, 2008.

[2] V. Álvarez, J. A. Armario, M. D. Frau and P. Real, "The homological reduction method for computing cocyclic Hadamard matrices", *J. Symb. Comput.*, vol. 44, pp. 558-570, 2009.

[3] V. Álvarez, F. Gudiel and M. B. Güemes, "On $\mathbb{Z}_t \times \mathbb{Z}_2^2$-cocyclic Hadamard matrices". *J. Comb. Des.*, DOI 10.1002/jcd.21406 (2015).

[4] A. Baliga (= A. Rao) and K.J. Horadam, "Cocyclic Hadamard matrices over $\mathbb{Z}_t \times \mathbb{Z}_2^2$", *Australas. J. Combin.*, vol. 11, pp. 123–134, 1995.

[5] W. de Launey and D. L. Flannery, *Algebraic design theory*, Mathematical Surveys and Monographs 175. American Mathematical Society, Providence, RI, 2011.

[6] D.L. Flannery and R. Egan, "On linear shift representations", *J. Pure Appl. Algebra*, http://dx.doi.org/10.1016/j.jpaa.2014.12.007 (2014).

[7] K. J. Horadam, "Progress in cocyclic matrices", *Congr. Numer.*, vol. 118, pp. 161–171, 1996.

[8] K. J. Horadam, "The shift action on 2-cocycles", *J. Pure Appl. Algebra*, vol. 188, pp. 127–143, 2004.

[9] K. J. Horadam, *Hadamard matrices and their applications*. Princeton: Princeton University Press, 2007.

[10] K. J. Horadam, "Hadamard matrices and their applications: Progress 2007–2010", *J Cryptogr. Commun.*, vol. 2 (2), pp. 129–154, 2010.

[11] K. J. Horadam and W. de Launey, "Generation of cocyclic Hadamard matrices", in: *Proc. Computational Algebra and Number Theory*, Sydney, 1992, in *Math. Appl.*, vol. 325, Kluwer Acad. Publ., Dordrecht, pp. 279–290, 1995.

[12] P. ÓCatháin, *Automorphisms of pairwise combinatorial designs*, PhD Thesis, National University of Ireland-Galway, 2011.

[13] P. ÓCatháin and M. Röder, "The cocyclic Hadamard matrices of order less than 40", *Des. Codes Cryptogr.*, vol. 58 (1), pp. 73–88, 2011.

[14] W. P. Orrick, "Switching operations for Hadamard matrices", *SIAM J. Discrete Math.*, vol. 22 (1), pp. 31–50, 2008.

[15] A. Rao, "Shift equivalence and cocyclic self dual codes", *J. Combin. Math. Combin. Comput*, vol. 54, pp. 175–185, 2005.