The cocyclic Hadamard matrices of order less than 40

Padraig Ó Catháin[1]
Marc Röder[2]
School of Mathematics, Statistics and Applied Mathematics,
National University of Ireland, Galway.

Abstract

In this paper all cocyclic Hadamard matrices of order less than 40 are classified. That is, all such Hadamard matrices are explicitly constructed, up to Hadamard equivalence. This represents a significant extension and completion of work by de Launey and Ito. The theory of cocyclic development is discussed, and an algorithm for determining whether a given Hadamard matrix is cocyclic is described. Since all Hadamard matrices of order at most 28 have been classified, this algorithm suffices to classify cocyclic Hadamard matrices of order at most 28. Not even the total numbers of Hadamard matrices of orders 32 and 36 are known. Thus we use a different method to construct all cocyclic Hadamard matrices at these orders. A result of de Launey, Flannery and Horadam on the relationship between cocyclic Hadamard matrices and relative difference sets is used in the classification of cocyclic Hadamard matrices of orders 32 and 36. This is achieved through a complete enumeration and construction of $(4t, 2, 4t, 2t)$-relative difference sets in the groups of orders 64 and 72.

1. Introduction

A Hadamard matrix, H, of order n is an $n \times n$ matrix containing entries drawn from the set $\{1, -1\}$, which satisfies the equality

$$HH^\top = nI_n.$$

The *Hadamard conjecture* states that there exists a Hadamard matrix of order $4n$ for every natural number n. A stronger version of the Hadamard conjecture, posed in [5], is the *cocyclic Hadamard conjecture*: this asserts that there exists a cocyclic Hadamard matrix (briefly CHM) at every possible order. At the time of writing the smallest order for which no Hadamard matrix is known is 668 [9], and the smallest order for which no CHM is known is 188 (see Theorem 6.19 of [5]).

Once existence of some combinatorial object has been verified, it is natural then to ask for a classification of all such objects, up to some notion of equivalence. The enumeration and classification of Hadamard matrices has involved contributions from dozens of mathematicians, and was completed for all orders less than or equal to 28 by the mid 1990s. The details of this classification are contained in [16]. In [12], Orrick

March 11, 2010

proves the existence of at least 3 million inequivalent Hadamard matrices of order 32; he has since constructed more than 13 million.

Recently, there has been some work on the classification of Hadamard matrices possessing special algebraic properties. The focus here has been on the automorphism groups of Hadamard matrices, as this approach allows the application of algebraic techniques to what is otherwise a purely combinatorial problem. In this paper, we use algebraic techniques to classify all cocyclic Hadamard matrices of order at most 36. Amongst other things, this work solves Research Problem 43 of Horadam's book [5] for $5 \leq t \leq 9$.

The concept of cocyclic Hadamard matrix was introduced in [6]. The cocyclic property can be interpreted as the existence of an almost-regular action of the automorphism group on the Hadamard matrix. As shown in [3], CHMs are in fact equivalent to Ito's Hadamard groups (see [7]). In this paper we complete the classification of cocyclic Hadamard matrices of order 36 begun in [8]. To our knowledge, no previous attempt has been made to classify the cocyclic Hadamard matrices of order 32.

This paper is organised as follows, Section 2 gives some preliminaries for the paper. Section 3 describes and characterises group development. Section 4 generalises the results of Section 3 to cocyclic development. Section 5 describes a computational test based on the theory of Section 2, which suffices to classify the CHMs of order at most 28. Then in Section 6, we describe the relation between CHMs and relative difference sets: this material is the basis for the analysis of orders 32 and 36, which comprises Section 7. The final section of the paper provides a summary of our results, along with some observations and remarks.

2. Preliminaries

We set up a general framework for studying symmetries of square matrices whose entries lie in an abelian group. This covers the special case of Hadamard matrices, in which we are particularly interested. It applies also to other important classes of designs, such as complex Hadamard matrices, complex generalised Hadamard matrices, and generalised Hadamard matrices over abelian groups. Note however that most of our results may be generalised to matrices with entries in any finite group, and without any orthogonality conditions assumed.

Throughout this paper, A will be a finite abelian group written multiplicatively, with identity 1.

Notation 1. A homomorphism of free $\mathbb{Z}A$-modules $(\mathbb{Z}A)^n \to (\mathbb{Z}A)^m$ can be represented by an $n \times m$ matrix M with entries in $\mathbb{Z}A$. Any such matrix M will be called a *$\mathbb{Z}A$-matrix.* A matrix containing only entries from A will be called an *A-matrix.* If M contains exactly one entry from A in every row and column and zeros elsewhere, M is called *A-monomial.*

Although multiplication of $\mathbb{Z}A$-matrices does in general involve addition in $\mathbb{Z}A$, in this paper, we shall only be interested in products of A-matrices with A-monomial matrices. In this case, it is easily verified that all multiplication is carried out over A. Additionally, we observe that the product of two A-monomial matrices is again A-monomial.

In fact, the A-monomial matrices of order n form a group, isomorphic to $A \wr S_n$. Let $Mon\,(n, A) = \{(P, Q)\,|\,P, Q$ A-monomial of order $n\}$ under direct product multiplication. Then there is an action of $Mon\,(n, A)$ on the set of all A-matrices of order n, given by

$$(P, Q) \cdot M = PMQ^\top.$$

As usual, this action defines an equivalence relation, whereby two A-matrices are equivalent if and only if they lie in the same orbit. When A is the multiplicative group $\langle -1\rangle$ of order 2, we get the usual definition of Hadamard equivalence.

Definition 2. Two A-matrices M and N are called A-*equivalent*, written $M \equiv_A N$, if and only if there exist a pair of A-monomial matrices P and Q with $PMQ^\top = N$. If $M = N$, then we call (P, Q) an *automorphism* of M.

