National University of Ireland, Galway

Group actions on Hadamard matrices

by

Padraig Ó Catháin

A thesis submitted in partial fulfillment for the
degree of Master of Literature

in the
Faculty of Arts
School of Mathematics, Statistics and Applied Mathematics
Supervisor: Dr. Dane Flannery
Head of School: Dr. Ray Ryan

November 2008

National University of Ireland, Galway

Abstract

Faculty of Arts
Mathematics Department

Master of Literature

by Padraig Ó Catháin

Hadamard matrices are an important item of study in combinatorial design theory. In this thesis, we explore the theory of cocyclic development of Hadamard matrices in terms of regular group actions on the expanded design. To this end a general theory of both group development and cocyclic development is formulated. This theory is used to classify all regular actions on the expanded designs of Hadamard matrices of order less then 32 that contain a special central involution. We show that such a regular action exists if and only if the matrix is cocyclic. In addition the cocyclic development properties of several Hadamard matrix constructions are reviewed. Some relevant results from the literature are presented, and some non-existence results are given for certain small orders. This work settles some research problems posed by K.J. Horadam in a recent book on Hadamard matrices.

Contents

List of Tables

Chapter 1

Introduction

The goal of this thesis is to develop the theory of group actions on square arrays. The first part of the thesis will develop a broad theory; the second part will apply this to the problem of the classification of Hadamard matrices, with certain regular group actions.

The first chapter begins with a brief introduction to combinatorial design theory as a background to Hadamard matrices. Group development of square matrices is also discussed, as a motivation for cocyclic development. We finish the chapter with an overview of the relationship between cocyclic Hadamard matrices and relative difference sets. The second chapter develops the cohomology of central extensions of groups. The third chapter then develops the theory of group actions on square arrays in an abstract fashion. The fourth chapter applies the theory developed thus far to the specific case of Hadamard matrices. The remaining chapters of the thesis apply this machinery to various open problems in the area of Hadamard matrices. Chapter 5 gives a classification of all cocyclic Hadamard matrices of order at most 28. Chapter 6 is a survey of the literature on cocyclic Hadamard matrix constructions. We show that a cocyclic Hadamard matrix exists at every possible order up to 188. In Chapter 7 we survey some constructions that are suspected not to be cocyclic. We give non-existence results at some small orders, providing partial answers to questions posed by Horadam in [1]. The thesis concludes with two short appendices that give, verbatim, some of the more important programs that we wrote for use with the Magma computer algebra system, [2].

The Magma database of Hadamard matrices and a paper by Kotsireas, Koukouvinos and Seberry, [3], dating from 2006 both agree on the number of known equivalence classes of Hadamard matrices of small order. As a by-product of some of our computations, several hundred equivalence classes of Hadamard matrices not found in these sources have been discovered.

1.1 Combinatorial designs

We begin with a brief introduction to combinatorial design theory, which is concerned primarily with the study of incidence structures. Designs are simply incidence structures to which additional constraints are added. Thus any results we give about incidence structures apply also to designs.

Definition 1.1. An incidence structure is a triple of sets $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ with $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. We will often present the information contained in $\mathcal{I}$ in the form of a $(0,1)$-matrix, with rows labelled by elements of $\mathcal{P}$, called points, and columns labelled by elements of $\mathcal{B}$, called blocks. The entry in row p, column b will be 1 if $(p,b) \in \mathcal{I}$, and 0 otherwise. We generally refer to p as being on b if $(p,b) \in \mathcal{I}$.

Incidence structures alone are too basic to be of any great theoretical interest. It is only when additional conditions are imposed on $\mathcal{I}$ that substantial results may be obtained. The family of incidence structures that has received the most attention in recent years is that of t-structures. By definition these structures contain blocks of fixed size k.

Definition 1.2. $\mathcal{S}$ is a t-structure if for any integer n such that $0 \leq n \leq t$, there exists $\lambda_n \geq 0$ such that any set of points of size n occurs on exactly λ_n different blocks.

Note that $\mathcal{S}$ is a 1-structure only if $\lambda_1 = |b|$ is fixed for all $b \in \mathcal{B}$. It is traditional to refer to λ_1 as k and $|\mathcal{P}|$ as v. When $t \neq 1$ we refer to λ_t simply as λ. We will be interested in structures that are *at least* 1-structures. In this case we will refer to them as $t-(v,k,\lambda)$ structures.

Standard combinatorial results show that t-structures exist only for suitable choices of v, k and λ. Two of the most important tools in this area are the following equalities, the first of which holds for any 1-structure, and the second for any 2-structure:

$$|\mathcal{B}|\, k = v\lambda \tag{1.1}$$

$$\lambda_1 (k-1) = \lambda_2 (v-1) \tag{1.2}$$

Derivations of these formulae may be found in Chapter 1 of [4]. In any case, they follow from simple counting arguments on the numbers of points and blocks. Finally, we give the formal definition for a design.

Definition 1.3. A design is a structure with no repeated blocks.
Equivalently, we require that the incidence matrix have no repeated columns. This restriction on the blocks of a design turns out to be very strong. For example, no non-trivial designs at all are known with $t \geq 7$. [4] In comparison, it is a relatively straightforward exercise to construct a non-trivial incidence structure for any value of t.

1.2 Symmetric designs and 2-designs

If $\mathcal{S}$ is a design with parameters 2-(v, k, λ), then any pair of distinct points will occur on exactly λ blocks. Since every 2-design is also a 1-design, every point will occur on exactly $\frac{|\mathcal{B}|k}{v}$ blocks, by (1.1), and there will be $\frac{\lambda v(v-1)}{k(k-1)}$ blocks in total, by (1.2).

We will be interested in particular in symmetric designs, which have $|\mathcal{B}| = |\mathcal{P}| = v$. Given this restriction, we observe that the number of blocks on a given point must be equal to k, the number of points on a block. This is the origin of the name symmetric: the transpose of such a design is also a symmetric design. This family of designs is one of the central objects of study in modern combinatorial design theory. It is a well established result that all symmetric designs with $t \geq 3$ are trivial, see Theorem 1.27 of [4] hence only symmetric 2-designs are suitable objects of study. Of particular interest are symmetric designs for extremal values of λ: if $\lambda = 1$, then the design is a projective plane, while if λ is maximal we obtain a Hadamard 2-design. In this thesis we will be mostly concerned with Hadamard 2-designs, which have parameters $(4\lambda + 3, 2\lambda + 1, \lambda)$ for $\lambda \in \mathbb{N}$. These Hadamard 2-designs, as well as the related Hadamard 3-designs, are so called because of their close relationship with Hadamard matrices. Most of our results will be given in terms of Hadamard matrices, but many can be reformulated as results on the existence or non-existence of Hadamard designs with certain properties, or at certain orders.

1.3 Hadamard matrices

In this section we give two alternative descriptions of Hadamard matrices. We observe that a Hadamard matrix may be obtained from a Hadamard 2-design by appending a row and column consisting entirely of $+1$ entries to the incidence matrix, and replacing all 0 entries with -1, see Theorem 3.26 of [4]. Alternatively, we may consider a Hadamard matrix to be a square $\{\pm 1\}$-matrix of order n with determinant $n^{n/2}$.

Definition 1.4. The order of a square matrix is the number of rows, equivalently columns, that it contains.

Hadamard matrices were first investigated by Sylvester in 1867. He observed that on a chessboard, the patterns of colours in any pair of rows agreed either everywhere or nowhere. His investigation of the problem of constructing *anallagmatic pavements*, or arrays in which any two rows had exactly half of their entries in common, led to the discovery of a construction method for what would become known as Sylvester Hadamard matrices of order 2^n. Jacques Hadamard later investigated such matrices as solutions to the problem of finding the maximum determinant of a matrix of order n with entries from the complex unit disk. He was the first to construct such matrices of orders 12

and 20. He also conjectured that there exists a Hadamard matrix of order $4n$ for all $n \in \mathbb{N}$. This problem, almost as simple in its statement as Fermat's Last Theorem or the Goldbach conjecture, remains unsolved.

Definition 1.5. A Hadamard matrix is an $n \times n$ matrix H containing entries from the set $\{\pm 1\}$, with the property that:

$$HH^\top = nI_n \tag{1.3}$$

This implies that all distinct rows are linearly independent, i.e. have an inner product of 0. An example of a 4×4 Hadamard matrix is given below:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{1.4}$$

1.3.1 The Hadamard Conjecture

The discovery of Hadamard matrices and the birth of the Hadamard conjecture are closely related to Hadamard's work on the determinants of complex valued matrices.
Hadamard's Determinant Bound: Let M be a matrix of order n over $\mathbb{C}$, with $|m_{i,j}| \leq 1$, for all entries $m_{i,j}$ of M. Then the determinant M is bounded above:

$$|detM| \leq n^{n/2} \tag{1.5}$$

Equality holds in (1.5) for a real valued matrix M if and only if M is Hadamard.

Lemma 1.6. *Equality in* (1.5) *and* (1.3) *are equivalent.*

Proof. Let H be a Hadamard matrix. One direction of the proof is immediate:

$$HH^\top = nI_n \Rightarrow det\,(H) = n^{n/2}$$

since the determinant of $H^\top$ is necessarily equal to that of H, and for any two square matrices, A and B, we have that $det\,(AB) = det\,(A) \times det\,(B)$. Conversely, we observe that if $det\,(H) = n^{n/2}$ then $HH^\top$ is a symmetric matrix with entries n along the main diagonal and determinant n^n. We show that all other entries are forced to be zero. Let the entry in position (i, j), and by symmetry the entry at (j, i), be k. It is a basic result in linear algebra that adding or subtracting rows of a matrix has no effect on the determinant. Thus we subtract k/n times row i from row j, and k/n times column i from column j. We obtain a matrix with entries 0 at (i, j) and (j, i) and n along the

main diagonal, except at position j, j, which contains $n^2 - k^2/n$. Now for any $k \neq 0$, the determinant of $HH^\top$ will be strictly less then n^n. This argument generalises to any number of off-diagonal entries. So if H is a $\{\pm 1\}$ matrix with determinant $n^{n/2}$, then $HH^\top = nI_n$. □

Hadamard proved that if M, a matrix with real entries, has the Hadamard property, then its order is 1, 2 or a multiple of 4. The Hadamard conjecture states that this condition on the order of M is sufficient. We note that complex Hadamard matrices, with entries in $\{\pm 1, \pm i\}$ can exist at even orders that are not divisible by 4.

The Hadamard Conjecture: There exists a Hadamard matrix of order $4n$ for all $n \in \mathbb{N}$.

This conjecture remains open. A positive solution to this conjecture would obviously solve several open problems in combinatorial design theory. Several infinite families of Hadamard matrices are known, but they are found only at certain orders. Sylvester's construction, for example, proves the existence of Hadamard matrices of order 2^n. Paley's theorem is a much stronger result; it guarantees the existence of a Hadamard matrix for all $m = 2^e (q^n + 1)$ where q is either 0 or prime, and 2^e is suitably chosen so that $m \equiv 0 \bmod 4$. Details of the Paley construction are given in (6.3). There exists a Paley Hadamard matrix of order $4n$ for all $n \leq 25$ with the exceptions of the orders 44, 52, 60, 76, 84, 88, 92 and 100. As the power of computers increases, it becomes possible to search exhaustively for larger and larger Hadamard matrices: existence of Hadamard matrices at all of the above orders was proved by the 1970s. It should be noted however that finding a Hadamard matrix of order n immediately yields a family of Hadamard matrices of orders $2^e n$, by the Sylvester construction. Orders of the form $4p$ where p is prime are the main consideration at present as several construction methods are known to generate a Hadamard matrix of order kn from one of order n, for many values of k. A Hadamard matrix of order 428 was discovered in 2004 [5]. Currently, the smallest order for which no Hadamard matrix is known to exist is 668 [1].

1.4 Group development

In this section we introduce some of the purely algebraic topics of the thesis. In particular we give the definition and some examples of group development for square matrices. We stress in particular the importance of regular actions. We also show that group development of Hadamard matrices is possible only if the order of the Hadamard matrix is square. We mention cocyclic development as a generalisation of group development, but postpone its description until Chapter 3, when we have developed some preliminary concepts.

Definition 1.7. A matrix, M, with entries in a set A, is *group developed* over a group G, if and only if there exists a function $\phi : G \to A$ such that $M = [\phi(gh)]_{g,h \in G}$.

Our notation $[a_{i,j}]_{i,j \in G}$ is intended to mimic the standard notation, in which i and j range over the set $\{1 \dots n\}$, where n is the order of the matrix. We will iterate over the elements of G in some arbitrary order. We observe that the different orderings of the elements of G, with ϕ fixed, will generate matrices permutation equivalent to M. In general we are interested in properties of matrices that are invariant under permutation of columns and rows. As such, we will often abuse the notation and equate M with its equivalence class under permutation of columns and rows, or briefly, its permutation equivalence class. When we wish to discuss a specific matrix, we will specify an ordering of the elements of G which will uniquely define M.

We will show in Chapter 3 that a matrix, M, of order n may be group developed over a group, G, if and only if there there exists a permutation representation of degree n of G as a subgroup of the automorphism group of M. In other words, there exists a regular permutation action of G on the rows and columns of M. Since the multiplication table of any group G is a Latin square, unique up to permutation of rows and columns, every row and column in M will be a permutation of the first row. Hadamard matrices with this property have constant row and column sums and are called *regular* in the literature. This conflicts with our use of the term to describe certain group actions, but we do not wish to introduce an unfamiliar term, so we can do little but bring it to the attention of the reader.

1.5 Group developed Hadamard matrices

Restricting our attention to $\{\pm 1\}$ Hadamard matrices, we can prove some surprisingly strong results. We define an s-regular Hadamard matrix to be one in which every row and every column sum is equal to s. We provide a small example of group development. Consider the cyclic group of order 4, with presentation $< c \mid c^4 = 1 >$, and the set map $\phi : C_4 \to \{\pm 1\}$ given by $\phi(1) = \phi(c) = \phi\left(c^3\right) = 1$ and $\phi\left(c^2\right) = -1$.

	1	c	c^2	c^3
1	1	c	c^2	c^3
c	c	c^2	c^3	1
c^2	c^2	c^3	1	c
c^3	c^3	1	c	c^2

$$\xrightarrow{\phi} \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

The reader is invited to verify that this matrix is in fact Hadamard. We observe that $n = s^2$, where n is the order of the Hadamard matrix in the above example. In fact this is true in general: we give two elementary proofs below. Hence group developed Hadamard matrices occur only at square orders.

Lemma 1.8. *Let H be an s-regular Hadamard matrix of order n. Then $n = s^2$.*

Proof. Let H be an s-regular Hadamard matrix of order n. Let r_i be the i^{th} row of H. Then

$$\sum_{i=1}^{n} (r_1 \cdot r_i) = n$$

by orthogonality. But since r_1 is a constant term in the summation, we have that

$$r_1 \cdot \left(\sum_{i=1}^{n} r_i \right) = r_1 \cdot (s, s, \ldots, s) = s^2$$

since all columns sums are s. Thus, $n = s^2$, as required. It follows that the order of a group developed matrix must be square. □

In an s-regular Hadamard matrix of order n there are precisely $\frac{n}{2} + \frac{s}{2}$ positive entries in each row and column, as well as $\frac{n}{2} - \frac{s}{2}$ negative entries. We give also an alternate proof, due to Warwick de Launey, in which the above constraint on the number of positive entries in any row of the matrix is derived:

Proof. Let H be an s-regular Hadamard matrix of order n as defined above. Recall that by definition, $HH^\top = nI_n$. Let J be the matrix consisting entirely of $+1$ entries. Then:

$$\begin{aligned} JH = JH^\top &= sJ \\ nJ &= JHH^\top \\ &= sJH^\top \\ &= s^2 J \\ n &= s^2 \end{aligned}$$

The restrictions on the order of a regular Hadamard matrix given above follow immediately. □

We observe that either of these arguments are essentially the same as proving that regular Hadamard matrices correspond exactly to square $\left(4t^2, 2t^2 \pm t, t^2 \pm t\right)$-designs. The converse is not true: that a Hadamard matrix has square order does not imply that it may be group developed. The smallest counterexamples occur at order 16. It is conjectured however, that a regular Hadamard matrix occurs at every even square

order. Crnkovic has proved that there exists a regular Hadamard matrix of order $4p^2$, for any prime p [6].

We call a Hadamard matrix *normalised* if its first row and column contain only positive entries. Every Hadamard matrix is Hadamard equivalent to a normalized matrix - see Section 4.2 for the relevant definitions. But obviously a normalised Hadamard matrix is not regular. Thus group development is restricted to square orders, and is not respected by the Hadamard equivalence relation. These shortcomings encourage us to look at generalisations of this technique. Thus we consider cocyclic development, on which no order restrictions are known. Our generalisation will also allow us to determine when a normalised Hadamard matrix is equivalent to a group developed one.

1.6 Cocyclic Hadamard matrices

In the case of group development, we began with the multiplication table of a group, and applied a function $\phi : G \to A$ to it. We observed that this method was quite restrictive with respect to the orders of Hadamard matrices that could be generated. As a generalisation of this technique, we consider functions of the form $\psi : G \times G \to A$, that satisfy the so-called cocycle identity:

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

Cocyclic developed Hadamard matrices are not limited to square orders. As an example, the reader is invited to consider the sample calculation given in Section 4.4.1. We shall see in Chapter 4, that a Hadamard matrix, H, is cocyclic over a group, G, only if there exists a regular action of a special central extension of C_2 by G on the expanded matrix associated with H. We call the matrix cocyclic developed because, analogously to the case of group development, we have that $H \equiv_H [\phi(g,h)]_{g,h\in G}$, where $\phi : G \times G \to \{\pm 1\}$ is a 2-cocycle and $\equiv_H$ is Hadamard equivalence. We will define all of these terms and symbols later in the thesis, but we stress now that a regular action in our definition must be regular on both the rows and the columns of the matrix. The cocycle appearing in the above equation suggests a link with group cohomology, which will be the topic of Chapter 2. The theory of regular actions comprises most of Chapter 3. Thus in Chapter 4 we will be in a position to give a full description of cocyclic development. Now however, we turn our attention again to combinatorial design theory, in particular to the topic of difference sets. Our goal is to highlight an important link between these two seemingly unconnected areas.

1.7 Relative difference sets

Definition 1.9. Let G be a group of order v, and D a subset of G of order k. We say that D is a *difference set* with parameters (v, k, λ) if every non-identity element of G can be expressed as $d_1 d_2^{-1}$ in exactly λ different ways, where $d_1, d_2 \in D$.

Difference sets may be thought of as a class of designs in which the elements of the point set form a group. They respect the conditions given on the parameters of designs given at (1.1). Difference sets are relatively well studied, particularly in Abelian groups. Relative difference sets are a generalisation of difference sets, but have received rather less attention, particularly when they occur in non-Abelian groups.

Definition 1.10. Let E be a group of order mn with a normal subgroup N of order n. A subset R of E of size k such that the multiset of quotients $r_1 r_2^{-1}, r_i \in R, r_1 \neq r_2$ contains each element of $E \backslash N$ exactly λ times and no element of N is called a (m, n, k, λ)-RDS in E with forbidden subgroup N.

When N is central, we say that R is an (n, m, k, λ)-CRDS. We note that groups of order $8t$ containing relative difference sets have been studied extensively by Ito, who refers to them as Hadamard groups [7]. Flannery later proved the equivalence of cocyclic Hadamard matrices and Hadamard groups [8]. The following result of de Launey outlines the relationship between cocyclic Hadamard matrices and central relative $(4t, 2, 4t, 2t)$ difference sets.

Theorem 1.11. *The following statements are equivalent.*

- *There is a cocyclic Hadamard matrix over G.*
- *There is a normal relative $(4t, 2, 4t, 2t)$ difference set in a central extension of $\langle -1 \rangle$ by G, relative to $\langle -1 \rangle$.*
- *There is a divisible $(4t, 2, 4t, 2t)$ design, class regular with respect to $\langle -1 \rangle$, and with a central extension of $\langle -1 \rangle$ by G as a regular group of automorphisms.*

Proof. We provide a proof of the equivalence of the first two items in Section 4.6. For the other parts of the proof, see [9], Theorem 2.4 □

As a result, our classification of cocyclic Hadamard matrices of orders ≤ 28 provides also a complete classification of relative $(4t, 2, 4t, 2t)$ difference sets for $t \leq 7$.

Chapter 2

Group Cohomology

While Sylvester and Hadamard investigated Hadamard matrices from the perspectives of linear algebra and complex analysis respectively, much current research focuses on the relation between Hadamard matrices and the theory of finite groups. In fact this approach has proved to be the most successful at finding Hadamard matrices of large order. The purpose of this chapter is to give a brief introduction to group 2-cohomology as a method of determining the central extensions of an Abelian group C, by a finite group G. There is a general cohomology theory for other dimensions as well as for non-central extensions, but it will not be discussed here. Our goal is to describe a correspondence between the second cohomology group, $H^2(G, N)$ and the central extensions of N by G. This will be made more precise later. All of the material covered here is standard, see Chapter 11 of [10] for example. We say that a group E is an *extension* of a group N, if E contains a normal subgroup isomorphic to N; when no confusion can arise we will refer to this isomorphic copy also as N. The quotient group, E/N, which we will normally denote by G, must be a finite group. In this case we refer to E as an extension of N by G. If $N \leq Z(E)$ we say that E is a *central extension of* N.

2.1 Short exact sequences

Definition 2.1. An *exact sequence* is a sequence of group or module homomorphisms, each of which has the property that the image of the incoming map is the kernel of the outgoing map.

A *short exact sequence* is an exact sequence of the following form:

$$1 \to N \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1 \tag{2.1}$$

where ι and π are group homomorphisms. In the following lemma, we show that a short exact sequence describes a group extension, and that any group extension may be described by a short exact sequence.

Lemma 2.2. *Short exact sequences and group extensions are equivalent.*

Proof. Let E be an extension of a group N by a finite group G, and define $\iota : N \to E$ to be inclusion. Recall that by the definition of an extension, $\iota(N)$ is normal in E. Furthermore, let $\pi : E \to E/N$ be the canonical projection homomorphism with kernel N. Then $\mathtt{Im}(\iota) = \mathtt{Ker}(\pi)$. Thus the following sequence is exact:

$$1 \to N \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$

Conversely: assume that (2.1) is exact. We observe that ι is necessarily a monomorphism, since $\mathtt{Ker}(\iota) = 1$, by exactness at N. Similarly, the kernel of the trivial map $G \to 1$ is $\mathtt{Im}(\pi)$ by exactness, hence π is an epimorphism. Furthermore, $\mathtt{Im}(\iota)$ is a normal subgroup of E, since it is precisely the kernel of the homomorphism π. Thus we have that E contains a normal subgroup, $\iota(N)$, isomorphic to N, and that $E/\iota(N) \cong G$, by the First Isomorphism Theorem. These are precisely the conditions that we require for E to be an extension of N by G. □

We observe that in central extensions, (2.1), the group N is necessarily Abelian since $\iota(N) \leq Z(E)$. In the next section, we will see that 2-cocycles may also be used to describe central extensions.

2.2 Cocycles

Definition 2.3. Let G be a finite group, and C a finitely generated Abelian group. A *2-cocycle* is a map, $\psi : G \times G \to C$, such that:

$$\psi(g,h)\,\psi(gh,k) = \psi(h,k)\,\psi(g,hk) \qquad \forall g,h,k \in G. \tag{2.2}$$

Throughout the remainder of this chapter we will understand *cocycle* to mean 2-cocycle. The following lemma, which will be used in later sections, shows that the 2-cocycles form a group under pointwise multiplication. This result may be generalised to n-cocycles with minor modifications.

Lemma 2.4. *The set of all cocycles $\psi : G \times G \to C$ forms an Abelian group, denoted $Z^2(G,C)$, under the operation*

$$\psi_1\psi_2(x,y) = \psi_1(x,y)\,\psi_2(x,y).$$

Proof. Closure: Let ψ_1 and ψ_2 be cocycles. We show that their product is itself a cocycle.

$$\begin{aligned} \psi_1\psi_2(a,b)\,\psi_1\psi_2(ab,c) &= \psi_1\psi_2(a,bc)\,\psi_1\psi_2(b,c) \\ \Leftrightarrow \psi_1(a,b)\,\psi_2(a,b)\,\psi_1(ab,c)\,\psi_2(ab,c) &= \psi_1(a,bc)\,\psi_2(a,bc)\,\psi_1(b,c)\,\psi_2(b,c) \\ \Leftrightarrow [\psi_1(a,b)\,\psi_1(ab,c)]\,\psi_2(a,b)\,\psi_2(ab,c) &= [\psi_1(a,bc)\,\psi_1(b,c)]\,\psi_2(a,bc)\,\psi_2(b,c) \end{aligned}$$

Both sides are equal since ψ_1 and ψ_2 both satisfy (2.2). Associativity follows from the definition of the multiplication and associativity in C:

$$\begin{aligned} \psi_1\psi_2(x,y)\,\psi_3(x,y) &= \psi_1(x,y)\,\psi_2(x,y)\,\psi_3(x,y) \\ &= \psi_1(x,y)\,\psi_2\psi_3(x,y). \end{aligned}$$

The identity is the cocycle $\psi_e(x,y) = 1, \forall x,y \in G$. Finally we define the inverse for a given cocycle, ψ: $\psi^{-1}(x,y) = (\psi(x,y))^{-1}$ for all $x,y \in G$. We observe that ψ^{-1} satisfies the cocycle identity if ψ does, and that hence every element of $Z^2(G,C)$ has an inverse. Thus $Z^2(G,C)$ satisfies the axioms of a group. □

As previously stated, the primary goal of this chapter is to prove a bijection between the second cohomology group, which is a quotient group of $Z^2(G,C)$, and the set of equivalence classes of central extensions of C by G. Thus, we begin by showing that cocycles may be used to describe extension groups. Then we turn our attention to the problem of extracting a cocycle from a given group extension.

Definition 2.5. We call a cocycle *normalised* if $\psi(1,g) = \psi(g,1) = 1$ for all $g \in G$.

For a given cocycle, $\psi \in Z^2(G,C)$, let

$$E(\psi) = \{(x,a) \ \ | x \in G, a \in C\}.$$

We define the following binary operation on $E(\psi)$, which we show in the next theorem satisfies all the axioms of a group multiplication.

$$(x,a)(y,b) = (xy, ab\,\psi(x,y)) \tag{2.3}$$

Theorem 2.6. *$E(\psi)$, with multiplication defined by* (2.3)*, is a group if and only if ψ is a normalised cocycle.*

Proof.

- $E(\psi)$ inherits closure from G and C, both of which are closed by definition, and ψ maps into C.

- Associativity: (2.3) defines an associative operation if and only if ψ satisfies (2.2). Since C is an Abelian group, we have that:

$$\begin{aligned}
[(x,a)(y,b)](z,c) &= (x,a)[(y,b)(z,c)] \\
\Leftrightarrow (xy, ab\,\psi(x,y))(z,c) &= (x,a)(yz, bc\,\psi(y,z)) \\
\Leftrightarrow (xyz, ab\,\psi(x,y)\,c\,\psi(xy,z)) &= (xyz, abc\,\psi(y,z)\,\psi(x,yz)) \\
\Leftrightarrow (xyz, abc\,\psi(x,y)\,\psi(xy,z)) &= (xyz, abc\,\psi(y,z)\,\psi(x,yz)) \\
\Leftrightarrow \psi(x,y)\,\psi(xy,z) &= \psi(x,yz)\,\psi(y,z)
\end{aligned}$$

  Thus, multiplication in $E(\psi)$ is associative precisely when ψ is a cocycle.

- The identity element is $e = (1_G, 1_C)$. For any (x,a) in E, we show that e is the right identity, the proof that it is also the left identity is identical.

$$(x,a)(1,1) = (x, a\,\psi(x,1)) = (x,a).$$

  Note that we require ψ to be normalised in the above equation.

- For any $(x,a) \in E(\psi)$, the inverse is $\left(x^{-1}, \left[\psi\left(x, x^{-1}\right) a\right]^{-1}\right)$, as may be checked using (2.3) and the definition of the identity given above. □

Now, when both G and C are finite it follows that $|E(\psi)| = |G|\,|C|$. We stress however that the group formed may not be isomorphic to the direct product $G \times C$, as the multiplication depends also on the cocycle, ψ.

We show in the next section that $E(\psi)$ is a group extension of C by G. We call $E(\psi)$ the *canonical extension* of C by G generated by ψ.

2.2.1 The canonical short exact sequence of a cocycle

Let $E(\psi)$ and ψ be as described above. Then $E(\psi)$ contains a subgroup isomorphic to C. Define $\iota_\psi : C \to E(\psi)$ by

$$\iota_\psi(c) = (1_G, c) \tag{2.4}$$

Then ι_ψ is an embedding of C into $E(\psi)$. It should be noted that this embedding is not unique; there will in general be automorphisms of both C and $E(\psi)$ that alter ι_ψ. However in the interest of clarity, we will restrict our attention to the canonical case. Since C is Abelian, $\iota_\psi(C)$ is central in $E(\psi)$: for any $(x,d) \in E(\psi)$, by equation (2.3) we have that

$$(x,d)(1,c) = (x,dc) = (x,cd) = (1,c)(x,d)$$

because ψ is normalised. We now define $\pi_\psi : E(\psi) \to G$ by

$$\pi_\psi(x, a) = x.$$

This is clearly a surjective homomorphism, with kernel $\iota_\psi(C)$. Thus $E(\psi)$ is a central extension of C by G. By Lemma 2.2, we can consider this as a short exact sequence,

$$1 \to C \xrightarrow{\iota_\psi} E(\psi) \xrightarrow{\pi_\psi} G \to 1$$

where ι_ψ and π_ψ are the inclusion and projection maps described above.

2.3 Extracting a cocycle from a short exact sequence

We have already described a process that generates a unique central extension from a given cocycle. We now consider the converse problem of extracting a cocycle from a central extension, as presented in a short exact sequence, (2.1). We stress that the cocycle thus generated will not be unique. All cocycles generated from a given short exact sequence will however be cohomologically equivalent. We will return to the question of equivalence later.

Definition 2.7. A transversal, T, of a group K with respect to a subgroup H is a complete and irredundant set of representatives for the cosets of H in K. We have

$$\bigcup_{t \in T} tH = K$$

where the union is disjoint. That is, any element of K has a unique expression th, for suitable $t \in T$, $h \in H$. Note that in general T is not itself a group, and since there are $|H|$ choices for each element of T, there are many different transversals. When the group K is finite, we have that $|T| = |K : U|$.

Now, let $1 \to C \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be a central extension. We define a map $\tau : G \to E$, such that

$$\pi\tau = id_G. \tag{2.5}$$

That is, for each $g \in G$, we choose $e_g \in E$ such that $\pi(e_g) = g$. This is possible because π is a surjective function. We then define $\tau(g) = e_g$. Note that τ is not unique, as there are $|C|$ choices for each $g \in G$. In fact $\tau(G)$ is a complete and irredundant set of representatives of the elements of the quotient group $E/\iota(C)$, i.e. a transversal of $\iota(C)$ in E. To see this, suppose that $\tau(g)\iota(C) = \tau(h)\iota(C)$. Then for some $c \in C$,

$$\tau(g) = \tau(h)\iota(c) \Leftrightarrow \pi\tau(g) = \pi\tau(h)\pi\iota(c) \Leftrightarrow g = h \cdot 1$$

This implies that τ is injective. Assuming that E is finite, we observe that $|G| = |E/\iota(C)|$ and then irredundancy implies completeness. We call τ a transversal map; it maps elements of G onto a transversal of the cosets of $\iota(C)$ in E. Note that there are $|C|^{|G|}$ possible choices of τ.

Now let $\psi_\tau : G \times G \to C$ be defined as follows:

$$\psi_\tau(g,h) = \iota^{-1}\left(\tau(g)\,\tau(h)\,\tau(gh)^{-1}\right). \tag{2.6}$$

Lemma 2.8. *ψ_τ is a cocycle.*

Proof. We begin by showing that ψ_τ maps into C, that is:

$$\tau(g)\,\tau(h)\,\tau(gh)^{-1} \in \iota(C) \quad \forall g,h \in G. \tag{2.7}$$

This is an easy consequence of (2.5), as we now show. We have that $\pi\tau(x) = x$, for all $x \in G$. It follows that

$$\begin{aligned}\pi\left(\tau(g)\,\tau(h)\,\tau(gh)^{-1}\right) &= \pi\tau(g)\,\pi\tau(h)\,\pi\tau(gh)^{-1}\\ &= gh\,(gh)^{-1}\\ &= 1_G\end{aligned}$$

Thus $\tau(g)\,\tau(h)\,\tau(gh)^{-1} \in Ker(\pi) = \iota(C)$.

We now show that ψ_τ satisfies the cocycle identity. Note that since ι is an embedding, ι^{-1} is a homomorphism, $\iota^{-1} : \iota(C) \to C$.

$$\begin{aligned}\psi_\tau(g,h)\,\psi_\tau(gh,k) &= \iota^{-1}\left(\tau(g)\,\tau(h)\,\tau(gh)^{-1}\right)\iota^{-1}\left(\tau(gh)\,\tau(k)\,\tau(ghk)^{-1}\right)\\ &= \iota^{-1}\left(\tau(g)\,\tau(h)\,\tau(k)\,\tau(ghk)^{-1}\right)\\ &= \iota^{-1}\left(\tau(g)\left[\tau(h)\,\tau(k)\,\tau(hk)^{-1}\right]\tau(hk)\,\tau(ghk)^{-1}\right)\\ &= \iota^{-1}\left(\tau(h)\,\tau(k)\,\tau(hk)^{-1}\right)\iota^{-1}\left(\tau(g)\,\tau(hk)\,\tau(ghk)^{-1}\right)\\ &= \psi_\tau(h,k)\,\psi_\tau(g,hk)\end{aligned}$$

Proceeding from the third to the fourth line, we use that $\tau(h)\,\tau(k)\,\tau(hk)^{-1}$ is central in E. Thus $\psi_\tau : G \times G \to C$ is a cocycle. □

The above construction generates a cocycle from a central extension. As we have noted, this cocycle is not canonical. But as we also stated previously, all cocycles generated from a given central extension are equivalent in a cohomologous sense. To explain this concept, we introduce coboundaries in the next section.

2.4 Coboundaries

Throughout this section we let G be a finite group, and let C be an Abelian group.

Definition 2.9. $\texttt{Fun}(G, C)$ is the set of all mappings $\varphi : G \to C$.
$\texttt{Fun}(G, C)$ is in fact a monoid under pointwise composition of maps. $\texttt{Hom}(G, C)$, the set of homomorphisms $G \to C$ is of course a submonoid of $\texttt{Fun}(G, C)$. Now for each $\varphi \in \texttt{Fun}(G, C)$. We define the *coboundary* $\partial\varphi$, by

$$\partial\varphi(x, y) = \varphi(x)\,\varphi(y)\,\varphi(xy)^{-1}. \tag{2.8}$$

Lemma 2.10. *Every coboundary is a cocycle.*

Proof. We simply show that a coboundary satisfies the cocycle equation, (2.2).

$$\begin{aligned}
\partial\varphi(x, y)\,\partial\varphi(xy, z) &= \varphi(x)\,\varphi(y)\,\varphi(xy)^{-1}\,\varphi(xy)\,\varphi(z)\,\varphi(xyz)^{-1} \\
&= \varphi(x)\,\varphi(y)\,\varphi(z)\,\varphi(xyz)^{-1} \\
&= \varphi(x)\,\varphi(y)\,\varphi(z)\,\varphi(xyz)^{-1}\,\varphi(yz)\,\varphi(yz)^{-1} \\
&= \varphi(x)\,\varphi(yz)\,\varphi(xyz)^{-1}\,\varphi(y)\,\varphi(z)\,\varphi(yz)^{-1} \\
&= \partial\varphi(xy, z)\,\partial\varphi(y, z).
\end{aligned}$$

□

Recall that we have a particular interest in normalised cocycles, as they may be used to construct extension groups. We observe that a coboundary, $\partial\varphi$, is normalised if and only if $\varphi(1) = 1$. Most of these our results in this section can be restated for n-cohomology with only minor adjustments; we restrict our attention to the case of 2-cohomology, however.

Lemma 2.11. *The set of 2-coboundaries, $B^2(G, C)$ is closed under pointwise composition.*

Proof.

$$\begin{aligned}
\partial\varphi_1\partial\varphi_2(x, y) &= \partial\varphi_1(x, y)\,\partial\varphi_2(x, y) \\
&= \varphi_1(x)\,\varphi_1(y)\,\varphi_1(xy)^{-1}\,\varphi_2(x)\,\varphi_2(y)\,\varphi_2(xy)^{-1} \\
&= \varphi_1(x)\,\varphi_2(x)\,\varphi_1(y)\,\varphi_2(y)\,\varphi_1(xy)^{-1}\,\varphi_2(xy)^{-1}
\end{aligned}$$

This satisfies (2.8), as we do not place any restrictions on the map $\varphi : G \to C$. □

The preceding two lemmas suffice to show that $B^2(G, C)$, the set of 2-coboundaries, is a subgroup of $Z^2(G, C)$, the group of 2-cocycles under pointwise multiplication. In the remainder of this section we prove $B^2(G, C)$ is a quotient group of $\texttt{Fun}(G, C)$. This result gives some insight into the structure of $B^2(G, C)$.

Lemma 2.12. *∂: $\mathtt{Fun}(G,C) \to B^2(G,C)$, is an epimorphism with kernel $\mathtt{Hom}(G,C)$.*

Proof. We show that ∂: $\mathtt{Fun}(G,C) \to B^2(G,C)$ is a homomorphism. Let φ_1 and $\varphi_2 \in \mathtt{Hom}(G,C)$.

$$\begin{aligned}
\partial\varphi_1(x,y)\,\partial\varphi_2(x,y) &= \varphi_1(x)\,\varphi_1(y)\,\varphi_1(xy)^{-1}\,\varphi_2(x)\,\varphi_2(y)\,\varphi_2(xy)^{-1} \\
&= \varphi_1(x)\,\varphi_2(x)\,\varphi_1(y)\,\varphi_2(y)\,\varphi_1(xy)^{-1}\,\varphi_2(xy)^{-1} \\
&= \varphi_1\varphi_2(x)\,\varphi_1\varphi_2(y)\,\varphi_1\varphi_2(xy)^{-1} \\
&= \partial\varphi_1\varphi_2(x,y)
\end{aligned}$$

If $\varphi \in \mathtt{Hom}(G,C)$, then by definition, $\varphi(x)\,\varphi(y) = \varphi(xy)$. It follows immediately that $\partial\varphi = 1_{B^2(G,C)}$. Thus $\mathtt{Ker}(\partial) \subseteq \mathtt{Hom}(G,C)$. Conversely, assume that $\varphi \in \mathtt{Ker}(\partial)$. Then $\varphi(x)\,\varphi(y)\,\varphi(xy)^{-1} = 1 \forall x, y \in G$. Hence φ is a homomorphism. □

Now, having defined both coboundaries and cocycles, we are in a position to define the second cohomology group, $H^2(G,C)$.

2.5 The Second Cohomology Group

The second cohomology group of G, with trivial coefficients in C, is defined to be

$$H^2(G,C) = Z^2(G,C)/B^2(G,C) \tag{2.9}$$

where, as defined previously, $Z^2(G,C)$ is the group of all cocycles, $G \times G \to C$, and $B^2(G,C)$ is the subgroup of all coboundaries. The elements of $H^2(G,C)$ are *cohomology classes* of cocycles, $[f]$, where $f \in Z^2(G,C)$. More precisely, each element of $H^2(G,C)$ is a coset of $B^2(G,C)$ in $Z^2(G,C)$. It follows that the elements of a single cohomology class differ from one another only by coboundaries; we call such elements *cohomologous*. In fact, this is the equivalence operation uniting all cocycles generated from a single central extension, as described earlier. Before expanding on this theme, we provide a lemma which describes the structure of $H^2(G,C)$.

Lemma 2.13. *If C is finite, then the exponent of $H^2(G,C)$ divides the exponent of C.*

Proof. Let $\psi \in Z^2(G,C)$, and let n be the exponent of C. Then $\psi(x,y) \in C$ for all $x, y \in G$. So $\psi(x,y)^n = 1$ for all $x, y \in G$. This result holds for all cocycles in Z^2. Hence the exponent of $Z^2(G,C)$ divides n. As a factor group of $Z^2(G,C)$, the exponent of $H^2(G,C)$ must also divide n. □

When working with Hadamard matrices, we often make use of groups of the form $H^2(G, C_2)$. By the above lemma, these are elementary Abelian 2-groups, which are in some sense easy to work with.

2.6 Equivalence of short exact sequences

We begin by introducing a standard lemma from homological algebra, the five lemma. Its proof is given by means of diagram chasing. We have already defined exact sequences. We say that a square in a diagram commutes if any two paths with identical origins and endpoints are equal as composite maps.

Lemma 2.14. *Consider the following diagram of group homomorphisms, in which both rows are exact, and all squares are commutative. If γ_2 is a monomorphism and both γ_{-1}*

$$\begin{array}{ccccccccc} V_{-2} & \overset{\alpha_{-2}}{\rightarrow} & V_{-1} & \overset{\alpha_{-1}}{\rightarrow} & V_0 & \overset{\alpha_0}{\rightarrow} & V_1 & \overset{\alpha_1}{\rightarrow} & V_2 \\ \downarrow \gamma_{-2} & & \downarrow \gamma_{-1} & & \downarrow \gamma_0 & & \downarrow \gamma_1 & & \downarrow \gamma_2 \\ W_{-2} & \overset{\beta_{-2}}{\rightarrow} & W_{-1} & \overset{\beta_{-1}}{\rightarrow} & W_0 & \overset{\beta_0}{\rightarrow} & W_1 & \overset{\beta_1}{\rightarrow} & W_2 \end{array}$$

and γ_1 are epimorphisms, then γ_0 is an epimorphism. If γ_{-2} is an epimorphism, and both γ_{-1} and γ_1 are monomorphisms, then γ_0 is a monomorphism.

Proof. The proof of the first part is given on page 46 of [11]. The proof of the second part follows.

Let $v_0 \in V_0$ such that $\gamma_0(v_0) = 1$. By commutativity, $\gamma_1\alpha_0(v_0) = \beta_0\gamma_0(v_0) = 1$. Since γ_1 is a monomorphism, we have that $\alpha_0(v_0) = 1$. By exactness, there exists $v_{-1} \in V_{-1}$ such that $\alpha_{-1}(v_{-1}) = v_0$. Again by commutativity, we have that $\beta_{-1}\gamma_{-1}(v_{-1}) = \gamma_0\alpha_{-1}(v_0) = 1$. And again by exactness, we have that there exists $w_{-2} \in W_{-2}$ such that $\beta_{-2}(w_{-2}) = \gamma_{-1}(v_{-1})$. Now we use the the assumption that γ_{-2} is an epimorphism; hence there exists $v_{-2} \in V_{-2}$ such that $\beta_{-2}\gamma_{-2}(v_{-2}) = \gamma_{-1}\alpha_{-2}(v_{-2}) = \beta_{-2}(w_{-2})$. But γ_{-1} is a monomorphism, so $\alpha_{-2}(v_{-2}) = v_{-1}$. Finally by exactness, we have that $\alpha_{-1}(v_{-1}) = v_0 = 1$. Hence, γ_0 is an monomorphism. □

We make use of this lemma to partition the set of central extensions of C by G into equivalence classes. Consider the following diagram, which illustrates a series of homomorphisms between two short exact sequences. We define γ_{-1} and γ_1 to be identity maps.