The pointwise stabiliser of M under the action of $Mon\,(n, A)$ is the set of all automorphisms of M. We denote this subgroup of $Mon\,(n, A)$ by $\mathrm{Aut}\,(M)$. If $(P, Q) \in \mathrm{Aut}(M)$ for permutation matrices P, Q, we call (P, Q) a *permutation automorphism*, and denote by $\mathrm{PermAut}\,(M)$ the subgroup of $\mathrm{Aut}\,(M)$ consisting of all permutation automorphisms of M. Since a subgroup U of $\mathrm{PermAut}\,(M)$ induces actions on the row numbers and column numbers of M (i.e. by sending row i to row j), we can apply standard permutation group terminology to U, e.g. we say that U is *regular* if U acts regularly on the row and column labels of M.

3. Group development

Definition 3. Let G be a group of order n. An $n \times n$ A-matrix M is called *group developed over* G if there exists a set map $\phi : G \to A$ such that

$$M = [\phi\,(gh)]_{g,h\in G}$$

where the rows and columns of M are indexed by the elements of G.

The notation introduced in Definition 3 assumes an ordering on the elements of G. The ordering is arbitrary, and need not be the same for rows and columns. Unless stated otherwise, there are no restrictions on this ordering; hence this notation really defines a permutation equivalence class of matrices.

Example 4. Let M be an $n \times n$ circulant matrix, with entries in A. Then M is group developed over the cyclic group $C_n = \langle c \mid c^n = 1\rangle$. We simply define the set map $\phi : C \to A$ by $\phi\left(c^{i-1}\right) = m_{1,i}$ for all $1 \leq i \leq n$. In fact, since we consider matrices only up to permutation of rows and columns, this result applies equally to back-circulant matrices.

In the remainder of this section, we show that group development of M is equivalent to the existence of a regular subgroup of $\mathrm{PermAut}(M)$. This permits a practical computational test of whether an A-matrix is group developed.

We recall the Kronecker delta notation: $\delta_r^s = 1$ if $r = s$ and $\delta_r^s = 0$ otherwise. For a group G of order n, and every $x \in G$, define the permutation matrices S_x and T_x by

$$S_x = [\delta_{xh}^g]_{g,h\in G} \qquad T_x = [\delta_h^{gx}]_{g,h\in G}\,.$$

Lemma 1. *Let M be an A-matrix of order n, and G a group of order n. Fix an ordering of the elements of G, and use this to index the rows and columns of M, T_x and S_x, $\forall x \in G$. Then M is group developed over G if and only if $(T_x, S_x) \in \mathrm{PermAut}\,(M)$ for all $x \in G$.*

Proof. Write $M = [\mu(g,h)]_{g,h\in G}$. Now

$$\begin{aligned} T_x M S_x^\top &= [\delta_a^{gx}]_{g,a\in G}\,[\mu(a,b)]_{a,b\in G}\,\left[\delta_h^{xb}\right]_{b,h\in G} \\ &= \left[\sum_{a\in G}\delta_a^{gx}\mu(a,b)\right]_{g,b\in G}\left[\delta_h^{xb}\right]_{b,h\in G} \\ &= [\mu(gx,b)]_{g,b\in G}\left[\delta_h^{xb}\right]_{b,h\in G} \\ &= \left[\sum_{b\in G}\mu(gx,b)\,\delta_h^{xb}\right]_{g,h\in G} \\ &= \left[\mu\left(gx,x^{-1}h\right)\right]_{g,h\in G}. \end{aligned}$$

Thus $(T_x,S_x)\in \mathrm{PermAut}(M)$ $\forall x\in G$ if and only if

$$\mu(g,h) = \mu\left(gx,x^{-1}h\right) \quad \forall g,h,x\in G. \tag{1}$$

If M is group developed, then $\mu(g,h) = \phi(gh)$ for some set map $\phi : G\to A$, and (1) is certainly satisfied:

$$\mu\left(gx,x^{-1}h\right) = \phi\left(gxx^{-1}h\right) = \phi(gh) = \mu(g,h).$$

Conversely, suppose that (1) is satisfied, and define $\phi(g) = \mu(g,1)$. Then

$$\mu(g,h) = \mu\left(gh,h^{-1}h\right) = \mu(gh,1) = \phi(gh) \quad \forall g,h\in G.$$

Hence M is group developed over G. □

Now, we impose a further condition on the ordering of G used in Lemma 1. We require that $T_1 = S_1 = I_n$. Note that the ordering of G may always be chosen such that this condition is satisfied. Thus we have the following result.

Theorem 2. *An A-matrix M is group developed over G if and only if* $\mathrm{PermAut}(M)$ *contains a subgroup isomorphic to G, acting regularly on the rows and columns of M.*

Proof. Suppose that M is group developed over G. Then by Lemma 1, $(T_x,S_x)\in \mathrm{PermAut}(M)$ for all $x\in G$. The map $x\mapsto (T_x,S_x)$ defines an isomorphism from G onto a subgroup of $\mathrm{PermAut}(M)$. Furthermore, this subgroup acts regularly on the rows and columns of M.

Conversely, suppose that $\mathrm{PermAut}(M)$ contains a subgroup isomorphic to G acting regularly on the rows and columns of M. We may write this subgroup as $\{(P_x,Q_x)\mid x\in G\}$ for permutation matrices P_x and Q_x such that $P_x M Q_x^\top = M$. As is well known, up to similarity, there is a single faithful regular permutation representation of G. This means that there exist permutation matrices U and V such that $UP_xU^\top = T_x$ and $VQ_xV^\top = S_x$ for all $x\in G$. Thus $UMV^\top$ is group developed over G by Lemma 1. Since group development is preserved by permutation equivalence, M is also group developed over G. □

Thus to determine whether a given A-matrix is group developed, we can compute its permutation automorphism group and check for the existence of regular subgroups.

It is well known that group developed Hadamard matrices have square order (see e.g. [5, p.21]). In the next section we define a generalisation of group development, drawing on group cohomology, which avoids this restriction.

4. Cocyclic development

Some of the ideas of this section, those behind Theorem 3 in particular, are due to Warwick de Launey, who first developed them for Hadamard matrices. Here, we present this material in a purely algebraic fashion, without imposing any orthogonality conditions on our matrices.