Definition 2.15. Two short exact sequences are equivalent if and only if the above diagram commutes. We observe that this is a true equivalence relation on the set of central extensions of C by G.

$$\begin{array}{ccccccccc} 1 & \rightarrow & C & \stackrel{\iota_1}{\rightarrow} & E_1 & \stackrel{\pi_1}{\rightarrow} & G & \rightarrow & 1 \\ & & \downarrow \gamma_{-1} & & \downarrow \gamma_0 & & \downarrow \gamma_1 & & \\ 1 & \rightarrow & C & \stackrel{\iota_2}{\rightarrow} & E_2 & \stackrel{\pi_2}{\rightarrow} & G & \rightarrow & 1 \end{array}$$

Lemma 2.16. *If the above diagram commutes, then γ_0 is an isomorphism.*

Proof. Assume the diagram commutes. We make use of the five lemma, 2.14. We begin by observing that any mapping from the trivial group, 1, to itself, is necessarily both an epimorphism and a monomorphism. It is then easy to see that γ_0 satisfies all the requirements of the five lemma to be both an epimorphism and a monomorphism. Thus it is in fact an isomorphism, as required. □

Thus, if two central extensions or short exact sequences are equivalent, then the extension groups are isomorphic. However if the extension groups are isomorphic the central extensions are not necessarily equivalent. The next section describes a correspondence between the elements of $H^2(G, C)$ and the central extensions of G by C. Assuming this, a simple counter example is given by $H^2\left(C_2^2, C_2\right)$. This cohomology group has order 8, yet there are only five isomorphism classes of groups of order 8.

2.7 Equivalence of short exact sequences and cohomological equivalence

In Section 2.5 we established an equivalence relation on the set of cocycles, $Z^2(G, C)$, and in Section 2.6 we established one on the set of central extensions of C by G. Recall that we also demonstrated methods of extracting cocycles from central extensions, and of generating central extensions from cocycles. In this section we establish a one-to-one correspondence between cohomology classes of cocycles and equivalence classes of central extensions.

Theorem 2.17. *The set of equivalence classes of central extensions of C by G is in one-to-one correspondence with $H^2(G, C)$.*

Proof. Let $\mathcal{S}$ denote the set of equivalence classes of central extensions of C by G. We define a map, $\alpha : H^2(G, C) \rightarrow \mathcal{S}$ by $\alpha([\psi]) = \left[1 \rightarrow C \stackrel{\iota_0}{\rightarrow} E(\psi) \stackrel{\pi_0}{\rightarrow} G \rightarrow 1\right]$, where $\iota_0(c) = (1, c)$ and $\pi_0(x, a) = x$. Recall that any cocycle cohomologous to ψ has the form $\psi\partial\varphi$, where $\partial\varphi \in B^2(G, C)$. We show that $E(\psi)$ and $E(\psi\partial\varphi)$ are equivalent in the sense of Definition 2.15, and hence that the map α is well defined. We define the map

$\gamma_0 : E(\psi) \to E(\psi\partial\varphi)$ given by $\gamma(\tau(g)\iota(c)) = (g,c)$. Then:

$$\begin{aligned}
\gamma_0(\tau(g)\iota(c)\tau(h)\iota(d)) &= \gamma_0(\tau(g)\tau(h))\iota(cd) \\
&= \gamma_0(\tau(gh)\iota(f_\tau(g,h))\iota(cd)) \\
&= (gh, f_\tau(g,h)\,cd) \\
&= (g,c)(h,d) \\
&= \gamma_0(\tau(g)\iota(c))\gamma_0(\tau(h)\iota(d)).
\end{aligned}$$

Thus γ_0 is a group homomorphism. Now, to show that the extensions are equivalent, we show that the following diagram commutes, where γ_{-1} and γ_1 are again identity maps: Observe that $\gamma_0\iota(c) = (1,c) = \iota'(c) = \iota'\gamma_{-1}(c)$ for all $c \in C$. Similarly, $\pi(\tau(g)\iota(c)) =$

$$\begin{array}{ccccccccc}
1 & \to & C & \xrightarrow{\iota} & E(\psi) & \xrightarrow{\pi} & G & \to & 1 \\
 & & \downarrow \gamma_{-1} & & \downarrow \gamma_0 & & \downarrow \gamma_1 & & \\
1 & \to & C & \xrightarrow{\iota'} & E(\psi\partial\varphi) & \xrightarrow{\pi'} & G & \to & 1
\end{array}$$

$\gamma_1\pi(\tau(g)\iota(c)) = g = \pi'(g,c) = \gamma_0\pi'(\tau(g),\iota(c))$. Hence the above diagram commutes, and the short exact sequences are equivalent.

We now prove the converse, that cocycles generated from a given central short exact sequence are cohomologous. We define a map, $\beta : \mathcal{S} \to [\psi_\tau]$, where τ is a transversal for $\iota(C)$ in E. We show that the map β is well defined in the sense that for a given central extension, any choice of transversal generates a cohomologous cocycle.

Let $E(\psi)$ be a central extension of C by G. Let τ be a transversal of $\iota(C)$ in E. We show that a cocycle, ψ' formed from some other transversal, τ' is cohomologous. Firstly, we note that $\tau'(x) = \tau(x)\phi(x)$, for some $\phi : G \to \iota(C)$. Note that by the definition of a short exact sequence, $\pi\phi = 1_G$.

$$\begin{aligned}
\psi'(x,y) &= \iota^{-1}\left(\tau(x)\phi(x)\tau(y)\phi(y)\tau(xy)^{-1}\phi(xy)^{-1}\right) \\
&= \iota^{-1}\left(\tau(x)\tau(y)\tau(xy)^{-1}\phi(x)\phi(y)\phi(xy)^{-1}\right) \\
&= \iota^{-1}\left(\tau(x)\tau(y)\tau(xy)^{-1}\right)\iota^{-1}\left(\phi(x)\phi(y)\phi(xy)^{-1}\right) \\
&= \psi(x,y)\,\partial\phi(x,y)
\end{aligned}$$

Now we come to a subtle point. Let $E(\psi)$ be the central extensions generated by ψ. We show that a cocycle generated from $E(\psi)$ lies in the same cohomology class as ψ. We have shown that all cocycles generated from a central short exact sequence are cohomologous, thus it suffices to prove that any single cocycle generated from $E(\psi)$ is cohomologous to ψ. In particular, we show that we can generate ψ from $E(\psi)$. We define the transversal map $\tau' : G \to E(\psi)$ by $\tau'(g) = (g,1)$. Let ψ' be the cocycle

generated from τ'. We show that it is cohomologous to ψ. Now by (2.6),

$$\begin{aligned}
\psi'(g,h) &= \iota^{-1}\left((g,1)(h,1)(gh,1)^{-1}\right) \\
&= \iota^{-1}\left(gh, \psi(g,h)\left(h^{-1}g^{-1}, \psi\left(gh, h^{-1}g^{-1}\right)\right)\right) \\
&= \iota^{-1}(1, \psi(g,h)) \\
&= \psi(g,h)
\end{aligned}$$

Thus we have that $\psi' = \psi$. We have established already that changing transversal does not affect the cohomology class, hence $[\psi] = [\psi']$ for any choice of transversal map, $G \to E(\psi)$.

Finally, we observe that $\alpha\beta = \beta\alpha = Id$. Consider $s \in \mathcal{S}$. By our definition of β, any two cocycles derived from $\mathcal{S}$ are cohomologous. But we proved in the first section of the proof that cohomologous cocycles generate equivalent extensions. Hence $\beta\alpha(s) = s$. In the other direction, consider $h \in H^2(G,C)$. Then $\alpha\beta(h) = h$. This establishes a bijection between equivalence classes of central extensions and the elements of $H^2(G,C)$ as required.

We point out that this theorem provides an answer to the central extension problem in finite group theory. Given an Abelian group, C and a finite group G, we can compute all extensions of C by G by computing the second cohomology group, $H^2(G,C)$, choosing a representative cocycle from each cohomology class, and generating the corresponding central extensions. This theorem will also be central to our classification of cocyclic Hadamard matrices.

Chapter 3

Group actions on square arrays

Like the previous chapter, this one is purely algebraic. We discuss the theory of group actions on square arrays. Throughout this chapter, G will denote a finite group of order n. Additionally, M will be an $n \times n$ array with entries from a finite Abelian group A. We denote by Λ the set of all such M. We define $\phi : G \to A$ to be an arbitrary function. Later in the chapter we will encounter cocycles, $\psi : G \times G \to A$. These will obey the cocycle identity, (2.2). The results in this chapter will be directly applicable to many types of combinatorial design. In the following chapter we will relate them to Hadamard matrices. This will give us the necessary machinery to classify all cocyclic Hadamard matrices of order ≤ 28 in terms of the groups over which they are cocyclic developed. Many of the concepts introduced in this chapter were known to Warwick de Launey by the early 1990's, though to the knowledge of the author, they have not as of yet appeared in print. They will be covered comprehensively in *Algebraic Design Theory*, a monograph by de Launey and Flannery which is currently nearing completion.

3.1 The automorphism group of a square array

It is standard practice to define Hadamard equivalence in terms of row and column permutations and negations. We generalise this concept to matrices with entries from an Abelian group A.

Definition 3.1. Let M be a matrix with entries in A. We say that M' is A-equivalent to M if and only if M' may be obtained from M by a finite sequence of row and column permutations, and multiplication of rows or columns by $a \in A$.

We will define and discuss the the action of a certain matrix group on M. The point stabiliser of a given matrix under this action will then be its automorphism group. We begin with a brief discussion of permutation matrices.

3.1.1 Permutation matrices

Definition 3.2. A square matrix with entries from $\{0, 1\}$ and with exactly one nonzero entry in each row and column is called a permutation matrix.

We introduce Kronecker δ notation, which we shall use extensively in the remainder of this chapter. It was originally a shorthand for the identity matrix,

$$\left[\delta^i_j\right]_{1\leq i,j\leq n} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{3.1}$$

There is a natural way to apply this to elements of the symmetric group. For $\alpha \in \mathtt{Sym}(n)$, we form the matrix $P_\alpha = \left[\delta^i_{\alpha(j)}\right]_{1\leq i,j\leq n}$.

Lemma 3.3. *The map $\alpha \mapsto P_\alpha$ defines an isomorphism of $\mathtt{Sym}(n)$ onto $\mathtt{Perm}(n)$.*

Proof. First of all we note that $\left[\delta^i_{\alpha(j)}\right]_{i,j} = I_n$ only if $i = \alpha(i) \quad \forall 1 \leq i \leq n$. Thus the map is injective. We now prove that it is a homomorphism.

$$\begin{aligned} P_\alpha P_\beta &= \left[\delta^i_{\alpha(k)}\right]_{i,k} \left[\delta^k_{\beta(j)}\right]_{k,j} \\ &= \left[\sum_k \delta^i_{\alpha(k)} \delta^k_{\beta(j)}\right]_{i,j} \\ &= \left[\delta^{\alpha^{-1}(k)}_{\beta(j)}\right] \\ &= \left[\delta^i_{\alpha\beta(j)}\right] \\ &= P_{\alpha\beta} \end{aligned}$$

Finally, both $\mathtt{Sym}(n)$ and $\mathtt{Perm}(n)$ have precisely the same size, $n!$. Hence $\alpha \mapsto P_\alpha$ is an isomorphism. □

We observe that the group $\mathtt{Perm}(n)$ acts on a square matrix, M, of order n, by left or right multiplication. In fact the orbit of M under the action $PMQ^\top$ where $P, Q \in \mathtt{Perm}(n)$ is the set of all matrices permutation equivalent to M. Our definition of A-equivalence extends beyond this however. We may also multiply a row or column by some $a \in A$. Thus, we consider monomial matrices.

3.1.2 Monomial matrices

Monomial matrices are a generalisation of permutation matrices. As with permutation matrices, monomial matrices contain one nonzero entry in each row and column, but this entry is drawn from an Abelian group, A. We denote by $\mathtt{Diag}(n, A)$ the set of diagonal

matrices of order n with entries from A along the main diagonal and zero elsewhere. $\texttt{Diag}(n, A)$ is a group, isomorphic to the direct product of n copies of A. The group of monomial matrices with entries in A is defined as a semidirect product of $\texttt{Diag}(n, A)$ and $\texttt{Perm}(n)$.

$$\texttt{Mon}\left(n, A\right) = \left\{Pa | a \in \texttt{Diag}\left(n, A\right), P \in \texttt{Perm}\left(n\right)\right\} = \texttt{Diag}\left(n, A\right) \rtimes \texttt{Perm}\left(n\right)$$

Note that $\texttt{Perm}(n)$ is not normal for $n \neq 1$, and as such $\texttt{Mon}(n, A)$ is not the direct product of these two groups. The order of this group is $n! \left|A\right|^n$.

Lemma 3.4. *Let* $(P, Q) \in \texttt{Mon}(n, A) \times \texttt{Mon}(n, A)$, $M \in \Lambda$. *Then* $(P, Q) \bullet M = PMQ^\top$ *is a group action of* $\texttt{Mon}(n, A) \times \texttt{Mon}(n, A)$ *on* Λ.

Proof. We begin by observing that Λ is closed under the action of $\texttt{Mon}(n, A) \times \texttt{Mon}(n, A)$. We observe that the identity in $\texttt{Mon}(n, A) \times \texttt{Mon}(n, A)$ is (I_n, I_n) and that for any $M \in \Lambda$,

$$(I_n, I_n) \bullet M = I_n M I_n^\top = I_n M I_n = M.$$

Secondly, we let $\left(P, Q\right), \left(R, A\right) \in \texttt{Mon}(n, A) \times \mathrm{Mon}(n, A)$, then

$$\begin{aligned}
\left(\left(P, Q\right)\left(R, S\right)\right) \bullet M &= (PR, QS) \bullet M \\
&= PRM\left(QS\right)^\top \\
&= PRMS^\top Q^\top \\
&= (P, Q) \bullet RMS^\top \\
&= (P, Q) \bullet \left((R, S) \bullet M\right)
\end{aligned}$$

Thus $\texttt{Mon}(n, A) \times \mathrm{Mon}(n, A)$ acts on Λ. □

Definition 3.5. Let M be a square matrix of order n, with entries in an abelian group A. The A-orbit of M is $\left\{PMQ^\top | P, Q \in \texttt{Mon}\left(n, A\right)\right\}$.

These orbits are equivalence classes, thus they partition the set of square A-matrices of order n into disjoint classes. We refer to two matrices as being A-equivalent if and only if they fall into the same A-orbit. The operation is clearly reflexive, symmetric and transitive. Unfortunately, finding suitable representatives for equivalence classes and testing for equivalence are computationally expensive problems in general.

3.1.3 Definition of the automorphism group

Definition 3.6. The automorphism group of M is defined to be its pointwise stabiliser under the action of $\mathtt{Mon}(n, A) \times \mathrm{Mon}(n, A)$. That is, $(P, Q) \in \mathtt{Aut}(M)$ if and only if

$$(P, Q) \bullet M = PMQ^{\top} = M$$

As the stabiliser of a point, this group is well defined. As previously stated, regular subgroups of these automorphism groups provide us with information about the group development properties of the square array.

An important subgroup of $\mathtt{Aut}(M)$ is $\mathtt{PermAut}(M) = \mathtt{Aut}(M) \cap \mathtt{Perm}(n)$.

Lemma 3.7. *Let M be an A-matrix in which all rows and columns are pairwise linearly independant. Then $\mathtt{Aut}(M)$ is isomorphic to a subgroup of $\mathtt{Mon}(n, A)$.*

Proof. For any element (P, Q) of $\mathtt{Aut}(M)$ we have that $PM = MQ$. By pairwise linear independance of rows and columns, Q is uniquely determined by P and vice versa. Thus $\mathtt{Aut}(M) \cong \{P | P \in (P, Q)\}$. Hence $\mathtt{Aut}(M)$ is isomorphic to a subgroup of $\mathtt{Mon}(n, A)$. □

Similarly, $\mathtt{PermAut}(M)$ is isomorphic to a subgroup of $\mathtt{Perm}(n, A)$, in the case where M is invertible. We observe that this condition that M be invertible is in fact necessary. We consider for example the following matrix, with entries in C_3:

$$M_3 = \begin{pmatrix} 1 & 1 & 1 \\ c & c & c \\ c^2 & c^2 & c^2 \end{pmatrix}$$

We content ourselves with calculation of $\mathtt{PermAut}(M_3)$. There is clearly no non-trivial permutation on the rows, while all of $\mathtt{Perm}(3)$ acts on the columns. Thus, for an arbitrary $(0, A)$-matrix, Lemma 3.7 does not hold. Considering both M_3 and its transpose, we see that in general, a homomorphism from the left acting part of the automorphism group to the right acting part need not be either a monomorphism or an epimorphism.

3.1.4 The regular action of a group on a finite set

We introduce some basic definitions and results about regular actions in this section.

Definition 3.8. The action of a group, G on a set, X is regular if it is both transitive and semiregular. Transitivity requires that for all x, y in X, there is some $g \in G$ such that $gx = y$. Semiregularity requires that the stabilisers of all points be trivial.
Obviously, if G acts regularly on X then $|G| = |X|$. In the context of square arrays,

we call a subgroup of $\texttt{Aut}(M)$ regular if and only if its action on **both the rows and columns** of M is regular. We stress that this means that the action of a subgroup, R of $\texttt{Aut}(M)$ on M is regular if and only if the left components of R act regularly on the rows of M **and** the right components of R act regularly on the rows of M.

Recall that Kronecker δ notation may be used to uniquely assign a permutation matrix of order n to a permutation. We now abuse notation slightly and iterate over the elements of a finite group, G. The concept is still the same however, the matrix $[\delta^a_b]_{a,b\in G}$ contains a 1 if $a = b$ and a 0 otherwise. Now we define the left-regular and right-regular permutation representations of a finite group G.

$$S_x = [\delta^a_{xb}]_{a,b\in G} \qquad T_x = [\delta^{ax}_b]_{a,b\in G} \tag{3.2}$$

Such matrices will contain a non-zero entry in position (a, b) precisely when $a = xb$ in the first case, and when $ax = b$ in the second. The existence and uniqueness of this element in each row and column follows directly from the group laws.

Lemma 3.9. *There is a unique faithful regular action of a finite group G, on a set, X, up to permutation equivalence.*

Proof. Recall that by Cayley's theorem, any finite group G may be embedded into $\texttt{Sym}(\{G\})$, the symmetric group on the elements of G. Furthermore, by the group laws the action of G, considered as a permutation group on its own elements is regular. Now suppose that G acts regularly on another set, Ω. We choose an arbitrary $\omega_0 \in \Omega$. Now by regularity of the action, there is a unique element of G such that $g\omega_0 = \omega$ for all $\omega \in \Omega$. So we can define a bijection, $f : \Omega \to \{G\}$ given by $f(g\omega) = g$. We then have $f(h\omega) = hf(\omega)$ for any $h \in G$. Hence up to permutation equivalence, the faithful regular action of G is unique.

Lemma 3.10. *1. $S_xS_y = S_{xy}$ and $T_xT_y = T_{xy}$ for all $x, y \in G$.*

2. Let X_n denote the set of $n \times 1$ column vectors $\alpha_y = \left[\delta^x_y\right]_{x\in G}$. Then $S_x\alpha_y = \alpha_{xy}$ and $T_x\alpha_y = \alpha_{yx^{-1}}$.

3. The assignments $x \mapsto S_x$ and $x \mapsto T_x$ define faithful regular permutation representations of G in $\texttt{Sym}(X_n)$.

Proof. 1. We have

$$S_xS_y = \left[\sum_c \delta^a_{xc}\delta^c_{yb}\right]_{a,b\in G} = \left[\delta^a_{xyb}\right]_{a,b\in G} = S_{xy}$$

The proof for T_x is similar.

2. Post-multiplying a matrix M by α_y picks out the column of M labelled by y. The $+1$ entry in column y occurs in row xy, that is the column of S_x labelled by y is α_{xy}. The argument for T_x is similar.

3. Firstly, $x \mapsto S_x$ defines a homomorphism $G \mapsto \mathtt{Sym}(X_n)$, by the first two parts of the lemma. The image of this homomorphism acts regularly. For, it is transitive: given $x, y \in G$, by part 2 we have that $S_{xy^{-1}}\alpha_y = \alpha_x$. Also, it is semiregular since $S_x\alpha_y = \alpha_y$ if and only if $x = 1$, by part 2. Again, the proof for T_x is similar.

3.2 Group development

In this section we give a practical and efficient method of determining the group development properties of a square matrix based on regular subgroups of its automorphism group.

Let M, as usual, be a square matrix of order n with entries in a set A. Let G be a group of order n. The elements of G may be used as an indexing set for the rows and columns of the matrix. Then we can trivially develop M over G with a function $\mu : G \times G \to A$, defined by the entries of M. In this section we provide necessary and sufficient conditions for the existence of a single variable map, $\phi : G \to A$, over which a square matrix M may be developed. This is the definition that we use of group development:

Definition 3.11. Let M be an $n \times n$ matrix, with entries in some set A. M is group developed over G if there exists a function $\phi : G \to A$ and a matrix, M', permutation equivalent to M such that $M' = [\phi(gh)]_{g,h \in G}$

Note that group development is a property of permutation equivalence classes of matrices. We will see later that cocyclic development, which is a generalisation of group development, is a property of A-equivalence classes of matrices.

Lemma 3.12. *M is developed over G if and only if $T_x M S_x = M$ for all $x \in G$.*

Proof. We write $M = [\mu(g,h)]_{g,h\in G}$. Then

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

We set $\phi(x) = \mu(x,1)$. It then follows that

$$\begin{aligned} T_x M S_x^\top &= M, \forall x \in G \iff \mu\left(gx, x^{-1}h\right) = \mu(g,h)\, \forall x,g,h \in G \\ &= \mu(g,h) = \mu\left(gh, h^{-1}h\right) = \phi(gh)\, \forall g,h \in G \end{aligned}$$

as required. □

The final lemma in this section puts this result in context, and provides us with a simple computational test that determines whether or not a given matrix is group developed.

Lemma 3.13. *An $n \times n$ matrix, M, with entries in a set A is developed over a group G, of order n, if and only if there exists a regular subgroup of* `PermAut`(M) *isomorphic to G.*

Proof. If M is G-developed, then by Lemma 3.12, $(T_x, S_x) \in \texttt{PermAut}(M)$ for all x. Then the map $\kappa : x \mapsto (T_x, S_x)$ is an isomorphism from G into $\texttt{PermAut}(M)$. We observe that $\kappa(G)$ is a regular subgroup of $\texttt{PermAut}(M)$, as its induced actions on the row set and column set of M are both regular by Lemma 3.10. This completes one direction of the proof. In the other direction, we assume that $\texttt{PermAut}(M)$ has a regular subgroup isomorphic to G. We denote the isomorphism $\kappa(x) = (P_x, Q_x)$. Now by definition the action of G on the row set of M is regular. By Lemma 3.9, there is, up to permutation isomorphism, only a single faithful regular action of G on this set. Thus there exists some permutation matrix U such that $UP_xU^\top = T_x \;\; \forall x \in G$. Similarly there exists a permutation matrix V such that $VQ_xV^\top = S_x \;\; \forall x \in G$. Then by Lemma 3.12, the matrix $UMV^\top$ is group developed over G. The ordering of the rows and columns of M being irrelevant, we conclude that M itself is also group developed over G. □

3.3 The expanded matrix

In our definition of group development, we restricted our attention to $\texttt{PermAut}(M)$, the group of permutation automorphisms of M. In the next section we describe a method for finding special transitive subgroups of the full automorphism group, $\texttt{Aut}(M)$, over which M may be cocyclic developed. First, we must describe the expanded matrix of M: that is the purpose of this section. In particular we prove that $\texttt{Aut}(M)$ embeds into $\texttt{PermAut}(E_M)$. We then use this fact, the method already developed and the cohomology of Chapter 2 to describe the cocyclic development of a square matrix. We will see that the expanded matrix is group developed over a group extension of G, and thus the development function will have the form of a 2-cocycle over G.

Unlike group development, the cocyclic development properties of M are inextricably linked to the set from which M draws its entries. In fact, we require that A be an Abelian group, written multiplicatively with identity 1, in the remainder of this chapter, as we only made a study of central extensions in Chapter 2. When appropriate, we consider $(0, A)$-matrices, in which all non-zero entries are drawn from A. With appropriate modifications, this theory may be applied to non-central extensions and even to extensions of non-Abelian groups. Given an $n \times n$ $(0, A)$-matrix M, we define the expanded matrix of M, E_M, to be the following $|A|\, n \times |A|\, n$ Kronecker product.

$$E_M = \begin{pmatrix} a_1Ma_1 & a_1Ma_2 & \dots & a_1Ma_n \\ a_2Ma_1 & a_2Ma_2 & \dots & a_2Ms_n \\ \vdots & \vdots & \ddots & \vdots \\ a_nMa_1 & a_nMa_2 & \dots & a_nMa_n \end{pmatrix} = [a_ia_j] \otimes M$$

We will assume, without loss of generality, that the order of the blocks in the first row and first column are identical. Note that multiplication of row x of M by $a \in A$ has a natural interpretation as a permutation of the rows of E_M. We simply apply the map $i \mapsto ai$ to the row x of M wherever it occurs in E_M. This action is regular because A is a group. The action on the columns is the corresponding right regular action. We note that E_1 is simply a multiplication table for the group A.

For a given $(0, A)$-matrix, M of order n, there exist a set of uniquely defined $\{0, 1\}$-matrices, $\alpha_a(M)$ such that

$$M = \sum_{a \in A} a\alpha_a(M). \tag{3.3}$$

Note that $\alpha_a(M) = \left[\delta^a_{m_{i,j}}\right]_{1 \le i,j \le n}$ where $m_{i,j}$ is the $(i,j)^{th}$ entry of M.

Now we define

$$\theta(M) = \left[\alpha_{a_i^{-1}a_j}(M)\right]_{i,j\in A} \tag{3.4}$$

where i and j run over A. Note that we use the same ordering of S here as in the expanded matrix.

Lemma 3.14. *θ is an injective map from the set of all $n \times n$ $(0, A)$-matrices into the set of all $n|A| \times n|A|$ $\{0, 1\}$-matrices.*

Proof. Let M and N be $n \times n$ $\{0, A\}$-matrices, such that $\theta(M) = \theta(N)$. Then the first columns of $\theta(M)$ and $\theta(N)$ are the same. Thus $\alpha_a(M) = \alpha_a(N)$ for all $a \in A$. Hence $M = N$ by (3.3). □

We observe that all of the results in this chapter, with minor modifications, hold for matrices over the integral group ring of an abelian group, $\mathbb{Z}A$. This is beyond the scope of the current project however. We note that the product of a monomial $(0, A)$-matrix with an arbitrary $(0, A)$-matrix is again a $(0, A)$-matrix. Since this is the only case that we will require in the remainder of this thesis, we restrict our attention to it.

Lemma 3.15. *θ is a homomorphism.*

Proof. Now by (3.3),

$$MN = \sum_{a,b\in A} ab\alpha_a(M)\,\alpha_b(N) = \sum_{ab\in S} ab\alpha_{ab}(MN).$$

But this implies that

$$\alpha_{a^{-1}b}(MN) = \sum_{c\in S} \alpha_{a^{-1}c}(M)\,\alpha_{c^{-1}b}(N).$$

By the definition of θ, the right hand side of this expression is the product of the i^{th} row block of M with the j^{th} row column of N. The left hand side is simply the block in position (i, j) of $\theta(MN)$. Hence $\theta(MN) = \theta(M)\,\theta(N)$. □

Lemma 3.16. *If $M \in$ `Mon`(n, A), then $\theta(M) \in$ `Perm`$(n|A|)$.*

Proof. Since M is monomial, $\sum_{a\in A} \alpha_a(M)$ is a permutation matrix. In particular it contains exactly one non-zero entry in each row. Hence $[\alpha_{a_1}(M)|\alpha_{a_2}(M)|\ldots|\alpha_{a_n}(M)]$ contains exactly one non zero entry on each row. The argument for columns is identical.

□

Theorem 3.17. *θ : `Mon`$(n, A) \to$ `Perm`$(n|A|)$ is an embedding.*

Proof. The proof follows immediately from the previous three lemmas. Lemma 3.16 shows that the the image of $\mathtt{Mon}(n, A)$ lies in $\mathtt{Perm}(n\,|A|)$. Lemmas 3.14 and 3.15 together show that the mapping is a monomorphism. □

Let $(P, Q) \in \mathtt{Aut}(M)$. We define

$$\Theta\,(P, Q) = (\theta\,(P)\,, \theta\,(Q))\,.$$

By Theorem 3.17, $\Theta : \mathtt{Aut}(M) \to \mathtt{Perm}(n\,|A|) \times \mathtt{Perm}(n\,|A|)$ is an embedding.

Lemma 3.18. *Let M be a $(0, A)$-matrix.* $(P, Q) \in \mathtt{Aut}(M) \Rightarrow \Theta\,(P, Q) \in \mathtt{PermAut}(E_M)$.

Proof. We show that the automorphism group of M forms a subgroup of $\mathtt{PermAut}(E_M)$. Firstly, we observe that for any $(0, A)$-matrix, $P = \sum_{k \in A} a_i^{-1} a_k \alpha_{a_i^{-1} a_k}\,(P)$. But a_i is a constant in this sum, so,

$$a_i P = \sum_{k \in A} a_k \alpha_{a_i^{-1} a_k}\,(P)$$

Now, we show that every block of E_M is fixed by $\Theta\,(P, Q)$ if (P, Q) is an automorphism of M. All summations are carried out over A, with a fixed ordering of elements.

$$\begin{aligned}
\theta\,(P)\,E_M \theta\left(Q^\top\right) &= \left[\sum_k \alpha_{a_i^{-1} a_k}\,(P)\,a_k M a_j\right]_{i,j} \theta\left(Q^\top\right) \\
&= \left[a_i P M a_j\right]_{i,j} \theta\left(Q^\top\right) \\
&= \left[\sum_l a_i P M a_l^{-1} \alpha_{a_j a_l^{-1}}\left(Q^\top\right)\right]_{i,j} \\
&= \left[a_i P M \sum_l a_l^{-1} \alpha_{a_j a_l^{-1}}\left(Q^\top\right)\right]_{i,j} \\
&= \left[a_i P M a_j Q^\top\right]_{i,j} \\
&= \left[a_i P M Q^\top a_j\right]_{i,j} \\
&= \left[a_i M a_j\right]_{i,j} \\
&= E_M
\end{aligned}$$

Note that we use the fact $\alpha\,(Q)^\top = \alpha\left(Q^\top\right)$ implicitly in our argument. □

We stress that in general, $\mathtt{Im}(\Theta) \neq \mathtt{PermAut}(E_M)$. Since all of our calculations are carried out inside of $\mathtt{Im}(\Theta)$ we have not investigated this problem in any depth. We will show in Chapter 4, that for any invertible matrix $\mathtt{Im}(\Theta) \cong \mathtt{PermAut}(E_M)$. We note that

it would be an interesting exercise to fully determine the relationship between $\mathtt{Im}(\Theta)$, $\mathtt{PermAut}(E_M)$ and $\mathtt{Aut}(E_M)$, for an arbitrary $(0, A)$-matrix M. Unfortunately this too falls outside of the scope of this thesis. In the case of central extensions, we observe that $\mathtt{Im}(\Theta)$ contains a special central subgroup, which is the last tool that we need to characterise cocyclic development.

Lemma 3.19. *The centre of* $\mathtt{Im}(\Theta)$ *contains a subgroup isomorphic to* A, $\Upsilon(A)$.

Proof. The set of scalar matrix pairs, $\left(aI_n, a^{-1}I_n\right)$ forms a central subgroup of $\mathtt{Aut}(M)$, isomorphic to S. Thus its image under Θ, $\Upsilon(A)$ is a central subgroup of $\mathtt{Im}(\Theta)$. □

3.4 Cocyclic development

Again, since the primary objects of study in this thesis are Hadamard matrices, which contain no zero entries, we define cocyclic development only for A-matrices. We experimented with various other definitions to expand this to $(A, 0)$ matrices, but most led to contradictions. In any case, the theory of this section is more than sufficient for the problems considered in the remainder of this thesis. We suspect a reformulation the theory of this chapter for matrices with entries in the group ring $\mathbb{Z}A$ would solve this problem. Unfortunately, this falls beyond the scope of the project. In any case, we now introduce our abstract definition of cocyclic development.

Definition 3.20. We say that an $n \times n$ A-matrix, M, is *cocyclic* if there exists a group G, of order n, a cocycle $\psi \in Z^2(G, A)$ and a set map: $\phi : G \to A$ such that $M \equiv_A [\psi(a, b)\,\phi(ab)]_{a,b\in A}$, where $\equiv_A$ simply denotes A equivalence.

When we wish to be more specific, we will say that ψ is a cocycle of M if $M \equiv_A [\psi(a, b)\,\phi(ab)]_{a,b\in A}$ where $\phi : G \to A$ is some set map. These definitions are quite abstract in that we rarely relate a specific cocycle to a given matrix or vice versa, but they lead to somewhat simpler statements in various proofs throughout this chapter. Note that A-equivalence is a finer equivalence relation than cohomological equivalence in this definition. Given $M \equiv_A [\psi(a, b)\,\phi(ab)]_{a,b\in A}$ by no means does it follow that $M \equiv_A [\psi'(a, b)\,\phi'(ab)]_{a,b\in A}$. This is one of the central problems in the theory of cocyclic designs. For example, in the case of Hadamard matrices, cohomology classes do not preserve orthogonality of the matrices generated from them. Conversely, however, if $M \equiv_A M'$ for some cocyclic developed matrix M, then M' is cocyclic developed, and its cocycle is cohomologous to that of M.

The goal of this section is to relate cocyclic development to group development via group cohomology. This result will characterise cocyclic development of a matrix in terms of a

special type of regular action on the expanded matrix. The point is that the existence of such an action is equivalent to cocyclic development. We will make extensive use of our results on group development given in Section 3.2 and the group cohomology developed in Chapter 2.

Lemma 3.21. *Let M and M' be square $\{0, A\}$-matrices. If $M \equiv_A M'$, then $\mathtt{PermAut}(E_M)$ is conjugate to $\mathtt{PermAut}(E_{M'})$ in $\mathtt{Mon}(n, A) \times \mathtt{Mon}(n, A)$.*

Proof. Let $M = PM'Q^\top$ where $P, Q \in \mathtt{Mon}(n, A)$. Now let $(U, V) \in \mathtt{PermAut}(E_M)$. Consider the mapping

$$(U, V) \mapsto \left(\theta(P) U \theta(P)^{-1}, \theta(Q) V \theta(Q)^{-1}\right)$$

which takes an automorphism of E_M to one of $E_{M'}$. That they are conjugate in $\mathtt{Mon}(n, A) \times \mathtt{Mon}(n, A)$ is clear from the definition of the map. □

Note additionally that the map of Lemma 3.21 fixes $\Upsilon(S)$ elementwise. We also observe that regular actions are preserved by conjugation. This will be crucial to the following Lemma.

Lemma 3.22. *Let M be an $n \times n$ A-matrix, and let K be a group of order $n|A|$ containing a central subgroup, $\overline{A}$, isomorphic to A. Suppose that $M \equiv_A [\psi(g, h)\phi(gh)]_{g,h \in G}$ for some cocycle $\psi \in Z^2(G, A)$ of the central extension*

$$1 \to A \xrightarrow{\iota} K \xrightarrow{\pi} K/\overline{A} \to 1$$

where ι is the composite of the inclusion $\overline{A} \to K$ and an isomorphism $A \to \overline{A}$. Then there is an isomorphism of K onto a regular subgroup of $\mathtt{PermAut}(E_M)$, mapping $\overline{A}$ onto $\Upsilon(A)$.

Proof. Our definition of cocyclic development is only up to A-equivalence. In particular, we can multiply a row or column by $a \in A$ and remain in the same equivalence class. By Lemma 3.21, we may consider

$$\begin{aligned} M &\equiv_A [\psi(g, h)\varphi(gh)]_{g,h \in G} \\ &\equiv_A \left[\psi(g, h)\varphi^{-1}(g)\varphi^{-1}(h)\varphi(gh)\right]_{g,h \in G} \\ &\equiv_A \left[\psi(g, h)\partial\varphi^{-1}(gh)\right]_{g,h \in G} \\ &\equiv_A \left[\psi'(g, h)\right]_{g,h \in G} \end{aligned}$$

Results for this matrix translate directly into statements about M. We begin by fixing total orders on the elements of G, $\{g_i | 1 \le i \le n\}$ and of A, $\{a_j | 1 \le j \le |A|\}$. We then

label the rows and columns of E_M with elements of $E(\psi')$ ordered as follows:

$$(g_1, a_1) \leq (g_2, a_1) \leq \ldots \leq (g_n, a_1), \leq (g_1, a_2) \leq \ldots \leq \left(g_n, a_{|A|}\right)$$

We stress that the ordering of the labels of the rows is the same as that of the columns, and depends only on our arbitrary orderings of the Abelian group, A, and the quotient group, G.

It is now easy to see that the map $\varpi : E(\psi') \to A$ by $\varpi(x, a) = a$ is the required group development function for E_M. Consider the $(i,j)^{th}$ block of E_M, which by definition is:

$$\begin{aligned} a_i a_j M &= \left[a_i a_j \psi'(g,h)\right]_{g,h\in G} \\ &= \left[\phi\left(gh, a_i a_j \psi'(g,h)\right)\right]_{g,h\in G} \\ &= \left[\phi\left((g,a_i)(h,a_j)\right)\right]_{g,h\in G}. \end{aligned}$$

Thus the entry in position $((g,a_i)(h,a_j))$ of the $E(\psi')$ indexed matrix E_M is given by $\phi((g,a_i),(h,a_j))$.

Thus we have that the expanded design, E_M is group developed over the canonical extension of A by G defined by ψ'. We now show that this implies that M is cocyclic developed over G. First we use Lemma 3.9. This gives us an isomorphism from $E(\psi')$ onto a regular subgroup of $\texttt{PermAut}(E_M)$ given by

$$(g,a) \in E\left(\psi'\right) \mapsto \left(T_{(g,a)}, S_{(g,a)}\right).$$

Note in particular that this isomorphism maps the subgroup $\{(1,a) \,|a \in A\}$ onto $\Upsilon(A)$. Recall that an element of $\Upsilon(A)$ is given by $\left(\theta(aI_n), \theta\left(a^{-1}I_n\right)\right)$ and that the $(i,j)^{th}$ block of $\theta(aI_n) = \left[\alpha_{a_i{}^{-1}a_j}(aI_n)\right]_{i,j}$ is I_n if $a_i^{-1}a_j = a$ and is the zero matrix otherwise. We compare this with the $(i,j)^{th}$ block of $T_{1,a} = \left[\delta^{(x,a_i)(1,a)}_{(y,a_j)}\right]_{(x,a_i)(y,a_j)}$, which is the matrix

$$\delta^{(x,a_i a)}_{(y,a_j)} = \begin{cases} \left[\delta^x_y\right]_{x,y\in G} & \text{if } a_i a = a_j \\ 0_n & \text{otherwise} \end{cases}$$

Hence, $T_{(1,a)} = \theta(aI_n)$ and similarly $S_{(1,a)} = \theta\left(a^{-1}I_n\right)$. Thus the inclusion, ι, given in the statement of the lemma maps $(1,a)$ to $\Upsilon(a)$, as claimed.

Now, we have verified that $E(\psi')$ is isomorphic to a regular subgroup of $\texttt{PermAut}(E_{M'})$, by an isomorphism mapping of $(1,S)$ onto $\Upsilon(S)$. Now obviously ψ' is a cocycle of the canonical central extension,

$$1 \to A \to E\left(\psi'\right) \to G \to 1.$$

But it is also a cocycle of the short exact sequence given in the statement of this lemma, and by Theorem 2.17, these extensions are equivalent. This means that there is an isomorphism of K onto $E(\psi)$ mapping $\overline{S}$ to $(1,S) \leq E(\psi)$. This is the required regular subgroup of $\texttt{PermAut}(E_M)$. This completes the proof. □

We now prove a converse of of Lemma 3.22.

Lemma 3.23. *Let M be an $n \times n$ A-matrix. Suppose that $\texttt{PermAut}(E_M)$ has a regular subgroup K containing $\Upsilon(A)$ as a central subgroup. Then up to A-equivalence,*

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

for some $\psi \in Z^2(G,A)$ where $G = K/\Upsilon(A)$.

Proof. We begin by defining the embedding $\iota : A \to K$ by

$$\iota(a) = \left(\theta(aI_n), \theta\left(a^{-1}I_n\right)\right) \in \Upsilon(A) \subset K$$

Let ψ be a cocycle of the central extension

$$1 \to A \xrightarrow{\iota} K \xrightarrow{\pi} G \to 1.$$

Then by Theorem 2.17, this exact sequence is equivalent to the canonical central extension

$$1 \to A \xrightarrow{\iota_0} E(\psi) \xrightarrow{\pi_0} G \to 1.$$

So there exists an isomorphism $\alpha : E(\psi) \to K$ such that $\alpha((1,a)) = \iota(a)$ for all $a \in A$. Hence by Lemma 3.10, we have that

$$E_M = [\phi((g,a)(h,b))]_{(g,a),(h,b) \in E(\psi)}$$

for some set map $\phi : E(\psi) \to A$, and some fixed indexing of the rows and columns of E_M by the elements of $E(\psi)$, where the indexings need not coincide.

Now E_M is defined according to a fixed ordering of the the elements of A, and the induced action of the $\iota(a)$ on the rows of E_M is to multiply them entrywise by a. Similarly, $\iota(a)$ multiplies the columns entrywise by a^{-1}. According to the representation given in Lemma 3.23 of E_M, the induced row action of $(1,a) \in E(\psi)$ on E_M moves (g,b) to row $(1,a)^{-1}(g,b)$, i.e. row (g,b) becomes row $(1,a)(g,b) =$ row (g,ab). Now these actions coincide via α, so we have

$$\phi((g,b)(1,a)) = s\phi((g,b)), \ \forall a,b \in A, g \in G.$$

In particular, $\phi(g,a) = a\phi(g,1)\ \forall s \in S, g \in G$. It follows that the entry in row (g,a) and column (h,b) is, by Lemma 3.23, equal to

$$\phi(gh, st\psi(g,h)) = st\psi(g,h)\,\phi(gh,1).$$

Now, we focus our attention on the block B in position $(1,1)$ of E_M, that is, M itself. All arguments made for rows apply with suitable modifications also to columns. We wish to show that the rows of B are labelled by a transversal of G in $E(\psi)$, under the row indexing used in Lemma 3.23. Assume that (g,a) labels a row in B. Then (g,b) cannot label a row in this block for any $a \neq b$. For if it did, then the induced action of $\left(1, a^{-1}b\right) \neq (1,1)$ moves distinct rows within M to each other. But, as we discussed earlier, the non trivial elements of $\iota(A)$ permute the block-rows of E_M transitively under the induced row action. Thus the rows of B are labelled by the elements (g, a_g), where G ranges completely and irredundantly over G. The argument for the columns is identical. Now, we multiply each row, (g,t) of B by t and each column (g,t) by t also. By Lemma 3.23, this yields that

$$M \equiv_A \left[\psi(g,h)\,\phi(gh,1)\right]_{g,h\in G}$$

where the indexing of rows and columns of M is by elements of G is a remnant of the indexing in Lemma 3.23. Now multiplication of the above matrix by $\phi(g,1)^{-1}$ and each column h by $\phi(h,1)^{-1}$ finally proves the result:

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

where $\psi' \in [\psi]$ □

Now the above pair of Lemmas prove the following theorem, which was the main goal of this chapter. We have produced an algebraic characterisation of the property of cocyclic development for a square matrix with entries in an Abelian group, A.