Definition 5. Let G be a group. A *2-cocycle*, or simply cocycle, is a map $\psi : G \times G \to A$ which obeys the following identity for all $g, h, k \in G$.

$$\psi\left(g,h\right)\psi\left(gh,k\right) = \psi\left(g,hk\right)\psi\left(h,k\right)$$

The set of all cocycles from G to A forms an abelian group under pointwise composition, denoted $Z^2\left(G, A\right)$. Without loss of generality, we may assume that all cocycles are normalised, i.e. that $\psi\left(1,1\right) = 1$. A *coboundary* is a cocycle of the form $\psi(g, h) = \phi(gh)\phi(g)^{-1}\phi(h)^{-1}$, where $\phi : G \to A$ is any nomralised set-map.

Definition 6. Let N, G be groups. An *extension of N by G* is a group E with a normal subgroup N', isomorphic to N, such that $E/N' \cong G$. We say that E is a *central extension of N by G* if N' is contained in the centre of E.

It is well known that a 2-cocycle $\psi : G \times G \to A$ determines a central extension of A by G: let $\Gamma_\psi = \{(g, a) \mid g \in G, a \in A\}$ with multiplication defined by

$$\left(g,a\right)\left(h,b\right) = \left(gh, ab\psi\left(g,h\right)\right).$$

Conversely, central extensions of A by G determine equivalence classes of cocycles from G to A. (Recall that to cocycles ψ and ψ' are equivalent if $\psi = \overline{\phi}\psi'$, where $\overline{\phi}$ is a coboundary.) This is the key idea that we use in defining cocyclic development of A-matrices.

Definition 7. An $n \times n$ A-matrix M is *cocyclic* if there exists a group G of order n, a cocycle $\psi \in Z^2\left(G, A\right)$ and a set map $\phi \colon G \to A$, such that

$$M \equiv_A \left[\psi\left(g,h\right)\phi\left(gh\right)\right]_{g,h\in G}.$$

We say that ψ *is a cocycle of M.*

A matrix, M as in Definition 7, where ϕ is trivial (as in Example 8 below) is called *pure cocyclic*. An A-matrix is cocyclic if and only if it is pure cocyclic. However in the more general setting of $\mathbb{Z}A$-matrices, the two notions are distinct. We note that just as permutation equivalence is the natural equivalence relation for group developed matrices, A-equivalence is the natural relation for cocyclic matrices.

Example 8. Let $C = \left\langle c \mid c^3 = 1\right\rangle$, and ω be a primitive complex cube root of unity. Let $\rho\left(1\right) = 1$ and $\rho\left(c\right) = \rho\left(c^2\right) = \omega$. Define the cocycle $\psi : C \times C \to \langle\omega\rangle$ by $\psi\left(c^i, c^j\right) = \rho\left(c^i\right)\rho\left(c^j\right)\rho\left(c^{i+j}\right)^{-1}$. Indexing row i and column i by c^{i-1}, we obtain the pure cocyclic matrix

$$M = \left[\psi(g,h)\right]_{g,h\in C} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}.$$

This matrix is a Butson Hadamard matrix of order 3 over the third roots of unity. Note that M is certainly not group developed, although it is $\langle\omega\rangle$-equivalent to a group developed matrix.

Cocyclic development is a generalisation of group development. Indeed group development corresponds to cocyclic development over the trivial cocycle (more generally, if M is cocyclic over a coboundary, then it is A-equivalent to a group developed matrix). Cocyclic development is associated with a special regular action of a central extension on an expanded matrix.

Definition 9. Let M be an $n \times n$ A-matrix, and fix an ordering $a_1, a_2, \ldots, a_k$ of the elements of A. With respect to this ordering, the expanded matrix of M, E_M, is the $kn \times kn$ A-matrix $[a_i a_j]_{a_i, a_j \in A} \otimes M$. That is:

$$E_M = \begin{pmatrix} a_1a_1M & a_1a_2M & \ldots & a_1a_kM \\ a_2a_1M & a_2a_2M & \ldots & a_2a_kM \\ \vdots & \vdots & \ddots & \vdots \\ a_ka_1M & a_ka_2M & \ldots & a_ka_kM \end{pmatrix}.$$

The following theorem characterises cocyclic development of M in terms of regular actions on E_M, and provides us with a practical test of whether an A-matrix is cocyclic. This is the foundation of our classification of cocyclic Hadamard matrices of order less than 32.

Theorem 3. *Let M be an $n \times n$ A-matrix. Then M is cocyclic with cocycle $\psi : G \times G \to A$ if and only if there is an isomorphism ι of Γ_ψ onto a regular subgroup of $\mathrm{PermAut}(E_M)$, such that $\iota\left((1, a)\right) = (T_a \otimes I_n, S_a \otimes I_n)$ for all $a \in A$.*

We refer to [11], Theorem 3.24, for a full proof of Theorem 3. Since Hadamard matrices are the main focus in the remainder of this paper, to illustrate the main ideas underlying Theorem 3 we include a proof for the special case $A = \langle -1 \rangle \cong C_2$.

Proof. Suppose that

$$M \equiv_A \left[\psi\left(g, h\right) \phi\left(gh\right)\right]_{g,h \in G}$$

for some cocycle $\psi : G \times G \to \langle -1 \rangle$ and set map $\phi : G \to \langle -1 \rangle$. Then

$$M \equiv_A \left[\psi'\left(g, h\right)\right]_{g,h \in G}$$

where $\psi'\left(g, h\right) = \psi\left(g, h\right) \phi\left(gh\right) \phi\left(g\right)^{-1} \phi\left(h\right)^{-1}$. As ψ and ψ' are cohomologically equivalent (i.e. differ by a coboundary), by basic cohomology theory we have that Γ_ψ and $\Gamma_{\psi'}$ are isomorphic by an isomorphism which maps the central involution $(1, -1)$ in the former group to $(1, -1)$ in the latter. It therefore suffices to assume in what follows that $M = \left[\psi\left(g, h\right)\right]_{g,h \in G}$.