Theorem 3.24. *An $n \times n$ A-matrix, M, is cocyclic with cocycle $\psi \in Z^2(G,A)$ if and only if* `PermAut`(E_M) *has a regular subgroup isomorphic to $E(\psi)$, which contains $\Upsilon(0,A)$ as a central subgroup.*

Proof. Immediate from Lemmas 3.22 and 3.23. □

Since we define cocyclic development in terms of group development, it seems fitting to close this chapter with a characterisation of group developed matrices in terms of development over a coboundary. Note that this discussion applies only to A-matrices, not to $(0,A)$-matrices as the first characterisation of group development did.

Lemma 3.25. *A square A-matrix, M is group developed over G if and only if it is developed over a coboundary, $\partial\phi : G \times G \to A$*

Proof. Assume that M is group developed. Then $M = [\phi(gh)]_{g,h\in G}$. But then M is A-equivalent to the matrix $M' = \left[\phi(g)^{-1}\phi(h)^{-1}\phi(gh)\right]_{g,h\in G}$. Thus M is developed over a coboundary.

Conversely, assume that M is developed over a coboundary. Then

$$\begin{aligned} M &= [\partial\phi(g,h)]_{g,h\in G} \\ &= \left[\phi(g)\phi(h)\phi^{-1}(gh)\right]_{g,h\in G} \\ &\equiv_A \left[\phi^{-1}(gh)\right]_{g,h\in G} \end{aligned}$$

Thus development over a coboundary is equivalent to group development for A-matrices. □

It follows from this lemma that if M is an A-matrix group developed over G, then it is cocyclic developed by a coboundary. This implies that the extension of A by G is split. In other words, the existence of a split extension group acting regularly on E_M implies that M is group developed over G.

Chapter 4

Group actions on Hadamard matrices

We begin this chapter with a review of some of the basic properties of Hadamard matrices, in particular with respect to their equivalence operations and automorphism groups. The remainder of this chapter will consist of a concrete application of the theory of the previous chapters to Hadamard matrices of small order. In particular, we explicitly calculate the expanded matrix, referred to here as the expanded design, of a Hadamard matrix. We prove that the permutation automorphism group of the expanded matrix is isomorphic to the automorphism group of an invertible matrix in this case. From this we derive necessary and sufficient conditions for a Hadamard matrix to be group developed or cocyclic developed. Throughout we use observations on the structure and combinatorial properties of Hadamard matrices to simplify our calculations. The most important of these properties is of course row-orthogonality, which we used in Chapter 1 to prove that group developed Hadamard matrices exist only at square orders. Note that this condition implies that there are no repeated rows or columns in the matrix. Also, it is a result of Hadamard that these matrices contain only $\{\pm 1\}$ entries, there will be no zeros in the matrices. All of this extra information on the structure of Hadamard matrices will allow us both to simplify the general theory of the previous chapter and to prove stronger results.

Recall that a Hadamard matrix is simply an orthogonal square array with an alphabet of size 2, normally denoted $\{1, -1\}$. As noted in Chapter 1, it is closely related to the incidence matrix of a 2-$(4\lambda - 1, 2\lambda - 1, \lambda - 1)$ design. Throughout this Chapter, H will usually refer to a Hadamard matrix of order n, and G will denote a group of order n. Also, $\psi : G \times G \to \langle -1 \rangle$ will be a cocycle. Finally, $E(\psi)$ will be the central canonical extension of C_2 by G corresponding to the cocycle ψ.

4.1 Row-Orthogonality

Definition 4.1. A matrix M is row-orthogonal if for any two rows, r_i, r_j, we have $r_i \bullet r_j = 0$.

All Hadamard matrices are row-orthogonal. Since the transpose of a Hadamard matrix is again Hadamard, we have also that Hadamard matrices are column orthogonal also. This is not a property that is preserved by cohomology classes in general. Thus given a cocyclic Hadamard matrix, $[\phi(x,y)]_{x,y\in G}$, we cannot in general predict whether or not a cohomologous cocycle, ϕ' will generate a Hadamard matrix. The best that we can do at present is to demonstrate a computationally cheap test that determines whether or not a cocyclic matrix is Hadamard. Recall that a matrix, M is cocyclic if and only if there exists a subgroup of $\texttt{Aut}(M)$ which acts regularly on E_M and contains the special central subgroup, $\langle\zeta\rangle$, which is defined to be

$$\left\{\left(aI, a^{-1}I\right) \mid a \in A\right\}$$

where A is the alphabet over which M is defined. In the case of Hadamard matrices, $\langle\zeta\rangle = \{(I,I),(-I,-I)\}$. Note that our lemma is slightly more general then this. It does not actually require the existence of a regular action: transitivity is sufficient.

Lemma 4.2. *Let M be a square $\{\pm 1\}$-matrix. Suppose that $\texttt{PermAut}(E_M)$ is transitive. Then M is Hadamard if and only if the i^{th} row of M is orthogonal to the j^{th} row of M, for all $j \neq i$ and some fixed i.*

Proof. Denote by r_i the i^{th} row of E_M. By hypothesis there exist permutation matrices such that $PE_MQ^\top = E_M$, and the first row of $PE_M = E_MQ$ is r_i. At the same time for $j \neq i$, $1 \leq j \leq v$, $r_jQ^\top = r_l$ for some l. We cannot have $l = 1$ since this would imply $r_j = r_1Q = r_i$. Neither can we have $l = v+1$: if this were true, then $r_j = -r_1Q = -r_i$, which contradicts that $j \leq v$. Therefore if the first row of M is orthogonal to every initial row, we have that

$$r_i r_j^\top = r_1 Q r_j^\top = r_1\left(r_jQ^\top\right)^\top = r_1 r_l^\top = 0$$

by the structure of E_M. It follows, again by the structure of E_M that the i^{th} row of M is orthogonal to the j^{th} row. □

4.2 Hadamard equivalence

Recall that two $n \times n$ matrices M and M' are A-equivalent if their entries lie in $(0, A)$, and there exist monomial A matrices, P and Q such that $PMQ^\top = M'$. Hadamard matrices have entries in $\langle -1 \rangle \cong C_2$. Furthermore, the action of $\mathtt{Mon}(n, \langle -1 \rangle) \times \mathtt{Mon}(n, \langle -1 \rangle)$ on the set of all (± 1)-matrices of order n restricts to an action on the possibly empty set of Hadamard matrices of order n. Thus we call two Hadamard matrices equivalent if there exists a finite sequence of row and column permutations and negations transforming one into the other. Clearly this is a true equivalence relation, which partitions the set of all Hadamard matrices of order n into disjoint classes. We observe in particular that this equivalence relation preserves the Hadamard property. For a Hadamard matrix, the monomial matrices P and Q are simply signed permutation matrices. Thus they have determinant in $\{\pm 1\}$. Recall that the determinant of a product of matrices is the product of the determinants. Thus if $|\mathtt{Det}\,(H)| = n^{n/2}$, it follows that $\left|\mathtt{Det}\left(PHQ^\top\right)\right| = n^{n/2}$. Thus predictably, the Hadamard property is preserved by Hadamard equivalence. Note that some authors include transposition as an equivalence relation: we do not. Matrices that are transposes of one another have isomorphic automorphism groups, however. Thus any computational or theoretical results for one equivalence class hold also for the other. Recall that group development is a property of individual matrices up to permutation equivalence, which is a finer equivalence relation then Hadamard equivalence. Thus a permutation equivalence class of group developed Hadamard matrices is contained entirely within a Hadamard equivalence class of Hadamard matrices. On the other hand, cohomological equivalence, in the sense of being cocyclic developed over cohomologous cocycles, is a coarser equivalence relation then Hadamard equivalence. Hadamard equivalence classes lie entirely within cohomological equivalence classes, but given $H \equiv_H [\psi(g,h)\,\phi(gh)]_{g,h\in G}$, and ψ' cohomologous to ψ it does not follow that $H \equiv_H [\psi'(g,h)\,\phi(gh)]_{g,h\in G}$.

Computationally, it is necessary to consider equivalence classes of Hadamard matrices as the number of Hadamard matrices equivalent to a given one increases exponentially. By the Orbit-Stabiliser theorem, the number of Hadamard matrices equivalent to a given matrix of order n is $2^{2n}n!^2/k$, where k is the order of $\mathtt{Aut}(H)$. To illustrate the vast number of matrices involved, we observe that there are exactly $2^{55}28!^2 = 6.7 \times 10^{75}$ matrices in each of 137 equivalence classes at order 28.

Additionally, the number of equivalence classes of Hadamard matrices is considerable even for relatively small n. At the time of writing, there were known to be more than 3.578 million equivalence classes of Hadamard matrices of order 32, and more then 18.29 million of order 36 [12]. Alternative definitions of equivalence abound; however we will

not consider these other definitions in the thesis. Our primary goal is classification at the orders where all Hadamard matrices are completely known.

We have already described the action of the group $\mathtt{Mon}(n, A) \times \mathtt{Mon}(n, A)$ on a square $(0, A)$-matrix, M, of order n. Recall that the pointwise stabiliser of M is the automorphism group of M, $\mathtt{Aut}(M)$. We now give an explicit definition of this group for Hadamard matrices.

Definition 4.3. The automorphism group of a Hadamard matrix, H, of order n, is the stabiliser of H in $\mathtt{Mon}(n, \langle -1 \rangle) \times \mathtt{Mon}(n, \langle -1 \rangle)$. We denote this group by $\mathtt{Aut}(H)$.
This is the group of all pairs of monomial matrices, (P, Q) with the property that $PHQ^\top = H$. As we noted earlier, the Hadamard property requires that matrices have non-zero determinant, hence Lemma 3.7 holds. Thus if (P, Q_1) and $(P, Q_2) \in \mathtt{Aut}(H)$, it follows that $Q_1 = Q_2$.

4.3 The expanded design of a Hadamard matrix

The small size of the alphabet for Hadamard matrices means that the expanded design is easily described:

$$E_H = \begin{pmatrix} H & -H \\ -H & H \end{pmatrix}. \tag{4.1}$$

Recall that Theorem 3.17 states that $\mathtt{Aut}(H)$ embeds into $\mathtt{PermAut}(E_H)$. In this section we show that for invertible matrices, and thus Hadamard matrices, these groups are in fact isomorphic. Recall from Chapter 3 our definition of the map θ, (3.4). Note that it associates with a signed permutation matrix, P, of order n, a permutation matrix of order $2n$, given by the following bijection:

$$\theta(P) = \begin{pmatrix} \alpha_1(P) & \alpha_{-1}(P) \\ \alpha_{-1}(P) & \alpha_1(P) \end{pmatrix}$$

where $\alpha_1(P)$ and $\alpha_{-1}(P)$ are uniquely defined $(0,1)$-matrices as defined in (3.3). Note in particular that they are related to P by the equality $P = \alpha_1(P) - \alpha_{-1}(P)$. We define $\Theta(P, Q) = (\theta(P), \theta(Q))$ as usual. In the next theorem we will make use of the following lemma.

Lemma 4.4. *Suppose that* $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}], D = [d_{ij}]$ *are* $n \times n$ $(0,1)$*-matrices such that* $A - B = D - C$*. Further suppose that*

$$P = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

is a permutation matrix. Then $A = D$ and $B = C$.

Proof. We write the hypothesis $A - B = D - C$ as an entrywise equality:

$$a_{ij} - b_{ij} = d_{ij} - c_{ij} \quad \forall\, 1 \leq i, j \leq n. \tag{4.2}$$

Fix i and j. Now, suppose that $a_{ij} = 1$. Since P is a permutation matrix (so has just one non-zero entry in each row and column), it follows that $b_{ij} = 0$ and $c_{ij} = 0$. Then (4.2) implies that $d_{ij} = 1$. So $a_{ij} = d_{ij}$ in this case.

Suppose that $a_{ij} = 0$. If $b_{ij} = 1$ then because P is a permutation matrix, $d_{ij} = 0$; in particular $a_{ij} = d_{ij}$. If $b_{ij} = 0$ then (4.2) implies that $d_{ij} = c_{ij}$; further, since $d_{ij}, c_{ij} \in \{0, 1\}$ and P is a permutation matrix, we must have $d_{ij} = c_{ij} = 0$.

Thus $a_{ij} = d_{ij}$ for all i and j. That is, $A = D$. Hence $C = D + B - A = B$. □

Theorem 4.5. *Let M be an invertible $\{\pm 1\}$-matrix. Then the homomorphism given by $\Theta : \mathtt{Aut}(M) \mapsto \mathtt{PermAut}(E_M)$ is an isomorphism.*

Proof. The proof that Θ is an injective homomorphism proceeds from the general result in Chapter 3, Theorem 3.17. Lemma 3.18 shows that it does map into $\mathtt{PermAut}(E_H)$. To show that Θ is an isomorphism, it suffices to prove that Θ is surjective. We now show that every element of $\mathtt{PermAut}(E_M)$ may be decomposed into a 2×2 block matrix such that the upper left and the lower right quadrants are equal, and the remaining two quadrants are likewise equal. We write the equality $PE_M = E_M Q$ as a block matrix equation:

$$\begin{pmatrix} P_\kappa & P_\beta \\ P_\gamma & P_\delta \end{pmatrix} \begin{pmatrix} M & -M \\ -M & M \end{pmatrix} = \begin{pmatrix} M & -M \\ -M & M \end{pmatrix} \begin{pmatrix} Q_\kappa & Q_\beta \\ Q_\gamma & Q_\delta \end{pmatrix}.$$

We show now that $P_\kappa = P_\delta$, that $P_\beta = P_\gamma$, and likewise for Q. Multiplying these matrices in the standard fashion gives the following identity:

$$\begin{pmatrix} (P_\kappa - P_\beta)\, M & (P_\beta - P_\kappa)\, M \\ (P_\gamma - P_\delta)\, M & (P_\delta - P_\gamma)\, M \end{pmatrix} = \begin{pmatrix} M\,(Q_\kappa - Q_\gamma) & M\,(Q_\beta - Q_\delta) \\ M\,(Q_\gamma - Q_\kappa) & M\,(Q_\delta - Q_\beta) \end{pmatrix}$$

From this, and the fact that M is invertible, it follows that:

$$\begin{aligned} (P_\kappa - P_\beta)\, M = M\,(Q_\kappa - Q_\gamma) &= -M\,(Q_\gamma - Q_\kappa) = -\,(P_\gamma - P_\delta)\, M \\ (P_\kappa - P_\beta)\, M M^{-1} &= -\,(P_\gamma - P_\delta)\, M M^{-1} \\ P_\kappa - P_\beta &= P_\delta - P_\gamma. \end{aligned}$$

Thus by Lemma 4.4:

$$P_\kappa = P_\delta \quad P_\beta = P_\gamma.$$

The argument for Q is exactly analogous. Thus every $(P, Q) \in \texttt{PermAut}(E_M)$ has the form

$$\left(\begin{pmatrix} P_\kappa & P_\beta \\ P_\beta & P_\kappa \end{pmatrix}, \begin{pmatrix} Q_\kappa & Q_\beta \\ Q_\beta & Q_\kappa \end{pmatrix} \right)$$

Now we show that $(P', Q') = ((P_\kappa - P_\beta), (Q_\kappa - Q_\beta)) \in \texttt{Aut}(M)$.

$$\begin{aligned}
\begin{pmatrix} M & -M \\ -M & M \end{pmatrix} &= \begin{pmatrix} P_\kappa & P_\beta \\ P_\beta & P_\kappa \end{pmatrix} \begin{pmatrix} M & -M \\ -M & M \end{pmatrix} \begin{pmatrix} Q_\kappa & Q_\beta \\ Q_\beta & Q_\kappa \end{pmatrix}^\top \\
&= \begin{pmatrix} (P_\kappa - P_\beta) M & -(P_\kappa - P_\beta) M \\ -(P_\kappa - P_\beta) M & (P_\kappa - P_\beta) M \end{pmatrix} \begin{pmatrix} Q_\kappa & Q_\beta \\ Q_\beta & Q_\kappa \end{pmatrix}^\top \\
&= \begin{pmatrix} P'M & -P'M \\ -P'M & P'M \end{pmatrix} \begin{pmatrix} Q_\kappa & Q_\beta \\ Q_\beta & Q_\kappa \end{pmatrix}^\top \\
&= \begin{pmatrix} P'MQ'^\top & -P'MQ'^\top \\ -P'MQ'^\top & P'MQ'^\top \end{pmatrix}.
\end{aligned}$$

Hence $P'MQ'^\top = M$, i.e. $(P', Q') \in \texttt{Aut}(M)$ as claimed. Thus Θ is a surjection, and hence also an isomorphism. □

We consider now the image of $(-I, -I) \in \texttt{Aut}(M)$ under Θ.

$$\zeta = \left(\begin{bmatrix} 0_n & I_n \\ I_n & 0_n \end{bmatrix}, \begin{bmatrix} 0_n & I_n \\ I_n & 0_n \end{bmatrix} \right)$$

Since Θ is an isomorphism, it follows that ζ is an involution of $\texttt{PermAut}(E_M)$. In fact it is also central by Lemma 3.19, so for any $(P, Q) \in \texttt{PermAut}(E_M)$, we have $\zeta\,(P, Q)\,\zeta = (P, Q)$. Note that this implies that negation of row i in M corresponds to the transposition of rows i and $i + n$ in E_M.

In the course of our research, we generated the automorphism groups of several hundreds of Hadamard matrices. We noticed that all had the following property:

$$\langle \zeta \rangle = Z\left(\texttt{Aut}\left(H\right)\right) \tag{4.3}$$

This leads us to the following conjecture.

Conjecture: *Let H be a cocyclic Hadamard matrix. Then $Z(H) = \langle \zeta \rangle$.*

4.4 Cocyclic Hadamard matrices

In this section, we give necessary and sufficient conditions for a Hadamard matrix, H, to be cocyclic developed over a group, G. This is essentially a restriction of Lemmas 3.22 and 3.23 to the case of Hadamard matrices. First however we restrict our definition of cocyclic to the case of Hadamard matrices.

Definition 4.6. A Hadamard matrix H is cocyclic over the group G with cocycle $\psi : G \times G \to C_2$ if and only if

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

where $\equiv_H$ denotes Hadamard equivalence and ϕ is some set map from G to $\langle \pm 1 \rangle$.

We call a Hadamard matrix pure cocyclic if $\phi\left(gh\right) = 1$ for all $g, h \in G$.

Lemma 4.7. *Every cocyclic Hadamard matrix is Hadamard equivalent to a pure cocyclic matrix.*

Proof. We use the argument given at the start of Theorem 3.22 to remove the set map ϕ. We observe that if H is cocyclic developed then:

$$\begin{aligned} H &\equiv_H \left[\psi\left(g,h\right)\phi\left(gh\right)\right]_{g,h\in G} \\ &\equiv_H \left[\psi\left(g,h\right)\phi^{-1}\left(g\right)\phi^{-1}\left(h\right)\phi\left(gh\right)\right]_{g,h\in G} \\ &\equiv_H \left[\psi\left(g,h\right)\partial\phi^{-1}\left(gh\right)\right]_{g,h\in G} \\ &\equiv_H \left[\psi'\left(g,h\right)\right]_{g,h\in G} \end{aligned}$$

as required. □

As we remarked in Chapter 3, we have experimented with several definitions of cocyclic development. We could use this Lemma to remove the set map from the definition, however we have found that retaining ϕ leads to somewhat more concise statements about cocyclic Hadamard matrices. When we refer to a Hadamard matrix as being cocyclic over ψ, we implicitly assume that ϕ has been suppressed via the above argument. The following theorem of course follows directly from more general results, but we consider it instructive to review it here in the context of Hadamard matrices.

Theorem 4.8. *A Hadamard matrix, H, is cocyclic, with cocycle ψ, if and only if there is an isomorphism, θ of E_ψ onto a centrally regular subgroup of PermAut(E_H), such that $\theta\left((1,-1)\right) = \zeta$.*

Proof. Suppose that H is cocyclic with cocycle $\psi : G \times G \to \langle -1 \rangle$. By Lemma 4.7,

$$E_H = \begin{pmatrix} \psi'(x,y) & -\psi'(x,y) \\ -\psi'(x,y) & \psi'(x,y) \end{pmatrix}$$

for $\psi' = \psi\partial\phi$, where $\partial\phi : G \times G \to C$ is some suitable coboundary. We label the first $|G|$ rows of E_H with elements $(x,1)$ of $E(\psi')$, and the remaining rows with elements $(x,-1)$. We label the columns in the same manner. Then defining a map $g : E(\psi') \to \langle -1 \rangle$ by $g(x,a) = a$, we have that

$$E_H = [g((x,a)(y,b))]_{(x,a),(y,b) \in E(\psi')}$$

Hence E_H is group developed over $E(\psi')$, which is equivalent in a cohomological sense to $E(\psi)$ and thus $E(\psi)$ acts regularly on E_H.

We observe that the involution $(1,-1)$ acts on the rows and columns of the matrix as follows:

$$(x,a)(1,-1) = (x,-a)$$
$$(1,-1)^{-1}(y,b) = (y,-b)$$

It swaps every row and column with its negation, thus it has the same action as ζ. It follows that there is a faithful representation of $E(\psi') \cong E(\psi)$ in $\texttt{PermAut}(E_H)$ that maps $(1,-1)$ to ζ.

We now prove the converse. Suppose that $E(\psi)$ acts regularly on E_H via an embedding θ into $\texttt{PermAut}(E_H)$, such that $\theta((1,-1)) = \zeta$. Therefore

$$E_H = \begin{pmatrix} H & -H \\ -H & H \end{pmatrix} = [g((x,a)(y,b))]_{(x,a),(y,b) \in E(\psi)}$$

for some appropriate set map $g : E(\psi) \to \langle -1 \rangle$. Since $(1,-1)$ acts like ζ,

$$g((x,-a)) = -g((x,a))$$

Hadamard matrices are linearly independent by definition, thus no row/column of H will be the negation of another row/column. Hence the first $|G|$ rows of E_H must be labeled by elements $(x,a) \in E(\psi)$ as x runs completely and irredundantly over G. So there is a Hadamard matrix, $H' \equiv H$ such that

$$H' = [g((x,1)(y,1))]_{(x,1)(y,1) \in E(\psi)} = [g(xy, \psi(x,y))]_{(x,1)(y,1) \in E(\psi)}$$

Finally, we define $h : G \to \langle -1 \rangle$ by $h(x) = g(x, 1)$. Then

$$H' = [\psi(x, yh(xy))]_{x,y \in G}$$

so that $H \equiv_H H'$ is cocyclic with cocycle ψ. □

This theorem provides us with the necessary theory to classify Hadamard matrices by their cocyclic development properties. Later in this chapter we describe in some detail how we implement this theory in the computer algebra system Magma, [2]. First however, we determine the automorphism group and cocyclic development properties of the unique Hadamard matrix of order 2.