We index the first n rows of E_M by the elements $(x, 1)$ of Γ_ψ, and index the remaining rows by the elements $(x, -1)$ of Γ_ψ. Let the columns of E_M be indexed in the same way. Then

$$E_M = \left[\mu\left((x, a)\left(y, b\right)\right)\right]_{(x,a),(y,b) \in \Gamma_\psi}$$

where $\mu : \Gamma_\psi \to \langle -1 \rangle$ is defined by $\mu(x, a) = a$. Hence by Theorem 2 there is an isomorphism of Γ_ψ onto a regular subgroup of $\mathrm{PermAut}(E_M)$. This isomorphism maps $(1, -1)$ to

$$\left(T_{(1,-1)}, S_{(1,-1)}\right) = (T_{-1} \otimes I_n, S_{-1} \otimes I_n) = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I_n, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I_n\right)$$

as required.

In the other direction, suppose that ι is an isomorphism of Γ_ψ onto a regular subgroup of $\mathrm{PermAut}(E_M)$. Then by Theorem 2,

$$E_M = [\phi((x, a)(y, b))]_{(x,a),(y,b) \in \Gamma_\psi}$$

for some map $\phi : \Gamma_\psi \to \langle -1 \rangle$. In particular, $\iota((1, -1))$ acts on E_M by moving row (x, a) to row $(x, -a)$, and column (y, a) to $(y, -a)$.

If we now impose the condition that $\iota(1, -1) = (T_{-1} \otimes I_n, S_{-1} \otimes I_n)$, we see that the first quadrant of E_M must have rows and columns indexed by elements (x, a) of Γ_ψ, where x ranges completely over G. Furthermore, the entry, $\phi(x, a)$, in row (x, a), column $(1, 1)$ of E_M, is equal to $-\phi(x, -a)$. Hence, $\phi(x, a) = a\phi(x, 1)$ for all $x \in G$, $a \in \langle -1 \rangle$. Thus,

$$E_M = [ab\psi(x, y)\,\phi(xy, 1)]_{(x,a),(y,b) \in \Gamma_\psi}\,.$$

Now, E_M is defined only up to permutation equivalence. Thus, we may rearrange the rows and columns so that the elements (x, a) in which $a = 1$ label the first half of the rows and columns of E_M. Then, from the definition of the expanded matrix,

$$M \equiv_{\langle -1 \rangle} \left[\psi(x, y)\,\widehat{\phi}(xy)\right]_{x,y \in G}$$

where $\widehat{\phi}(g) = \phi(g, 1)\ \forall g \in G$. This completes the proof of Theorem 3 for the case $A = \langle -1 \rangle$. □

Example 10. All Hadamard matrices of order 4 are Hadamard equivalent to

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

(As in Example 2, this matrix is not group developed, though it is equivalent to a group developed one.)

Let $Q_8 = \left\langle a, b \mid a^4 = 1, a^2 = b^2, b^a = b^{-1} \right\rangle$, the quaternion group of order 8, and denote the central involution $\left\langle a^2 \right\rangle$ of Q_8 by z. Define $\phi : Q_8 \to \langle -1 \rangle$ by $\phi(x) = 1$ if $x \in \{1, a, b, ab\}$ and $\phi(x) = -1$ otherwise. Indexing the rows and columns of E_H by the elements of Q_8 under the ordering $\{1, a, b, ab, z, az, bz, abz\}$, it is easily verified that $E_{H_4} = [\phi(xy)]_{x,y \in Q_8}$. Furthermore, z acts as required by Theorem 3, i.e. it interchanges the top half of E_{H_4} with the bottom, and the right half with the left. Hence H_4 is cocyclic over $Q_8 / \langle z \rangle \cong C_2 \times C_2$ by Theorem 3.

As the above proof of the special case of Theorem 3 indicates, the presence of a cocycle in a cocyclic matrix M occurs precisely because of the existence of a special regular action on the expanded matrix E_M of M. Although this is a purely algebraic phenomenon, E_M does have combinatorial significance when M is a design. For example, when M is a Hadamard matrix, E_M gives rise to the incidence matrix of a symmetric balanced incomplete block design in a natural way.

5. Testing whether a matrix is cocyclic

Let M be an $n \times n$ A-matrix. Assuming that we can compute $\mathrm{PermAut}(E_M)$, Theorem 3 provides a simple computational test for whether M is cocyclic: we search for regular subgroups of $\mathrm{PermAut}(E_M)$ containing $\Upsilon(A) := \{(T_a \otimes I_n, S_a \otimes I_n) \mid a \in A\}$ as a central subgroup. If we find such a regular subgroup R of $\mathrm{PermAut}(E_M)$, then M is cocyclic over $G \cong R/\Upsilon(A)$. In fact, using basic cohomology, we can even determine all cocycles of M. If no such subgroup of $\mathrm{PermAut}(E_M)$ exists, then M is not cocyclic.

The practical difficulty in this approach is that there is no publically available implemented algorithm for computing $\mathrm{PermAut}(E_M)$ when M has entries in an arbitrary abelian group, A. On the other hand there does exist a practical algorithm for computing the automorphism group of a $(0,1)$-array, using Brendan McKay's *nauty* programme [10], as implemented in the computer algebra system MAGMA [1]. To take advantage of this, we introduce the notion of the *associated matrix* L_M of M.

Definition 11. Let M be an $n \times n$ A-matrix. Define $e_{i,j}$ to be the entry in row i and column j of E_M. Then

$$L_M = \left[\delta^1_{e_{i,j}}\right]_{i,j}.$$

So if $l_{i,j}$ is in block a, b of L_M, then it contains a 1 if and only if the corresponding entry in E_M is $b^{-1}a^{-1}$.

Lemma 4. $\mathrm{PermAut}\,(E_M) = \mathrm{Aut}(L_M)$.

Proof. See [11]. In the special case that M is a $\langle -1 \rangle$-matrix, we observe that $L_M = 1/2\,(E_M + J_{2n})$, where J_{2n} is the all 1s matrix of order $2n$. Let (P,Q) be an automorphism of L_M; note that since L_M is a $(0,1)$-matrix, P and Q are necessarily permutation matrices. Then

$$PL_MQ^\top = 1/2\left(PE_MQ^\top + PJ_{2n}Q^\top\right).$$

Now, J_{2n} is invariant under permutation of rows and columns, which implies that $(P,Q) \in \mathrm{PermAut}(E_M)$. The proof in the other direction is similar. □

Thus, we now have a practical method of determining whether a given matrix defined over an abelian group is cocyclic. This provides us with the necessary tool to classify all cocyclic Hadamard matrices of a given order n, as long as we have a classification, up to Hadamard equivalence, of all Hadamard matrices of order n. That is, selecting a representative, H, from each Hadamard equivalence class, we compute $\mathrm{Aut}(L_H)$, and determine all regular subgroups of $\mathrm{Aut}(L_H)$ containing $\Upsilon(\langle -1 \rangle)$ as a central subgroup of order 2.

A summary of the computational results that we obtained via this procedure, amounting to a complete classification of all cocyclic Hadamard matrices of order less than 32, appears in the final section of this paper.

To conclude this section, we emphasize again that the preceding discussion makes no assumption that the A-matrices have any combinatorial properties (such as orthogonality). However, one can obtain additional results by imposing conditions on M, as in the following theorem.

Theorem 5. *Let M be an invertible A-matrix. Then* $\mathrm{Aut}\,(M) \cong \mathrm{PermAut}\,(E_M)$.

Proof. See [11, pp. 42-43]. □

6. Cocyclic Hadamard matrices and Relative Difference Sets

In this section, we expand upon a result of de Launey, Flannery and Horadam. We prove that each equivalence class of relative difference sets with parameters $(4t, 2, 4t, 2t)$ corresponds to at least one and at most two equivalence classes of cocyclic Hadamard matrices of order $4t$. We use this result in Section 7 to determine all cocyclic Hadamard matrices of orders 32 and 36. We begin with a review of some relevant definitions.

Definition 12. Let G be a finite group, with normal subgroup N. We say that $R \subset G$ is a relative difference set (RDS) with respect to N, if in the multiset of elements $\left\{r_1 r_2^{-1} \mid r_1, r_2 \in R\right\}$, every element of $G - N$ occurs exactly λ times, and no non-trivial element of N occurs.

We refer to N as the *forbidden subgroup.* If N is of order n, G is of order nm and the RDS contains k elements, then we speak of a (m, n, k, λ)-RDS. We are particularly interested in $(4t, 2, 4t, 2t)$-RDSs, as a consequence of the following theorem.

Theorem 6. *Let G be a group of order $4t$. Then there exists a Hadamard matrix cocyclic over G if and only if there exists a $(4t, 2, 4t, 2t)$-RDS in a central extension of $N \cong \mathrm{C}_2$ by G, with forbidden subgroup N.*

Proof. See [2], Theorem 2.4. □

A group of order $8t$ containing a $(4t, 2, 4t, 2t)$-RDS is called a Hadamard group by Ito [7]. Following this usage, we call a $(4t, 2, 4t, 2t)$-RDS a *Hadamard relative difference set* (HRDS).

Definition 13. Let R be a subset of a group G of order n. The *development* of R, denoted $Dev\,(R)$, is the matrix

$$2\left[\chi_R\,(ab)\right]_{a,b\in G} - J_n$$

where χ_R is the characteristic function of R, taking the value 1 on ab if $ab \in R$ and 0 otherwise.

We will be interested in the case where Γ is a group of order $8t$ and R is a HRDS in Γ. In this case, $Dev\,(R)$ is the expanded matrix of a CHM. A normalised CHM is obtained by extracting all rows and columns from $Dev\,(R)$ that are labelled by elements of R.

The crucial observation here is that if R is a HRDS, then $|R \cap gR| = 2t$, for $g \in \Gamma - N$. This of course implies that all rows extracted are orthogonal. A similar argument shows that if the development of $R \subset \Gamma$ is the expanded matrix of a CHM, then R is a HRDS. Given a CHM, H, there exists a group Γ which acts regularly on E_H. A HRDS in Γ corresponds to the elements which label rows with initial entry 1 in the expanded matrix.

Thus, denoting permutation equivalence of matrices by $\approx$, we have the following result.

Theorem 7. *H is a cocyclic Hadamard matrix if and only if $E_H \approx Dev\,(R)$, where R is a HRDS in some group Γ.*

In the remainder of this section, we relate the standard definitions for equivalence of RDSs and Hadamard matrices to show that a given HRDS corresponds to either one or two cocyclic Hadamard matrices. Equivalence of RDSs motivates the following definitions.

Definition 14. We call a map $\vartheta : G \to G$ an *antiendomorphism* of G if $\vartheta\,(gh) = \vartheta\,(h)\,\vartheta\,(g)$, for all $g, h \in G$. An *antiautomorphism* is a bijective antiendomorphism.

We denote the group consisting of all automorphisms and antiautomorphisms of G by $\mathrm{AntiAut}\,(G)$. We observe that $\mathrm{Aut}\,(G)$ is a normal subgroup of index at most 2 in $\mathrm{AntiAut}\,(G)$, and that this group is generated by $\mathrm{Aut}\,(G)$ and the inversion map. (Thus $\mathrm{AntiAut}(G) = \mathrm{Aut}(G)$ if and only if G is abelian.) Our definition of equivalence for RDSs differs from that in [5, p.164], in that we allow not just automorphisms, but antiautomorphisms of the group G.

Definition 15. Let $R, R' \subset G$ be (m, n, k, λ)-RDSs, with forbidden subgroups N and N' respectively. Then R is *equivalent* to R' if and only if there exist $g \in G$ and $\vartheta \in \mathrm{AntiAut}\,(G)$ such that $\vartheta(N) = N'$ and

$$R' = \vartheta(R)g = \{\vartheta\,(x)\,g \mid x \in R\}\,.$$

It is routine to check that this is indeed an equivalence relation on the set of all (m, n, k, λ)-RDSs in G.

Lemma 8. *Let $R \subset G$ be an RDS, $g \in G$ and $\zeta \in \mathrm{Aut}(G)$. Then*

1. *$Dev(\zeta(R)g) \approx Dev(R)$;*
2. *$Dev(R^{-1}) \approx Dev(R)^\top$.*

Proof. The first part follows directly from the fact that automorphisms of G induce permutations on the rows and columns of $Dev(R)$.