4.4.1 Example: Order 2

We note that as the order of this matrix is not square, it cannot be group developed. We show that it is cocyclic developed over the cyclic group of order 2, however.

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The group $\texttt{Mon}(2, \langle -1 \rangle)$ has order 8 and is isomorphic to D_4 since it clearly contains more then one involution. $\texttt{Mon}(2, \langle -1 \rangle) \times \texttt{Mon}(2, \langle -1 \rangle)$ thus has order 64, and is isomorphic to the direct product. It is easy to see that there are 8 elements in the orbit of H: 4 equivalent through permutations alone, and their 4 negations. Thus by the Orbit-Stabiliser Theorem, the order of $\texttt{Aut}(H)$ is 8.

Recall that if H is invertible, and $(P, Q) \in \texttt{Aut}(H)$ then $P = HQH^{-1}$. Thus for each element, P of $\texttt{Mon}(2, \langle -1 \rangle)$ there is a unique automorphism of H, given by $\left(P, HPH^{-1}\right)$. It follows that $\texttt{Aut}(H) \cong D_4$. We need not calculate the subgroups of $\texttt{Aut}(H)$ that act regularly on E_H as in this case it is unnecessary. We observe that there is only one candidate for a regular subgroup of order 2, containing the central involution, $\zeta : \langle (-I, -I) \rangle$, that is ζ itself. Finally we observe that the normalised cocycle $\psi : C_2 \times C_2 \to C_2$ uniquely defined by $\psi(c, c) = -1$ does indeed generate the Hadamard matrix of order 2.

4.5 Computation of Automorphism groups

Theorem 4.8 gives us a characterisation of the cocyclic development properties of H in terms of subgroups of $\texttt{Aut}(H)$ that act regularly on $E(H)$, and contain ζ. The problem

of classifying Hadamard matrices by their cocyclic development properties now begins to look amenable to computation. At the time of writing, no computer algebra system is equipped to compute the automorphism groups of matrices with entries in an arbitrary group. There do exist highly efficient algorithms for computing the automorphism group of a $\{0,1\}$-array, using Brendan McKay's *nauty* programme, [13], as implemented in Magma. Thus we introduce a lemma to relate the automorphism group of H to the automorphism group of a $\{0,1\}$-matrix. We begin, however, by defining the associated design of a Hadamard matrix to be

$$A_H = 1/2\left[E_H + J_{2n}\right] \tag{4.4}$$

Where J_{2n} is the all $1's$ matrix of order $2n$. Essentially, we change the -1 entries of E_H to zeros. We observe that the expanded design is in fact a symmetric balanced incomplete block design.

Lemma 4.9. $\texttt{Aut}(A_H) = \texttt{PermAut}(A_H) = \texttt{PermAut}(E_H)$

Proof. Since A_H is a $(0,1)$-matrix, the first isomorphism is trivial. As to the second, let $P, Q \in \texttt{PermAut}(A_H)$. Then

$$PA_HQ^\top = 1/2\left[PE_HQ^\top + PJ_{2n}Q^\top\right] = 1/2\left[PE_HQ^\top + J_{2n}\right] = 1/2\left[E_H + J_{2n}\right] = A_H$$

Note that $\texttt{Aut}(A_H)$ and $\texttt{PermAut}(E_H)$ are not merely isomorphic, they are in fact equal. This means, in particular, that regular actions are preserved. □

Combining this Lemma with Theorem 4.5, we get the following result:

Theorem 4.10. $\texttt{Aut}(H) \cong \texttt{PermAut}(E_H) = \texttt{Aut}(A_H)$

Proof. Immediate from Theorem 4.5 and Lemma 4.9. □

This associated design may thus be used to efficiently calculate the automorphism group of a Hadamard matrix: since it is a $(0,1)$-array, we may use *nauty* to do so efficiently. There is an inbuilt Magma function that determines subgroups that act regularly on E_H. Further discussion of this function may be found in Appendix A, which also contains a copy of the code that we wrote. It is a simple matter to check that a regular subgroup, R contains ζ. Furthermore, since $\zeta \in Z(R)$, we have that $\langle\zeta\rangle$ is a normal subgroup of R and hence we may form the quotient group $R/\langle\zeta\rangle$. By the cohomology of Chapter 2 and the general results of Chapter 3, we have that H is cocyclic developed over this $R/\langle\zeta\rangle$. Note that this approach may of course be generalised to many other types of pairwise combinatorial design. We will restrict our attention to Hadamard matrices, however.

The computer algebra system Magma, [2], contains a library of Hadamard matrices which is complete for orders up to 28, and which contains a representative matrix for every order up to 256. We used the procedure, described in detail in Appendix A, on each of the Hadamard matrices of order at most 28 to generate information on their cocyclic development properties.

4.6 Equivalence of cocyclic Hadamard matrices and relative difference sets

We promised in Chapter 1 a partial proof of a theorem of Warwick de Launey which establishes a relationship between Central Relative Difference Sets in groups of order $8t$ and cocyclic Hadamard matrices of order $4t$. We elaborate on that remark here, and prove the first part of the equivalence. This proof is due originally to Flannery, see section 3 of [8]. The key observation in the following Lemmas is that a CRDS, if it exists, is a special transversal of the forbidden subgroup, C, in E. The forbidden subgroup is of course precisely that generated by the special central involution, ζ that we have discussed at length in this chapter.

Lemma 4.11. *Suppose that G is a group of order $4t$ and $\psi \in Z^2(G, \langle -1 \rangle)$ a cocycle such that $[\psi(x,y)]_{x,y\in G}$ is a Hadamard matrix. Then*

$$R = \{(x,1) \,|x \in G\}$$

is a $(4t, 2, 4t, 2t)$-RDS in $E(\phi)$ with forbidden subgroup $C = \{(1,1),(1,-1)\} \cong \mathbb{Z}_2$.

Proof. Let $(x,1)$ and $(y,1) \in R, x \neq y$. Then

$$\begin{aligned}(x,1)(y,1) &= (x,1)\left(y^{-1}, \psi\left(y,y^{-1}\right)\right)\\ &= \left(xy^{-1}, \psi\left(x,y^{-1}\right)\right)\psi\left(y,y^{-1}\right)\\ &= \left(xy^{-1}, \psi\left(xy^{-1},y\right)\right)\end{aligned}$$

Note that we used the cocycle identity, (2.2), in the last line of the above proof to show that $\psi\left(xy^{-1},y\right)\psi\left(x,y^{-1}\right) = \psi\left(y,y^{-1}\right)\psi\left(xy^{-1},yy^{-1}\right)$. We also made use of the fact that the exponent of $Z^2(G,C_2)$ is 2. Now since $[\psi(a,b)]_{a,b\in G}$ is Hadamard, every non-initial row contains the same number of $1's$ and $-1's$. So for fixed $xy^{-1} \in G\backslash 1$ there are exactly $2t$ elements $y \in G$ such that $\psi\left(xy^{-1},y\right) = 1$ and $2t$ elements $y \in G$ such that $\psi\left(xy^{-1},y\right) = -1$. Equivalently, each element of $E(\psi)\backslash C$ occurs $2t$ times in the multiset of quotients $(x,1)(y,1)^{-1} \neq (1,1)$ formed from distinct elements of R. □

This lemma shows how to extract a relative difference set from a cocyclic Hadamard matrix. We now show how a cocyclic Hadamard matrix may be constructed from a $(4t, 2, 4t, 2t)$-RDS.

Lemma 4.12. *Let E be a group containing a $(4t, 2, 4t, 2t)$-RDS, with forbidden subgroup $C \cong \langle 1, -1\rangle$. Then E acts centrally regularly on E_H for some Hadamard matrix H, i.e. for some $f \in Z^2(E/C, \langle -1\rangle)$, $[f(x, y)]_{x,y\in G}$ is Hadamard.*

Proof. Let R be a $(4t, 2, 4t, 2t)$-RDS in E with forbidden subgroup C. If $r, s \in R$ with $rC = sC$ then $rs^{-1} \in C$. We observe that $|R| = |E/C|$, hence R is a transversal of C in E. Now, write $E/C = G$, and define a transversal function $\tau : G \to E$ by $\tau(rC) = r$. Let $f_\tau : E/C \to \langle -1\rangle$ be the associated cocycle:

$$f_\tau(rC, sC) = rs\tau(rsC)^{-1}.$$

Recall that since E is a group, f_τ is necessarily normalised. Fix $r \neq 1$. Then

$$f_\tau(rC, sC) = 1 \Leftrightarrow rs \in R \Leftrightarrow us^{-1} = r$$

for some $u \in R$. Since $r \neq 1$ there are exactly $2t$ pairs, $u, s \in R$ such that $us^{-1} = r$ by the definition of a RDS. Thus for fixed $r \neq 1$ row rC of $M = [f_\tau(rC, sC)]_{rC,sC\in E/C}$ contains precisely $2t$ occurrences of 1 and $2t$ occurrences of -1. Now by Lemma 4.2, a $\{\pm 1\}$ cocyclic matrix is Hadamard if and only if each non-identity row is orthogonal to the first. □

The above two lemmas prove the first part of de Launey's theorem: that there exists a $(4t, 2, 4t, 2t)$-CRDS if and only if there exists a cocyclic Hadamard matrix of order $4t$. Towards the end of the project, we became interested in the problem of constructing Hadamard matrices from Relative Difference Sets. Using Marc Röder's Gap package, *RDS*, [14, 15] we wrote a series of short programs to generate a Hadamard matrix from a suitable relative difference set. We search for all difference sets in the groups of order 16, 24, 32, and 40, and used these to generate Hadamard matrices. Up to transpose equivalence, all matrices were represented. This problem is of exponential complexity however. It is conceivable that this technique could be used to construct all cocyclic Hadamard matrices of, say, order 32, without further optomisations it is not a feasible method for finding cocyclic Hadamard matrices of large order, however.

The next chapter of the thesis gives the full classification of cocyclic Hadamard matrices of order at most 28 that we promised in Chapter 1. We observe that by the above lemmas that this gives us a complete census of all CRDS's with parameters $(8t, 2, 4t, 2t)$ essentially for free.

Chapter 5

Classification of small cocyclic Hadamard matrices

In this section we describe the results of our application of the Magma procedure described in Appendix A to all Hadamard matrices of order $4n$ for $n \leq 7$. The Hadamard matrices were drawn from Magma's database, [2]. It is a well established result that all Hadamard matrices of order $4n$ are known for $n \leq 7$, see for example page 268 of [16], or page 17 of [1]. For each matrix, we enumerate and analyse the subgroups of its automorphism group that act regularly on the expanded design and contain ζ. The theory of the previous chapters shows that this is sufficient to establish the groups over which each of the Hadamard matrices are cocyclic. Throughout this chapter, we shall use the term regular subgroup to mean a subgroup of the automorphism group acting regularly on the expanded design of the matrix. By a centrally regular subgroup, we will mean a regular subgroup containing ζ. We stress that, in general, a regular subgroup in this sense will not act regularly on the Hadamard matrix itself. If we have a centrally regular subgroup, we can factor out by $\langle\zeta\rangle$ to get an indexing group over which the Hadamard matrix is cocyclic. It should be noted that an automorphism group may contain several isomorphic centrally regular subgroups, but factoring out by the central involution ζ may give non-isomorphic factor groups. Conversely, non-isomorphic extensions of the indexing groups can also appear. We list the factor groups first, with the corresponding extensions to the right. In listing groups, we first checked if they belonged to any well known family, then we attempted to classify them as direct products of well known groups, failing this, they are given as semidirect products. The remaining cases may all be described as non-split extensions; as there is no well established symbol in the literature for such a product, we define one. Throughout this chapter, we will denote a non-split extension of N by G as $N \sqsupset G$. Group extensions are not in general unique,

we have in places found it expedient to use the same description for non-isomorphic extensions. When this occurs, we uniquely identify such groups with a reference number. Power commutator presentations of groups not uniquely defined will be given at the end of the section in which they occur. In general, the group descriptions given were computed with GAP, while the presentations were computed with Magma.

Since we make extensive use of the groups of order 16, we give a table of our shorthand notation for the non-Abelian groups. The Abelian groups will be presented as direct products of cyclic groups. In our group presentations we omit commutators. Thus we will not in general include relations of the form $a^b = a$. We also omit relations of the form $a^2 = 1$, though we do not omit relations of the form $a^n = 1$ for $n \neq 2$. The notation D_n will denote the dihedral group of order $2n$ throughout this section.

Label	Presentation
$(C_4 \times C_2) \rtimes C_2$	$\langle a, b, c \mid a^2 = d, b^a = bc \rangle$
$C_4 \rtimes C_4$	$\langle a, b, c \mid a^2 = d, b^2 = c, b^a = bc \rangle$
$C_8 \rtimes C_2$	$\langle a, b, c \mid a^2 = c, c^2 = d, b^a = bd \rangle$
D_8	$\langle a, b, c \mid c^2 = d, b^a = bc, c^a = cd, c^b = cd \rangle$
QD_8	$\langle a, b, c \mid a^2 = d, c^2 = d, b^a = bc, c^a = cd, c^b = cd \rangle$
GQ	$\langle a, b, c \mid a^2 = d, b^2 = d, c^2 = d, b^a = bc, c^a = cd, c^b = cd \rangle$
$D_4 \times C_2$	$\langle a, b, c \mid b^a = bd \rangle$
$Q \times C_2$	$\langle a, b, c \mid a^2 = d, b^2 = d, b^a = bd \rangle$
$C_4 \sqsupset C_2^2$	$\langle a, b \mid c^2 = d, b^a = bd \rangle$

5.1 Order 4

We observe that the calculations of Section 4.4.1 show that the Hadamard matrix of order 2 is cocyclic. Since 2 is not square, we know that a regular subgroup acting on the expanded design of the Hadamard matrix of order 2 will not be split. Hence there is a unique centrally regular action on the expanded design by C_4.

We showed in Section 1.5 that the Hadamard matrix of order 4 is group developed over C_4. Of course this implies that it is cocyclic over $C_4 \times C_2$, which is indeed the case. We provide here a summary of all centrally regular subgroups of $\texttt{PermAut}(E_H)$. First however, we note that the automorphism group has order 192, and contains 5 regular subgroups. One of these is not centrally regular however. As we noted in the introduction, we will present our results in the following format: the groups of order n that the Hadamard matrix in question is cocyclic over will be given in the left hand column. The corresponding groups of order $2n$ over which the expanded design is group developed will be given in the right hand column. Where necessary we will give presentations for the groups described in the table.

Indexing Group	Extension Groups
$C_2 \times C_2$	$C_4 \times C_2$
C_4	$C_4 \times C_2$, Q_8, C_2^3

5.2 Order 8

The unique, up to equivalence, matrix of order 8 has an automorphism group of order 21504. This group turned out to have 10 centrally regular subgroups.

Indexing Group	Extension Groups
$C_4 \times C_2$	$C_4 \times C_4$, $C_4 \rtimes C_4$, $C_8 \times C_2$
D_4	$(C_4 \times C_2) \rtimes C_2$, $C_4 \rtimes C_4$, GQ
C_2^3	$C_4 \times C_2^3$, $C_2 \times D_4$, $C_2 \times Q$, $C_4 \sqsupset C_2^2$

5.3 Order 12

There is up to equivalence only a single Hadamard matrix of order 12. Its automorphism group is the Schur cover of M_{12} which has order 190,080. This group has only 3 regular subgroups of order 24, all of which contain ζ. None are Abelian, though when $\langle\zeta\rangle$ is factored out, one does become Abelian.

Indexing Group	Extension Groups
$C_2^2 \times C_3$	$Q_8 \times C_3$
$Alt\,(4)$	$SL\,(2,3)$
D_6	$C_3 \rtimes Q_8$

Since semi-direct products are not in general unique, we give a power commutator presentation for $C_3 \rtimes Q_8$: $\langle a, b, c, d \mid a^3 = 1, b^2 = c^2 = d, b^a = c, c^a = bc, c^b = cd\rangle$

5.4 Order 16

This order was by far the most time consuming to consider. There were in total 165 centrally regular subgroups of order 32 to consider, including all but 6 of the isomorphism classes of groups of order 32. All of the groups that did occur will be described later in this section, but we consider it instructive to mention explicitly those that do not occur as extension groups. Ito's results preclude both C_{32} and D_{16} from occurring. The other groups that fail to appear are closely related to these. They are of the types: $C_{16} \times C_2$, $C_{16} \rtimes C_2$, $C_2 \times D_8$ and QD_{16}, the quasidihedral group of order 32. It should be noted that the only group of exponent 32 is included in this list as well as all but one of the groups of exponent 16. No group of lower exponent appears here.

5.4.1 The Sylvester Hadamard Matrix of order 16

This Hadamard matrix has an automorphism group of order 10,321,920. This group contains 113 centrally regular subgroups of order 32, which belong to 34 different isomorphism types. In fact, this matrix is cocyclic over all but two of the groups of order 16. The two exclusions are the cyclic group C_{16} and the dihedral group, D_8. Note also that this matrix is group developed over no less then 6 different groups of order 16.

Indexing Group	Extension Groups
$C_4 \times C_4$	$C_4^2 \times C_2$, $(C_4 \times C_2) \rtimes C_4$
$(C_4 \times C_2) \rtimes C_2$	$(C_4 \times C_2) \rtimes C_4$, $(C_8 \times C_2) \rtimes C_2$ [7], $(C_4 \times C_2) \sqsupset C_4$, $Q_8 \rtimes C_4$, $C_4^2 \rtimes C_2$ [11], $C_2^2 \sqsupset (C_4 \times C_2)$ [5]
$C_4 \rtimes C_4$	$(C_4 \times C_2) \rtimes C_4$, $C_2^2 \sqsupset (C_4 \times C_2)$ [6]
$C_2 \times C_8$	$(C_8 \times C_2) \rtimes C_2$ [7], $C_8 \times C_2^2$
$C_8 \rtimes C_2$	$(C_8 \times C_2) \rtimes C_2$ [7], $(C_4 \times C_2) \sqsupset C_2^2$
QD_8	$Q \rtimes C_4$, $QH_8 \times C_2$
GQ	$Q \rtimes C_4$, $GQ \times C_2$
$C_4 \times C_2^2$	$C_4^2 \times C_2$, $C_2^2 \sqsupset (C_4 \times C_2)$ [5, 6], $C_4^2 \times C_2$, $D_4 \times C_4$, $Q \times C_4$, $C_8 \times C_2^2$, $(C_4 \times C_2) \sqsupset C_2^2$, $(C_8 \times C_2) \rtimes C_2$ [9], $C_4 \times C_2^3$
$D_4 \times C_2$	$C_2^2 \sqsupset (C_4 \times C_2)$ [5, 6], $C_4 \times D_4$, $C_2^4 \rtimes C_2$, $\left(C_4 \times C_2^2\right) \rtimes C_2$ [21, 22], $(C_2 \times Q) \rtimes C_2$ [16], $C_4^2 \rtimes C_2$ [13], $C_4 \rtimes Q_8$, $C_2 \times QH_8$, $C_2 \times GQ$, $(C_2 \times C_8) \rtimes C_2$ [10], $(D_4 \times C_2) \rtimes C_2$, $C_8 \sqsupset C_2^2$, $D_4 \times C_2^2$
$Q \times C_2$	$C_2^2 \sqsupset (C_4 \times C_2)$ [6], $(Q \times C_2) \rtimes C_2$, $Q \times C_2^2$
$C_4 \sqsupset C_2^2$	$C_4^2 \rtimes C_2$, $D_4 \times C_4$, $Q \times C_4$, $C_4 \times C_2^2 \rtimes C_2$ [21, 22], $(C_2 \times Q) \rtimes C_2$ [16], $C_2^2 \sqsupset C_2^3$ [18, 19], $C_4^2 \rtimes C_2$ [14]
C_2^4	$C_4 \times C_2^3$, $D_4 \times C_2^2$, $Q \times C_2^2$, $C_2^2 \sqsupset C_2^3$, $(C_2 \times D_4) \rtimes C_2$, $(C_2 \times Q) \rtimes C_2$ [17], C_2^5

TABLE 5.1: Groups over which the Sylvester Hadamard matrix of order 16 is cocyclic

5.4.2 The second Hadamard matrix of order 16

This matrix has an automorphism group of order 49152. It has 48 centrally regular subgroups, comprising 25 different isomorphism types. Despite having the smallest automorphism group of all of the matrices of order 16, this Hadamard matrix is cocyclic over 12 of the fourteen groups of order 16. Its associated design may be group developed from any one of 25 groups of order 32.