For the second part it suffices to consider $Dev(R^{-1})$ in which the columns and rows are permuted so that $Dev(R) = \left[\chi\left(gh^{-1}\right)\right]_{g,h\in G}$. Then $Dev(R^{-1}) = \left[\chi\left(g^{-1}h\right)\right]_{g,h\in G} \approx Dev(R)^\top$. (Note in particular that unless G is abelian, $Dev(R)$ and its transpose need not be permutation equivalent.) □

Lemma 9. *Let H and H' be Hadamard matrices. Then $E_H \approx E_{H'}$ if and only if $H \equiv_{\langle -1\rangle} H'$.*

Proof. Assume that $H \equiv_{\langle -1\rangle} H'$. Then there exist a pair of $\langle -1\rangle$-monomial matrices, (P, Q) such that $PHQ^\top = H'$. Both P and Q may be uniquely decomposed into $(0, 1)$ matrices, P_1, P_{-1}, Q_1 and Q_1 such that $P = P_1 - P_{-1}, Q = Q_1 - Q_{-1}$. It is then easily verified that:

$$\begin{pmatrix} P_1 & P_{-1} \\ P_{-1} & P_1 \end{pmatrix} \begin{pmatrix} H & -H \\ -H & H \end{pmatrix} \begin{pmatrix} Q_1^\top & Q_{-1}^\top \\ Q_{-1}^\top & Q_1^\top \end{pmatrix} = \begin{pmatrix} H' & -H' \\ -H' & H' \end{pmatrix}$$

This suffices for one direction of the proof.

Now, assume that $E_H \approx E_{H'}$. Then

$$\begin{pmatrix} P_\alpha & P_\beta \\ P_\gamma & P_\delta \end{pmatrix} \begin{pmatrix} H & -H \\ -H & H \end{pmatrix} \begin{pmatrix} Q_\alpha^\top & Q_\gamma^\top \\ Q_\beta^\top & Q_\delta^\top \end{pmatrix} = \begin{pmatrix} H' & -H' \\ -H' & H' \end{pmatrix}.$$

Multiplying out these block matrices, we obtain four equations of the form

$$(P_\alpha - P_\beta)\, H \left(Q_\alpha^\top - Q_\beta^\top\right) = H'. \tag{2}$$

Consideration of any one suffices in this context however. The matrix H' is Hadamard, and so contains no zero entries. Thus $(P_\alpha - P_\beta)$ and $\left(Q_\alpha^\top - Q_\beta^\top\right)$ are necessarily $\langle -1\rangle$-monomial matrices. Hence $H \equiv_{\langle -1\rangle} H'$, as required. □

Note that this result can be extended in several directions. As an example, the equations (2) imply that $P_\alpha = P_\delta$, $P_\beta = P_\gamma$, $Q_\alpha = Q_\delta$ and $Q_\beta = Q_\gamma$, which imposes non-trivial restrictions on the automorphism group of an expanded matrix. This is the essence of the proof of Theorem 5. In this paper, we develop these ideas only enough for our purpose, which is the proof of Theorem 10.

Definition 16. Let $R \subset G$ be a HRDS, with $Dev(R) \approx E_H$ for some cocyclic Hadamard matrix, H. We say that R is *associated with* H.

Theorem 10. *Suppose that R is a HRDS associated with H. Then R is also associated with $H^\top$. R is associated with a single class of cocyclic Hadamard matrices precisely when $H \equiv_{\langle -1\rangle} H^\top$.*

Proof. Immediate from Lemmas 8 and 9. □

Now, we have shown that if H is a CHM, then $E_H \approx Dev(R)$ for some HRDS R in a group Γ. Furthermore, any CHM, H', which is Hadamard equivalent either to H or $H^\top$ will have $E_{H'} \approx Dev(R')$, where R' is equivalent to R. Thus, to find representatives of all equivalence classes of CHMs of order $4t$, up to transposition, it suffices to find all HRDSs in groups of order $8t$, up to equivalence. Recall that we allow anti-automorphisms of G in our definition of RDS equivalence. Restricting to automorphisms gives a one-to-one correspondance between equivalence classes of CHMs and HRDSs. We use the coarser definition of equivalence to increase the efficiency of our computer search.

We conducted our search for $t = 8$ and $t = 9$ using the GAP package RDS (see [4] & [15]) for construction of all HRDSs at the appropriate orders, and then extracted CHMs from their developments. Details of these computations are contained in the next section.

7. Analysis of orders 32 and 36

In this section we describe our search for all HRDSs in the groups of order 64 and 72. We begin by generalising a classical result of Bruck on relative difference sets; for a fuller treatment, see [13].

Theorem 11. *Let G be a group of order mn. Let R be a (m, n, k, λ)-RDS in G, with forbidden subgroup N, of order n. Let U be a normal subgroup of G, and denote by $T = \{g_1, g_2, \ldots, g_{|G:U|}\}$ a transversal of U in G. Furthermore, let $v_i = |R \cap g_iU|$ and $v_{ij} = |R \cap g_ig_jU|$. Then the following relations hold.*

$$\sum_{i\in T} v_i = k \tag{3}$$

$$\sum_{i\in T} v_i^2 = \lambda\left(|U| - |U \cap N|\right) + k \tag{4}$$

$$\sum_{j\in T} v_jv_{ij} = \lambda\left(|U| - |g_iU \cap N|\right) \textit{for } g_i \notin U \tag{5}$$

Proof. Let $\vartheta\colon \mathbb{Z}[G] \to \mathbb{Z}[G/U]$ be the epimorphism of group-rings induced by the canonical epimorphism of groups $\rho\colon G \to G/U$.