5.4.3 The remaining Hadamard matrices of order 16

There exist a pair of equivalence classes of Hadamard matrices at order 16 such that each is the transpose of the other. As a result their automorphism groups are isomorphic,

Indexing Group	Extension Groups
$C_4 \times C_4$	$C_8 \times C_4$, $C_8 \rtimes C_4$ [1]
$(C_4 \times C_2) \rtimes C_2$	$C_2^2 \sqsupset (C_4 \times C_2)$ [20], $C_2^3 \sqsupset C_4$
$C_4 \rtimes C_4$	$C_4 \rtimes C_8$ [4], $C_4 \sqsupset D_4$
$C_8 \times C_2$	$C_8 \times C_4$, $C_4 \rtimes C_8$ [4]
$C_8 \rtimes C_2$	$C_4 \rtimes C_8$ [4], $C_8 \rtimes C_4$ [3]
D_8	$(C_8 \times C_2) \rtimes C_2$ [8], $C_8 \rtimes C_4$ [3]
QD_8	$Q_8 \rtimes C_4$, $C_8 \rtimes C_4$ [2]
$C_4 \times C_2^2$	$C_4^2 \times C_2$, $D_4 \times C_4$, $Q \times C_4$, $C_4^2 \rtimes C^2$ [12], $(C_4 \times C_2) \sqsupset C_2^2$
$D_4 \times C_2$	$D_4 \times C_4$, $C_4^2 \rtimes C_2$ [13, 15], $C_4 \rtimes Q_8$, $GQ \times C_2$, $C_8 \sqsupset C_2^2$, $(C_2 \times Q) \rtimes C_2$ [16]
$Q \times C_2$	$Q \times C_4$, $C_2^2 \sqsupset C_2^3$ [18], $C_4 \rtimes Q$, $Q \times C_2^2$, $(C_2 \times Q) \rtimes C_2$ [16]
$C_4 \sqsupset C_2^2$	$D_4 \times C_4$, $Q \times C_4$, $C_4^2 \rtimes C_2$ [12], $(C_2 \times Q) \rtimes C_2$ [16], $C_4^2 \rtimes C_2$ [13, 14], $C_2^2 \sqsupset C_2^2$ [18, 19]
C_2^4	$Q \times C_2^2$, $C_2^2 \sqsupset C_2^3$ [19]

Indexing Group	Extension Groups
D_8	GQ_{32}

and we need only analyse one. This automorphism group has order 86016, and has only one regular subgroup, which contains ζ.

The remaining Hadamard matrix of order 16 has an automorphism group of order 294912. It has however only two regular subgroups containing ζ. One group is Abelian, the other is, like the previous pair, cocyclic over D_8, but has a different extension group. Note that the Abelian extension is split: thus by Lemma 3.25, this matrix is group developed over $C_8 \times C_2$.

Indexing Group	Extension Groups
$C_8 \times C_2$	$C_8 \times C_2 \times C_2$
D_8	$C_8 \rtimes C_4$ [1]

$$
\begin{aligned}
C_8 \rtimes C_4\,[1] &= \langle a,b,c,d,e \mid a^2=c, b^2=d, c^2=e, b^a=be\rangle\\
C_8 \rtimes C_4\,[2] &= \langle a,b,c,d,e \mid a^2=d, b^2=c, c^2=e, b^a=bc, c^a=ce\rangle\\
C_8 \rtimes C_4\,[3] &= \langle a,b,c,d,e \mid a^2=d, b^2=ce, c^2=e, b^a=bc, c^a=ce\rangle\\
C_4 \rtimes C_8\,[4] &= \langle a,b,c,d,e \mid a^2=d, b^2=c, d^2=e, b^a=bc\rangle\\
C_2^2 \sqsupset (C_4 \times C_2)\,[5] &= \langle a,b,c,d,e \mid a^2=e, b^a=bd\rangle\\
C_2^2 \sqsupset (C_4 \times C_2)\,[6] &= \langle a,b,c,d,e \mid a^2=e, b^2=d, b^a=bd\rangle\\
(C_8 \times C_2) \rtimes C_2\,[7] &= \langle a,b,c,d,e \mid a^2=d, d^2=e, b^a=bc\rangle\\
(C_8 \times C_2) \rtimes C_2\,[8] &= \left\langle a,b,c,d,e \mid a^2=d, c^2=e, b^a=bc, c^a=ce, c^b=ce\right\rangle\\
(C_8 \times C_2) \rtimes C_2\,[9] &= \left\langle a,b,c,d,e \mid a^2=d, d^2=e, c^b=ce\right\rangle\\
(C_8 \times C_2) \rtimes C_2\,[10] &= \left\langle a,b,c,d,e \mid c^2=e, d^2=e, b^a=bd, d^a=de, d^b=de\right\rangle\\
C_4^2 \rtimes C_2\,[11] &= \left\langle a,b,c,d,e \mid a^2=d, c^2=e, d^2=e, b^a=bc, c^a=ce, c^b=ce\right\rangle\\
C_4^2 \rtimes C_2\,[12] &= \langle a,b,c,d,e \mid a^2=e, c^2=d, b^a=bd\rangle\\
C_4^2 \rtimes C_2\,[13] &= \langle a,b,c,d,e \mid b^2=e, c^2=d, b^a=bd, c^a=ce\rangle\\
C_4^2 \rtimes C_2\,[14] &= \langle a,b,c,d,e \mid b^2=de, c^2=d, b^a=bd, c^a=ce\rangle\\
C_4^2 \rtimes C_2\,[15] &= \langle a,b,c,d,e \mid b^2=d, c^2=e, b^a=bd, c^a=ce\rangle\\
(Q_8 \times C_2) \rtimes C_2\,[16] &= \langle a,b,c,d,e \mid a^2=d, b^2=d, b^a=bd, c^a=ce\rangle\\
(Q_8 \times C_2) \rtimes C_2\,[17] &= \left\langle a,b,c,d,e \mid b^2=e, c^2=e, b^a=be, c^b=ce, d^a=de\right\rangle\\
C_2^2 \sqsupset C_2^3\,[18] &= \langle a,b,c,d,e \mid a^2=d, b^2=e, c^2=d, b^a=bd, c^a=ce\rangle\\
C_2^2 \sqsupset C_2^3\,[19] &= \langle a,b,c,d,e \mid c^2=e, b^a=be\rangle\\
C_2^2 \sqsupset (C_4 \times C_2)\,[20] &= \left\langle a,b,c,d,e \mid a^2=d, b^2=e, d^2=e, b^a=bc, c^a=ce, d^b=de\right\rangle\\
\left(C_4 \times C_2^2\right) \rtimes C_2\,[21] &= \langle a,b,c,d,e \mid b^2=d, b^a=bd, c^a=ce\rangle\\
\left(C_4 \times C_2^2\right) \rtimes C_2\,[22] &= \langle a,b,c,d,e \mid c^2=d, b^a=bd, c^a=ce\rangle\\
(C_4 \times C_2) \rtimes C_4 &= \langle a,b,c,d,e \mid a^2=d, b^2=e, b^a=bc\rangle\\
(C_4 \times C_2) \sqsupset C_4 &= \left\langle a,b,c,d,e \mid a^2=d, b^a=bc, c^a=ce, d^b=de\right\rangle\\
C_2^3 \sqsupset C_4 &= \left\langle a,b,c,d,e \mid a^2=d, d^2=e, b^a=bc, c^a=ce, d^b=de\right\rangle\\
Q_8 \rtimes C_4 &= \left\langle a,b,c,d,e \mid a^2=d, b^2=e, c^2=e, b^a=bc, c^a=ce, c^b=ce\right\rangle\\
C_4 \sqsupset D_4 &= \langle a,b,c,d,e \mid a^2=d, b^2=c, c^2=e, d^2=e, b^a=bc, c^a=ce\rangle\\
C_2^4 \rtimes C_2 &= \langle a,b,c,d,e \mid b^a=bd, c^a=ce\rangle\\
C_4 \rtimes Q_8 &= \langle a,b,c,d,e \mid a^2=d, b^2=d, c^2=e, b^a=bd, c^a=ce\rangle\\
(C_4 \times C_2) \sqsupset C_2^2 &= \langle a,b,c,d,e \mid a^2=d, d^2=e, b^a=be\rangle\\
(D_4 \times C_2) \rtimes C_2 &= \left\langle a,b,c,d,e \mid d^2=e, b^a=bd, c^a=ce, d^a=de, d^b=de\right\rangle\\
C_8 \sqsupset C_2^2 &= \left\langle a,b,c,d,e \mid b^2=e, d^2=e, b^a=bd, c^a=ce, d^a=de, d^b=de\right\rangle\\
C_2^3 \sqsupset C_2^2 &= \left\langle a,b,c,d,e \mid b^a=be, c^b=ce, d^a=de\right\rangle
\end{aligned}
$$

5.5 Order 20

There are three Hadamard matrices of order 20. All are cocyclic, though as there are only 5 groups of order 20, this case is much simpler than that of order 16.

The first Hadamard matrix of order 20 has an automorphism group of order 6840. $\texttt{PermAut}(E_H)$ has only a single centrally regular subgroup. The presentation for the group of order 40 follows below.

Indexing Group	Extension Groups
$D_5 \times C_2$	$D_{10} \rtimes C_2$

$$D_{10} \rtimes C_2 : \langle a, b, c, d \mid a^2 = b^2 = c, d^5 = 1, b^a = bc, d^a = d^4 \rangle$$

The second matrix has an automorphism group of order 5760. $\texttt{PermAut}(E_H)$ has four centrally regular subgroups, though three of these are isomorphic in all respects to the regular subgroup of the first matrix. The presentation for the second group of order 40 follows below.

Indexing Group	Extension Groups
$D_5 \times C_2$	$D_{10} \rtimes C_2$
$C_{10} \times C_2$	$C_{20} \rtimes C_2$

$$C_{20} \rtimes C_2 : \langle a, b, c, d \mid a^2 = b^2 = c, d^5 = 1, b^a = bd \rangle$$

The final Hadamard matrix of order 20 has an automorphism group of order 3840. Again, $\texttt{PermAut}(E_H)$ has only a single centrally regular subgroup. Note that the extension group is in this case a direct product, in contrast to the previous cases. Observe that this does not mean that H is group developed, however.

Indexing Group	Extension Groups
$D_5 \times C_2$	$D_{10} \times C_2$

5.6 Order 24

As the number of Hadamard matrices begins to grow rapidly at this order, we adapt our method slightly. We observe that the `PermAut`(E_H), for a Hadamard matrix H of order n, will contain a regular subgroup only if its order is some multiple of $2n$. So in this case, we discard all Hadamard matrices with automorphism groups not divisible by 48.

Of the 60 Hadamard matrices of order 24, 27 have automorphism groups with order in $\{8, 16, 24, 32, 64, 72, 128, 256\}$. None of these can have regular subgroups of order 48, so we discard them immediately. Calculation of the centrally regular subgroups of the remaining automorphism groups eliminated a further 17 matrices. In fact there are only 16 matrices at this order that are cocyclic. It would, however, be tiresome to present all of the centrally regular subgroups for each matrix. We instead give a summary of the information. The largest automorphism group that occurs at order 24 has 760320 elements, a number of matrices have automorphism groups of order 96. One occurrence of note is an automorphism group of order 576 having 9 centrally regular subgroups, which is a high number for such a small group.

We provide a table giving all indexing groups and their respective extensions. We observe that 8 groups of order 24 occur as indexing sets, and that 14 groups of order 48 occur as extension groups.

Indexing Group	Extension Groups
$C_4 \times S_3$	$C_8 \times S_3$
D_{14}	$C_3 \rtimes GQ\,[1]$
$\left(C_2^2 \times C_3\right) \rtimes C_2$	$C_3 \rtimes GQ\,[2]$
$C_3 \times D_4$	$C_3 \times GQ$
S_4	$C_2 \sqsupset S_4$
$C_2 \times A_4$	$C_2 \times SL\,(2,3)$, $SL\,(2,3) \rtimes C_2$
$C_2^2 \times D_3$	$(C_3 \rtimes Q_8) \times C_2$, $\left(C_2^3 \times C_3\right) \rtimes C_2$, $C_{12} \sqsupset C_2^2$, $Q_8 \times D_3$, $(C_4 \times D_3) \rtimes C_2$
$C_2^2 \times C_6$	$C_6 \times Q_8$, $Q_8 \sqsupset C_6$

TABLE 5.2: Indexing groups and extension groups of Hadamard matrices of order 24

There follow presentations of the groups described above in non-unique terms above.

$$
\begin{aligned}
\left(C_2^2 \times C_3\right) \rtimes C_2 &= \left\langle a,b,c,d \mid d^3=1, b^a=bc, d^a=d^2 \right\rangle \\
C_3 \rtimes GQ\,[1] &= \left\langle a,b,c,d,e \mid a^2=c^2=d, b^2=cd, e^3=1, b^a=bc, c^a=cd, e^a=e^2 \right\rangle \\
C_3 \rtimes GQ\,[2] &= \left\langle a,b,c,d,e \mid a^2=b^2=c^2=d, e^3=1, b^a=bc, c^a=cd, c^b=cd, e^a=e^2 \right\rangle \\
C_2 \sqsupset S_4 &= \left\langle a,b,c,d,e \mid a^2=c^2=d^2=e, b^3=1, b^a=b^2, \right. \\
&\qquad \left. c^a=d, c^b=de, d^a=c, d^b=cd, d^c=de \right\rangle \\
SL\,(2,3) \rtimes C_2 &= \left\langle a,b,c,d,e \mid a^2=c^2=d^2=e, b^3=1, c^b=d, d^b=cd, d^c=de \right\rangle \\
(C_3 \rtimes Q_8) \times C_2 &= \left\langle a,b,c,d,e \mid a^2=c^2=d, e^3=1, c^a=cd, e^a=e^2 \right\rangle \\
\left(C_2^3 \times C_3\right) \rtimes C_2 &= \left\langle a,b,c,d,e \mid b^2=d, e^3=1, c^a=cd, e^a=e^2 \right\rangle \\
C_{12} \sqsupset C_2^2 &= \left\langle a,b,c,d,e \mid b^2=d, e^3=1, c^a=cd, c^b=cd, e^a=e^2 \right\rangle \\
(C_4 \times D_3) \rtimes C_2 &= \left\langle a,b,c,d,e \mid b^2=c^2=d, e^3=1, c^a=cd, c^b=cd, e^a=e^2 \right\rangle \\
Q_8 \sqsupset C_6 &= \left\langle a,b,c,d,e \mid c^2=e, d^3=1, b^a=be \right\rangle
\end{aligned}
$$

5.7 Order 28

An analysis similar to that described for order 24 quickly shows that of the 487 matrices of order 28, at most 8 are cocyclic. For two of these matrices, $\texttt{PermAut}(E_H)$ lacks centrally regular subgroups. As a result, precisely 6 Hadamard matrices of order 28 are cocyclic. Furthermore, all these matrices are cocyclic over one of only two groups of order 28, and have expanded designs group developed over one of only two groups of order 56. It is also interesting to note that at this order we find the first minimally cocyclic matrices, that is, a single centrally regular subgroup forms the entire automorphism group. Also at this order we find the first Hadamard matrices with automorphism groups of order 2, that is those that consist only of $\langle(-I,-I)\rangle$. Within the six equivalence classes of matrices, there are two pairs of equivalence classes that are transposes of one another. As stated earlier, these necessarily have isomorphic automorphism groups, and hence are acted upon centrally regularly by the same groups. Thus we need consider only four matrices at this order to complete our classification of the cocyclic Hadamard matrices of order at most 28.

5.7.1 The cocyclic Hadamard matrices of order 28

The first matrix has an automorphism group of order 58968, but has only a single centrally regular subgroup. The presentation of the semidirect product follows at the

Indexing Group	Extension Groups
D_{14}	$C_7 \rtimes Q_8$

end of the section. We observe that the second and third cocyclic Hadamard matrices are transposes of one another and are cocyclic over D_{14}, just as is the first matrix. In their case however, the entire automorphism group is of order 56.

The fourth cocyclic Hadamard matrix of order 28 has an automorphism group of order 8736 and has 4 centrally regular subgroups. Three of these are isomorphic as groups however. As a result, this Hadamard matrix is cocyclic over 2 groups of order 28. The groups in the first line of the table are those described above; it is these groups that appear as three non-permutation-isomorphic centrally regular subgroups in the automorphism group. Note that those in the second line are direct products. The

Indexing Group	Extension Groups
D_{14}	$Q_8 \rtimes C_7$
$C_2^2 \times C_7$	$Q_8 \times C_7$

final pair of cocyclic Hadamard matrices are again transpose equivalent. They have automorphism group of order 336, and are cocyclic over the same two groups as are given in the table above. Note that each group appears as a centrally regular subgroup only once in the automorphism group however.

$$C_7 \rtimes Q_8 : \langle a, b, c, d \mid a^2 = b^2 = c, d^7 = 1, b^a = bc, d^a = d^6 \rangle$$

5.8 Summary of Results

In the following table, we give a summary of the information collected in this chapter. In the second column we list the number of cocyclic Hadamard matrices at that order. Where a fraction appears, the numerator is the number of cocyclic matrices and the denominator is the total. Where a single number appears, it implies that all matrices at that order are cocyclic. In particular, it can be immediately seen from the table that all matrices of order at most 20 are cocyclic. The third column gives the proportion of indexing groups of order n, while the last column gives the proportion of groups of order $2n$ that act regularly on (E_H). The first two columns as far down as order 20 were known

to de Launey by the early 1990's. On page 136 of [1], Horadam comments on this result of de Launey, and poses as a research problem the determination of the proportion of cocyclic Hadamard matrices among all Hadamard matrices for larger orders. The following table provides an answer to this question for orders 24 and 28.

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

TABLE 5.3: Summary of cocyclic equivalence classes of Hadamard matrices

We observe that the even Dihedral groups seem to always occur as indexing groups of Hadamard matrices, though it is a well established result of Ito that Dihedral groups never occur as extension groups. As we observed in our analysis of the groups of order 16, the exponent of a group seems to be somehow related to its likelihood of being a Hadamard group. It is difficult to draw more meaningful information from the above table without access to information on at least the next few terms in each column. In the next chapter, we consider Hadamard matrix constructions that are known to be cocyclic. We use this information to show that there exists a cocyclic Hadamard matrix of order $4t$ for all $t \leq 50$ apart from $t = 47$.

Chapter 6

Cocyclic Hadamard matrix constructions

In this chapter we give summary results of the existence of cocyclic Hadamard matrices at larger orders. We show that many constructions always generate cocyclic Hadamard matrices, and that there is a known cocyclic Hadamard matrix of order n for all suitable $n \leq 184$.

6.1 The Sylvester construction

Sylvester's construction generates Hadamard matrices of order 2^n for all $n \in \mathbb{N}$. The n^{th} Sylvester Hadamard matrix is:

$$\otimes^n \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

As an example, the Sylvester Hadamard matrix of order 8 follows below.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \tag{6.1}$$

The Sylvester Hadamard matrices are closely related to Walsh functions in coding theory. This tensor product construction may be used with any Hadamard matrix of order k to yield Hadamard matrices of order $2^n k$ for any $n \in \mathbb{N}$. Thus to resolve the Hadamard conjecture it is sufficient to search for Hadamard matrices of order $4n$ where n is odd.

6.1.1 Proof of cocyclic property

Lemma 6.1. *$M \otimes N$ is a Hadamard matrix if M and N are both Hadamard matrices.*

Proof. Let A and B be square non-singular matrices, let the determinant of A be a, and the determinant of B be b. Then by elementary linear algebra, $det\,(A \otimes B) = (detA)^b\,(detB)^a$. Recall that a $\{\pm 1\}$-matrix M is Hadamard if and only if $|detM| = m^{m/2}$, where m is the number of rows in M. Then:

$$\begin{aligned} |det\,(M \otimes N)| &= \left(m^{m/2}\right)^n \left(n^{n/2}\right)^m \\ &= m^{mn/2} n^{mn/2} \\ &= (mn)^{mn/2} \end{aligned}$$

□

Lemma 6.2. *The tensor product of cocyclic matrices is cocyclic.*

Proof. Let $\phi_1 \in Z^2\,(G, C)$ and $\phi_2 \in Z^2\,(H, C)$. We define $\phi_1 \otimes \phi_2 : (G \times H) \times (G \times H) \to C$ by

$$\phi_1 \otimes \phi_2\,((g_1, h_1)\,, (g_2, h_2)) = \phi_1\,(g_1, g_2)\,\phi_2\,(h_1, h_2)\,.$$

The cocyclic matrix associated with $\phi_1 \otimes \phi_2$ is the tensor product of the cocyclic matrices associated with ϕ_1 and ϕ_2. This is immediate from the definition of the tensor product of matrices. □

Thus the n^{th} Sylvester Hadamard matrix is cocyclic, by Lemma 6.2 and our verification in Section 4.4.1 that the first Sylvester matrix is indeed cocyclic over C_2.

6.2 The Williamson construction

This construction was first described by Williamson in the early 1940s. Details can be found in [17]. Let A, B, C and D be circulant, or back circulant, matrices of order n satisfying the following equalities:

$$XY^\top = YX^\top \quad \forall X, Y \in \{A, B, C, D\}$$

$$AA^\top + BB^\top + CC^\top + DD^\top = 4nI_n$$

We observe that the first condition is often bypassed by requiring that all component matrices be symmetric. Williamson proves that under these constraints, the above matrices may be composed as follows to give a Hadamard matrix:

$$H = \begin{pmatrix} A & B & C & D \\ B & -A & D & -C \\ C & -D & -A & B \\ D & C & -B & -A \end{pmatrix}$$

The Williamson construction has been the object of much study since Baumert and Golomb's discovery of a Williamson matrix of order 92 in 1962, [18]. This was significant in that it was the last order less then 100 for which no Hadamard matrix was known. It is known that no Williamson matrix with symmetric components of order 35 exists. It is conjectured that there exist Williamson matrices with arbitrary circulant components for all $n \in \mathbb{N}$. Variations upon the Williamson construction have been developed by other authors, notably Goethals and Seidel that relax the above requirements. We shall see in Chapter 7 that such modifications drastically change the cocyclic-development properties of the construction.

6.2.1 Proof of cocyclic property

The proof that the Williamson Hadamard matrices are cocyclic was one of the earliest results in this area. The proof is given in a series of papers by Baliga, de Launey, Flannery and Horadam, beginning in 1993 with [19] and culminating in 2000 with [9]. The argument is based on a detailed analysis of the properties of cocyclic matrices. In particular, any matrix cocyclic developed over a group G may be decomposed into a Hadamard, or componentwise, product: $M = S \bullet P \bullet C$ where S is the tensor product of an all 1's matrix with a backcirculant matrix, P is developed over a coboundary, and C is developed over a commutator cocycle, which is determined by the Schur Multiplicator of G. In essence, the proof generalises Lemma 6.2 to include some simple plug-in constructions. Setting the circulant components to be 1, we observe that the Williamson construction template is cocyclic over C_2^2. Since the input matrices are all circulant of order n, they are cocyclic over C_n. Thus it turns out that a Williamson Hadamard matrix is cocyclic over $C_2^2 \times C_n$. The full argument is given in [20].