We have:

$$\vartheta(R) = \sum_{g_i\in T} v_ig_iU$$

$$\vartheta(R^{-1}) = \vartheta(\sum_{r\in R} r^{-1}) = \sum_{i=1}^{|G:N|} v_ig_i^{-1}U.$$

Hence

$$\vartheta(RR^{-1}) = \Big(\sum_{i=1}^{|G:N|} v_ig_iU\Big)\Big(\sum_{j=1}^{|G:N|} v_jg_j^{-1}U\Big) = \sum_{i=1}^{|G:N|}\Big(\sum_{j=1}^{|G:N|} v_jv_{ij}\Big)g_iU. \tag{6}$$

Writing $\mathcal{N} = \{g_i \in T \mid g_iU \cap N \neq \emptyset\}$ and assuming $g_1 \in U$, we get from the definition of relative difference sets

$$\vartheta(RR^{-1}) = k \cdot g_1U + \lambda\Big(\sum_{g\in(G-N)} gU\Big) \tag{7}$$

$$= k \cdot g_1U + \lambda\Big(\sum_{g_i\in T-\mathcal{N}} g_iU|U| - \sum_{g_i\in\mathcal{N}} g_iU|g_iU \cap N|\Big). \tag{8}$$

Comparing coefficients in (6) and (8), we get

$$\sum v_iv_{1i} = \sum v_i^2 = k + \lambda(|U| - |U \cap N|)$$

and

$$\sum_j v_jv_{ij} = \begin{cases} \lambda|U| \text{ if } g_iU \notin \rho(N) \\ \lambda(|U| - |U \cap N|) \text{ if } \rho(g_i) \in \rho(N) - \{U\} \end{cases}$$

□

We call $[v_i \mid 1 \leq i \leq |G : U|]$ a *signature* for R with respect to U. Note that the ordering of the signature depends on the ordering of the cosets of U. If the equations have no solution for a given group G, then there can be no relative difference set with the given parameters. We show there are only two signatures possible for a HRDS in a group of order 64. We consider a normal subgroup of order 16. This is permissible: a routine calculation shows that all groups of order 64 contain a normal subgroup of index 4.

Lemma 12. *Let G be a group of order 64 and let U be a normal subgroup of index 4. Suppose that R is a HRDS in G with forbidden subgroup N. Then the signature of R with respect to U is of one of two types:* $[6, 6, 10, 10]$*, or* $[8, 8, 8, 8]$*. Furthermore, signatures of the first kind occur only when $G/U \cong C_4$, and the non-trivial element of N lies in the unique coset of U of order 2.*

Proof. We simply apply the conditions of Theorem 11 to a HRDS in G. Now, from (3) we have that

$$v_1 + v_2 + v_3 + v_4 = 32.$$

From here we break our analysis into two cases: in the first, $|U \cap N| = 1$, and in the second $N \leq U$.

- If $|U \cap N| = 1$, then by (4)

  $$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 16 \cdot 17.$$

  We observe that all squares modulo 16 lie in $\{0, 1, 4, 9\}$. The only solutions modulo 16 to the above equation are:

  $$0 + 0 + 0 + 0 = 0, \quad 4 + 4 + 4 + 4 = 0.$$

  Inspection shows that there exist only two valid solutions to the above equation, namely $2^2+6^2+6^2+14^2 = 272$ and $6^2+6^2+10^2+10^2 = 272$. However $2+6+6+14 \neq 32$. Thus we are left with only a single valid solution.

- If $|U \cap N| = 2$, then

  $$v_1^2 + v_2^2 + v_3^2 + v_4^2 = 16\,(16 - 2) + 32 = 16^2.$$

  We observe that in this case the sum of the squares is in fact minimal, and is achieved only if

  $$v_1 = v_2 = v_3 = v_4 = 8.$$

As for the second part of the lemma, we observe that if $|U \cap N| = 1$ then $U \times N$ is a normal subgroup of G of index 2. Now $G/U \cong C_2 \times C_2$ only if G splits over N. In this case the corresponding Hadamard matrix is equivalent to a group developed matrix. This is a contradiction as the order of the matrix, 32, is not a square. Thus $G/U \cong C_4 = \langle \alpha \mid \alpha^4 = 1 \rangle$, and $n \neq 1 \in N$ lies in the coset $\alpha^2 U$. □

A similar result for the groups of order 72 can be derived by the same method. Of the 50 groups of order 72, all but one contain a normal subgroup of order 12. The exception does not contain a normal subgroup of order 2, and so does not warrant further consideration. There are four possible signatures when $|U \cap N| = 1$.

Lemma 13. *Let G be a group of order 72 and let U be a normal subgroup of index 6. Suppose that R is a HRDS in G with forbidden subgroup N. Then the signature of R is one of the following:*

- $[6,6,6,6,6,6]$ *if* $|U \cap N| = 2$,
- *one of* $[3,5,6,6,8,8]\,,[3,6,6,6,6,9]\,,[4,4,5,7,8,8]\,,[4,4,6,6,7,9]$ *if* $|U \cap N| = 1$.

Definition 17. We call $R \subset G$ a *partial difference set* (short: pRDS) with parameters $(4t, 2, 4t, 2t)$ relative to $N \trianglelefteq G$, if every element of $G - N$ can be written in at most $2t$ ways as a quotient in R, and no element of N can be expressed in this way. We say that a pRDS has *length k* if it contains k elements.

Our search for all HRDSs in the groups of order 64 and 72 was carried out using the computer algebra system GAP, using the RDS package to search for relative difference sets. The following algorithm was used.

1. Calculate all normal subgroups of order 2.
2. Calculate a system of representatives $\mathcal{N}$ of $\mathrm{Aut}(G)$-orbits on the normal subgroups of order 2.

The elements of $\mathcal{N}$ are used as forbidden subgroups of relative difference sets. So for every $N \in \mathcal{N}$, we find the relative difference sets with respect to N:

3. Calculate signatures (solutions of the equations of Theorem 11) with respect to every normal subgroup of order ≥ 16 (12 respectively). (The signatures of subgroups of smaller index may be used in the reduction step.)
4. Find $U \trianglelefteq G$ with unique signature of the form $\{i, \ldots, i\}$ (all entries the same). Such a subgroup always exists in the cases we considered.

Next, we generate all relative difference sets coset-wise. We start with the coset U and the set $P = \{\{1\}\}$ of partial difference sets (note that this can be done without loss of generality). For the reduction steps (6) below, we use equivalence as defined in Theorem 8 with a smaller automorphism group $A \leq (\mathrm{Aut}(G)_N)_U$ which acts trivially on G/U.

5. Calculate $P' := \bigcup_{p \in P} \{p \subset p' \subset U \mid |p'| = |p| + 1, \text{ and } p' \text{ is pRDS}\}$.
6. Calculate a system of representatives P'' of equivalence classes on P'.

Steps 5 and 6 are iterated to get partial difference sets of length i in U. By step 4, we know that this is the maximal length for partial difference sets in U.

This procedure is repeated with the next coset modulo U starting with partial difference sets of length i and generating sets of length $2i$. Continuing in this fashion, we find all relative difference sets in G with forbidden subgroup $N \in \mathcal{N}$.

Notes

The actual implementation of our algorithm differs slightly from the outline above, as we made use of the following heuristic methods.

(i) The signatures calculated in step 3 can be used in the reduction step 6 as an invariant. See [13, 14] for details.

(ii) The reduction steps are very time-consuming, so steps 5 and 6 are not iterated i times, but a brute-force algorithm is used after fewer steps.
Also, steps 5 and 6 were not used for all cosets modulo U. Depending on the specific case, we used a brute-force method after a few cosets.

(iii) A final reduction step was introduced just before changing cosets to compensate for the redundancy generated by the brute-force method.

(iv) After generating all difference sets in G (for all possible forbidden subgroups in $\mathcal{N}$), we apply a reduction step with the full group $\mathrm{Aut}(G)$ to get all RDSs up to equivalence.

8. Summary of Results

All Hadamard matrices of order at most 20 are cocyclic. Beyond this, it seems that that the number of cocyclic Hadamard matrices is approximately proportional to the number of indexing groups. A result of Ito [7, Propositions 6,7] proves that the group G cannot contain a HRDS if it has cyclic or dihedral type Sylow 2-subgroup. The existence of a cyclic Hadamard group of order ≥ 4 would disprove the Circulant Hadamard conjecture. We observe that up to order 36, groups of lower exponent are more likely to be Hadamard groups.

The algorithm of Section 5 and the classification of Hadamard matrices in [16] were used to construct all CHMs of order less than 30. The algorithm of Section 7 and information from the Small Groups Library, available in MAGMA [1], were used to generated all cocyclic matrices of orders $20, 24, 28, 32$ and 36. Both classifications agreed on their intersection.

The classification of CHMs of order 32 is, to our knowledge, entirely new. The classification of CHMs of order 72 was begun by Ito and Okomoto [8], who found 15 matrices, but is completed here.

The following table gives a brief summary of our results. We list the number of cocyclic Hadamard matrices for all orders less than 40 (given as a fraction of the total number of Hadamard matrices where appropriate - these numbers are taken from [12]). Likewise we list the number of indexing and extension groups at each order as a fraction of the total.

Order	Cocyclic	Indexing Groups	Extension Groups
2	1	1	2
4	1	2	3 / 5
8	1	3 / 5	9 / 14
12	1	3 / 5	3 / 15
16	5	13 / 14	45 / 51
20	3	2 / 5	3 / 14
24	16 / 60	8 / 15	14 / 52
28	6 / 487	2 / 4	2 / 13
32	$100/ \geq 3 \times 10^6$	49/51	261/267
36	$35 / \geq 3 \times 10^6$	12 /14	21 / 50

It is not practical to list here the CHMs that were found. Instead, we direct interested readers to `www.maths.nuigalway.ie/~padraig`, where the matrices are available. We provide generators for the full automorphism group of each matrix (given as a permutation group acting the rows and columns of the expanded matrix). We also provide a list of groups over which each matrix is cocyclic, and the extension group over which the expanded matrix is group developed. These computations were all carried out in MAGMA.

Acknowledgements

The first author would like to thank Dr. Dane Flannery, for his advice and support.

The first author would also like to thank Dr. Warwick de Launey, who encouraged the writing of this paper, and gave generous observations on the ideas contained herein.

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. the user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[2] Warwick de Launey, D. L. Flannery, and K. J. Horadam. Cocyclic Hadamard matrices and difference sets. *Discrete Appl. Math.*, 102(1-2):47–61, 2000.

[3] D. L. Flannery. Cocyclic Hadamard matrices and Hadamard groups are equivalent. *J. Algebra*, 192(2):749–779, 1997.

[4] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12.* http://www.gap-system.org.

[5] K. J. Horadam. *Hadamard Matrices and their Applications.* Princeton University Press, Princeton, NJ, 2007.

[6] K. J. Horadam and W. de Launey. Cocyclic development of designs. *J. Algebraic Combin.*, 2(3):267–290, 1993.

[7] Noboru Ito. On Hadamard groups. *J. Algebra*, 168(3):981–987, 1994.

[8] Noboru Ito and Takeo Okamoto. On Hadamard groups of order 72. *Algebra Colloq.*, 3(4):307–324, 1996.

[9] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *J. Combin. Des.*, 13(6):435–440, 2005.

[10] B. McKay. *nauty User's Guide, Version 2.2.* http://cs.anu.edu.au/~bdm/nauty/nug.pdf, 2007.

[11] Padraig Ó Catháin. *Group Actions on Hadamard matrices.* M.Litt. Thesis, National University of Ireland, Galway, 2008. http://www.maths.nuigalway.ie/~padraig/research.shtml.

[12] William P. Orrick. Switching operations for Hadamard matrices. *SIAM J. Discrete Math.*, 22(1):31–50, 2008.

[13] Marc Röder. *Quasiregular Projective Planes of Order* 16 *– A Computational Approach.* PhD thesis, Technische Universität Kaiserslautern, 2006. http://kluedo.ub.uni-kl.de/volltexte/2006/2036/.

[14] Marc Röder. The quasiregular projective planes of order 16. *Glasnik Matematicki*, 43(2):231–242, 2008.

[15] Marc Röder. *RDS, Version 1.1.* http://www.gap-system.org/Packages/rds.html, 2008.

[16] Edward Spence. Classification of Hadamard matrices of order 24 and 28. *Discrete Math.*, 140(1-3):185–243, 1995.