We observe also that Williamson matrices are a subset of Ito's type Q matrices, details of which are given in section (6.4). As such the Williamson matrices are also cocyclic over the dihedral group, D_{2p}.

6.3 The Paley construction

As stated above, this construction is based on the quadratic residues of a finite field. Let F be a finite field of order p^a. The quadratic character, χ, of an element of F is defined to be 1 if f is a quadratic residue, and -1 otherwise, in addition, $\chi(0) = 0$. We may form a matrix, Q, of order p^a by

$$Q = [\chi(f_i - f_j)]_{1 \leq i,j \leq p^a}$$

where i, $j \in \{0, 1, 2, \ldots, p^a - 1\}$. We then define the square $p^a + 1$ matrix, S by

$$S = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1}^\top & Q \end{pmatrix}$$

Here, and in all later constructions, $\mathbf{1}$ is the all one's vector of length p^a. The Paley construction consists in fact of two separate constructions, depending on whether $p^a \equiv 3 \mod 4$, or $p^a \equiv 1 \mod 4$. In the first case, we insert Q into the following template:

$$P_{p^a} = \begin{pmatrix} 1 & \mathbf{-1} \\ \mathbf{1} & Q + I_{p^a} \end{pmatrix}$$

and P_{p^a} is Hadamard of order $p^a + 1$. This construction is generally known as Paley Type I. Otherwise, $p^a \equiv 1 \mod 4$, and we use the following template:

$$P'_{p^a} = \begin{pmatrix} S + I_{p^a+1} & S - I_{p^a+1} \\ S - I_{p^a+1} & -S - I_{p^a+1} \end{pmatrix}$$

In this case, P'_{p^a} is a Hadamard matrix of order $2(q+1)$. This is Paley Type II. Although the theory behind these constructions is similar, the standard proofs that they always generate cocyclic matrices are quite different, so we present them separately.

6.3.1 Proof of cocyclic property - Paley Type I

Building on work by Kantor, de Launey and Stafford have completely determined the structure of the Automorphism group of the Paley Type I matrices. Details of this work are given in [21]. The full automorphism group of the Paley matrix derived from the field of order p^a is closely related to the general linear group $GL(2, p^a)$. de Launey and Stafford define $GS(2, p^a)$ to be the subgroup of index 2 of $GL(2, p^a)$, in which all matrices have square determinants. The centre of this group, L, consists of all non-zero multiples of the identity matrix. We denote by Q the subgroup of the centre formed by $\left\{\lambda^2 I | \lambda \in GF(p^a)\right\}$. Note that $|L : Q| = 2$. Now, we consider in particular the action

of $GS\left(2,p^a\right)$ on the elements of $GF\left(p^{2a}\right)$, considered as a vector space of dimension 2 over $GF\left(p^a\right)$. We may then form a group $G\Gamma S\left(2,p^a\right)$ by appending the Frobenius automorphism, $\sigma\left(x,y\right)\mapsto\left(x^p,y^p\right)$, to $GS\left(2,p^a\right)$. Finally, the automorphism group of a Paley Type I Hadamard matrix of order p^a+1 is isomorphic to the quotient group $GS\left(2,p^a\right)/Q$.

The only regular subgroup acting on the expanded design of the Paley Type I matrix of order p^a+1 is the generalised quaternion group, Q_{2p^a+2}. All nontrivial generalised quaternion groups have centre of order 2. This coincides with the central involution of the Automorphism group. Factoring out by this central involution, we see that the Paley Type I Hadamard matrices are cocyclic over the Dihedral groups of appropriate order, and over these groups only. The cases $q=3,7,11,23,59$ are exceptional. In each case, the Hadamard matrix admits some additional regular actions. In all cases they admit the regular action described above, and thus all Paley Type I Hadamard matrices are cocyclic.

6.3.2 Proof of cocyclic property - Paley Type II

The following elementary proof, due originally to Turyn, is taken from a paper on cocyclic Hadamard matrices and difference sets by De Launey, Flannery and Horadam, [9]. It relies on the fact that Williamson Hadamard matrices are cocyclic, and that the matrix Q given above is Hadamard equivalent to a matrix of the form:

$$Q'=\begin{pmatrix} A & B \\ B & -A \end{pmatrix}$$

where A and B are symmetric circulant matrices. A has 0's on the main diagonal, and ±1 everywhere else, and B is a ±1 matrix. Now with this observation, the Paley Type

II matrix may be rewritten as follows:

$$
\begin{aligned}
P_{p^a} &= \begin{pmatrix} I+C & I-C \\ I-C & -I-C \end{pmatrix} \\
&= \begin{pmatrix} I+A & B & I-A & -B \\ B & -I-A & -B & I+A \\ I-A & -B & -I-A & -B \\ -B & I+A & -B & -I+A \end{pmatrix} \\
&\approx_H \begin{pmatrix} I+A & I-A & B & B \\ -I+A & I+A & -B & B \\ -B & B & I+A & -I+A \\ -B & -B & I-A & I+A \end{pmatrix}
\end{aligned}
$$

Now, $I+A$, $I-A$, and B are all symmetric circulant matrices. Inspection shows that this matrix is in fact in the form of a Williamson Hadamard matrix. Thus all Paley Type II matrices are of Williamson type, and as such are cocyclic over both $C_2^2 \times C_{p^a/2}$ and the dihedral group D_{2t}.

6.4 The Ito Type Q matrices

In the early 1990s Ito began investigating what he termed Hadamard groups, which are groups of order $8t$ containing a central relative difference set with parameters $(4t, 2, 4t, 2t)$. As we demonstrated in Section 4.6, the existence of these difference sets is equivalent to the existence of a cocyclic Hadamard matrix. The Paley Type II Hadamard matrices have already been shown to be a subset of the Williamson Hadamard matrices. Ito's Type Q construction weakens some of the conditions on the component matrices of the Williamson construction to give a larger family of matrices. This construction includes also Paley Type I matrices. In all cases, the expanded design of the Hadamard matrix in question is shown to be group developed over the group

$$Q_{8w} = \left\langle a, b \mid a^{4w} = b^4 = 1, a^{2w} = b^2, a^b = a^{-1} \right\rangle$$

The forbidden subgroup in all cases is $\left\langle b^2 \right\rangle$ and the quotient $Q_{8w}/\left\langle b^2 \right\rangle$ is D_{2t}. We do not attempt to give a proof of Ito's results, referring the reader instead to a series of papers by Ito. Type Q matrices are introduced in [7]. The Paley constructions are shown to be of this type in [22]. Further results are contained in a number of papers by Ito on the subject, notably the other papers in the series *On Hadamard Groups* and in [23].

6.4.1 The Golay construction

The Golay construction is another example of a Type Q construction. It relies on the existence of a pair of Golay sequences of length n. Such sequences are described in detail, and some existence results are given by Golay in [24]. These are a pair of sequences $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_n)$ such that the sum of their autocorrelation functions, $R(A)$ and $R(B)$ is the zero vector. The i^{th} entry of $R(A)$ is given by the sum:

$$\sum_{k=1}^{n-i} a_k a_{k+i}$$

In this application we are interested in complex Golay sequences, that is sequences in which all entries of A and B come from $\{\pm 1, \pm i\}$. Define $A = W + iX$, $B = Y + iZ$, where W, X, Y and Z are $\{0, \pm 1\}$ sequences. Then we form four circulant matrices with the following initial rows: $A_1 = W + X$, $A_2 = W - X$, $B_1 = Y + Z$ and $B_2 = Y - Z$. Holzmann and Karaghani, in [25] have shown that these matrices satisfy the conditions for Ito's Type Q construction. Thus Golay Hadamard matrices belong also to Ito's Type Q, and as such are cocyclic over D_{2t}.

6.5 Existence of cocyclic Hadamard matrices

We showed in Chapter 5 that all Hadamard matrices of order at most 20 were cocyclic. In the following table we give some existence results for larger orders. In particular, we show that a cocyclic Hadamard matrix of order $4t$ exists for $t \leq 7$. We now expand this result.

Several different constructions may give cocyclic Hadamard matrices at any given order. We have given preference to the Sylvester and Paley constructions, as they generate unique matrices at each of the orders for which they exist. Where a product of two numbers is given, the tensor product of cocyclic Hadamard matrices of these orders can be taken. Details of the Williamson matrices of the orders listed above are given in [26], pages 160-162. Currently the smallest order for which the existence of a cocyclic Hadamard matrix is unknown appears to be 188.

Matrix order	Construction	Matrix order	Construction
4	Sylvester	104	Paley I
8	Sylvester	108	Paley I
12	Paley I	112	4×28
16	Sylvester	116	Williamson
20	Paley I	120	2×60
24	Paley I	124	Paley II
28	Paley I	128	Sylvester
32	Sylvester	132	Paley I
36	Paley II	136	2×68
40	2×20	140	Paley I
44	Paley I	144	2×72
48	Paley I	148	Paley II
52	Paley II	152	Paley I
56	2×28	156	Williamson
60	Paley I	160	2×80
64	Sylvester	164	Paley I
68	Paley I	168	Paley I
72	Paley I	172	Williamson
76	Paley II	176	4×44
80	Paley I	180	Paley I
84	Paley I	184	2×92
88	2×44	188	Unknown
92	Williamson	192	Paley I
96	2×48	196	Paley II
100	Paley II	200	Paley I

TABLE 6.1: Existence of cocyclic Hadamard matrices

Chapter 7

Non-cocyclic Hadamard matrix constructions

In the previous chapter, we examined some constructions that are known always to give cocyclic Hadamard matrices. We now investigate some constructions for Hadamard matrices which may not be cocyclic. This work is prompted by the research questions numbered 39-42 posed in Chapter 6 of [1]. We wish to distinguish between Hadamard matrix constructions that always produce cocyclic matrices, constructions which produce a mixture of cocyclic and non-cocyclic matrices and constructions which never produce cocyclic matrices. In this chapter we will refer to constructions of the first type as *strongly cocyclic*, the second type as *weakly cocyclic*, and the third type as *non-cocyclic*.

7.1 The Goethals-Seidel Construction

The Goethals-Seidel construction, described originally in [27], takes as its input 4 circulant $\{\pm 1\}$-matrices of odd order n, normally labeled A, B, C and D, which satisfy the condition:

$$AA^\top = BB^\top = CC^\top = DD^\top = 4nI_n \tag{7.1}$$

The back diagonal matrix of order n is denoted by R. A GS-Hadamard matrix of order $4n$ may then be constructed in the following manner:

$$\begin{pmatrix} A & BR & CR & DR \\ -BR & A & D^\top R & -C^\top R \\ -CR & -D^\top R & A & B^\top R \\ -DR & C^\top R & -B^\top R & A \end{pmatrix} \tag{7.2}$$

If A, B, C and D are all symmetric, then this construction is identical to the Williamson construction. There are several orders for which a GS-Hadamard matrix exists, but for which it has been shown that no Williamson Hadamard matrix exists.

7.1.1 Order 28

There are 128 distinct ± 1 vectors of length 7. We may form one circulant matrix from each of these. With no restrictions on the circulant matrices, A, B, C and D, there are $5,378,240$ solutions to (7.1). Since there are only 487 Hadamard matrices of order 28, it is obvious that many of these solutions give Hadamard equivalent matrices. Thus we impose some restrictions on our parameters.

We discard J and $-J$ from our set of circulant matrices, since they will never occur in a Hadamard matrix. Then there are precisely 9 Hadamard inequivalent circulant matrices of order 7, since every nontrivial matrix is Hadamard equivalent to 14 other circulant matrices. We restrict our search for solutions to these 9 matrices. By this method, we found exactly two GS-Hadamard matrices of order 28. They are generated by the following sequences:

$$(1,1,1,1,1,1,-1),(1,1,1,1,-1,-1,-1),(1,1,-1,1,1,-1,-1),(1,1,-1,1,-1,1,-1)$$
$$(1,1,1,1,1,-1,-1),(1,1,1,1,-1,1,-1),(1,1,1,-1,1,1,-1),(-1,-1,-1,1,-1,1,1)$$

The first of these matrices has an automorphism group of order 48. The second has an automorphism group of order 24. It follows immediately that there is no cocyclic Goethals-Seidel-Hadamard matrix of order 28, and that this construction is not strongly cocyclic.

7.1.2 Larger orders

We undertook a partial search for GS-Hadamard matrices at larger orders. Our results are given below.

Order	Matrices
28	2
36	15
44	105
52	1305

TABLE 7.1: Goethals-Seidel Hadamard matrices

None of the matrices found were cocyclic; in fact only a single matrix even had a sufficiently large automorphism group to make searching for regular subgroups necessary.

Thus we have partially answered Horadam's Problem 40, at least for the strong cocyclic property and we provide strong evidence that there is no cocyclic Hadamard matrix of Goethals-Seidel type of order ≤ 52. It seems reasonable to conjecture that the Goethals-Seidel construction never generates cocyclic Hadamard matrices for orders greater than or equal to 28.

Conjecture: *The Goethals-Seidel construction is non-cocyclic.*

7.2 Two circulant cores construction

This construction, due to Fletcher, Gysin and Seberry and described in [28], uses a pair of circulant matrices as the basis for a Hadamard matrix, instead of using four, as the Goethals-Seidel and Williamson constructions do. The construction requires a pair of circulant matrices, A and B, of odd order l such that

$$AA^\top + BB^\top = (2l+2)\, I_l - 2J_l$$

where I_l is the identity matrix of order l and J_l is the all $+1$ matrix of order l. If this condition is satisfied, then

$$\begin{pmatrix} -1 & -1 & \mathbf{1} & \mathbf{1} \\ -1 & 1 & \mathbf{1} & \mathbf{-1} \\ \mathbf{1}^\top & \mathbf{1}^\top & A & B \\ \mathbf{1}^\top & \mathbf{-1}^\top & B^\top & -A^\top \end{pmatrix} \tag{7.3}$$

is a Hadamard matrix, where $\mathbf{1}$ represents an all-1's row vector of length l. It is conjectured by Seberry et al. in [3] that TCC-Hadamard matrices exist at every order $4n$. Since all Hadamard matrices of order at most 20 are known to be cocyclic, we began our investigation with the TCC matrices of order 24.

7.2.1 Orders investigated

We observe that by negating the first two columns of a TCC Hadamard matrix, we obtain an equivalent matrix in which the first row consists entirely of positive entries and A and B are unchanged. Since the matrix is orthogonal, we obtain constraints on the row sums of the component matrices. In particular, for any row we have that:

$$\sum_{j=1}^{l} a_{i,j} = \sum_{j=1}^{l} b_{i,j} = 1.$$

This greatly reduces the number of matrices that we must iterate over in our searches. For small orders we did a complete search for solutions. Our results follow below.

l	Matrix order	Number of matrices	Number of cocyclic matrices
11	24	3	3
13	28	4	2
15	32	13	1
17	36	11	1
19	40	17	2

TABLE 7.2: Twin circulant cores Hadamard matrices

Our results at order 28 proved to be typical. We observe that two of the Hadamard matrices were cocyclic, and that two were not. It is interesting that the orders of the automorphism groups seem to vary widely and unpredictably. In this case the largest automorphism group had order 58968, the smallest only order 52. It is notable that all have a subgroups of order 13. The twin circulant cores construction has the weak cocyclic property for all orders investigated. This result may be regarded as a partial solution to Horadam's Problem 42.

7.3 Twin prime power difference set construction

This construction, described in [1], and due originally to Paley, is loosely related to both the Paley Type I and Type II matrices, being also based on the quadratic residue characters of finite fields. If k and $k+2$ are prime powers, then there exists a difference set with parameters $2-(k(k+2), [k(k+2)-1]/2, [k(k+2)-3]/4)$ in the direct product of the additive groups $(GF(k), +) \times (GF(k+2), +)$. The elements of this difference set are all elements of the form $(g, 0), g \in GF(k)$ or $(g, h), g \in GF(k), h \in GF(k+2)$ where $\chi(g)\chi(h) = 1$ and χ is the standard quadratic residue. We observe that this difference set has the parameters of a Hadamard 2-design. Recall that we described a method in Section 1.3 to obtain a Hadamard matrix from a 2-design.

7.3.1 Orders at which TPP-Hadamard matrices exist

Let $k-1$ and $k+1$ be prime powers. Then we can generate a unique Hadamard matrix of order $(k-1)(k+1)+1 = k^2$ by the twin prime power construction. Thus TPP Hadamard matrices occur only at square orders. In the table below we provide a list of all twin prime powers that generate Hadamard matrices of order at most 1000.

Our computation has shown that the smallest TPP-Hadamard matrix, of order 16, is equivalent to the Sylvester matrix of order 16, and thus is cocyclic. Note that by

Twin prime powers	Matrix order	Order of Automorphism Group
3, 5	16	10321920
5, 7	36	840
7, 9	64	6048
9, 11	100	15840
11, 13	144	17160
17, 19	324	93024
23, 25	576	607200
25, 27	676	2527200
27, 29	784	1710072
29, 31	900	755160

TABLE 7.3: Twin prime powers

our classification in Chapter 5 that all Hadamard matrices of order 16 are cocyclic. Examination of the orders of the automorphism groups of the matrices of larger orders shows that they cannot be cocyclic. This is a surprising result, as the Paley constructions generate only cocyclic Hadamard matrices in a similar fashion from prime powers. We observe however that the order of the automorphism group of the matrix generated by the prime powers k and $(k+2)$ is divisible by $k\,(k+1)\,(k+2)$. A study of the subgroup structure of the automorphism group may provide a proof that this construction does not generate cocyclic Hadamard matrices. We provide a copy of the Magma code that we used to generate these twin prime power matrices in Appendix B. In any case, we have proved that apart from order 16, which we consider exceptional, the twin prime power Hadamard construction is non-cocyclic for all orders less then 1000. This provides at least a partial answer to Horadam's Problem 39: this construction is not strongly cocyclic and furthermore, is non-cocyclic for all orders less then 1764. We make the following conjecture:

Conjecture: *The twin prime power construction is non-cocyclic.*

7.4 Kimura construction

Kimura's construction, described in [29], is notable in that it yields a Hadamard matrix of order $8n+4$, where n is odd, from an ordered set of four $\{0,1\}$-matrices of order $2n$ that satisfy certain conditions. As we have previously noted, it is sufficient to prove the existence of Hadamard matrices at all orders $4n$ for odd n to prove the Hadamard conjecture, as all other orders may be obtained from these via the Sylvester construction. Kimura's construction produces a $(0,1)$-matrix, we obtain a Hadamard matrix from this simply by replacing 0 with -1 wherever it occurs. The template for the Kimura

construction is as follows:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\
1 & 1 & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\
1 & 0 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\
1 & 0 & 0 & 1 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\
\mathbf{1}^\top & \mathbf{1}^\top & \mathbf{1}^\top & \mathbf{0}^\top & A & B & C & D \\
\mathbf{1}^\top & \mathbf{1}^\top & \mathbf{0}^\top & \mathbf{1}^\top & \widetilde{B} & A & D & \widetilde{C} \\
\mathbf{1}^\top & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{1}^\top & \widetilde{C} & \widetilde{D} & A & B \\
\mathbf{1}^\top & \mathbf{0}^\top & \mathbf{0}^\top & \mathbf{0}^\top & D & \widetilde{C} & B & \widetilde{A}
\end{pmatrix}$$

Where $\widetilde{A}$ is the complement of A, this will be clarified below in our discussion of the component matrices. First however, we observe that the above template produces a Hadamard matrix if and only if the component matrices satisfy the following equations:

$$\begin{aligned}
A^\top A + B^\top B + C^\top C + D^\top D &= (2n+1)\, I + (2n-2)\, J \\
A\widetilde{B}^\top + BA^\top + CD^\top + D\widetilde{C}^\top &= (2n-1)\, J \\
A\widetilde{C}^\top + CA^\top + BD^\top + D\widetilde{B}^\top &= (2n-1)\, J \\
D\widetilde{A}^\top + AD^\top + CB^\top + B\widetilde{C}^\top &= (2n-1)\, J.
\end{aligned}$$

The matrices above are not necessarily circulant, though they are required to have constant row-sum. In particular we require that A have constant row sum $n-1$, and that the remaining matrices have row sum n. A y-invariant subset of a group G, for some $y \in G$, is a subset K that satisfies $yKy = K$. Kimura and Niwasaki demonstrate in [29] that y-invariant subsets of D_n, where n is odd, satisfying the first property above automatically satisfy the remaining three. Thus it is in Dihedral groups that we search for solutions. On finding such a subset in D_n, we take a regular degree $2n$ matrix representation of the group, and add the matrices that belong to K. If K gives rise to the matrix A then the complement of K in G gives rise to $\widetilde{A}$. After construction of all y invariant subsets of a Dihedral group, searching for Hadamard matrices is equivalent to searching for solutions of the first equation above.

7.4.1 Orders at which Kimura matrices exist

n	Matrix order	Number of matrices	Order of Automorphism Group
5	44	1	160
7	60	8	224
9	76	8	288

TABLE 7.4: Kimura Hadamard matrices

We carried out comprehensive searches for Kimura matrices generated from Dihedral groups of small orders. Our data is summarised in the table above. Note that, by the orders of the automorphism groups, none of the Kimura matrices generated are cocyclic. We observe that for a Kimura matrix of order $8n + 4$, the automorphism group is of order $32n$. We conjecture that this is the case for all Kimura Hadamard matrices. If this is so, then this construction will never generate cocyclic Hadamard matrices. Thus we have partially answered Horadam's Problem 41: we have shown that the Kimura construction is not strongly cocyclic. Furthermore when restricted to Dihedral groups, as described by Kimura and Niwasaki, the construction is non-cocyclic for orders ≤ 76. For this construction we give a somewhat stronger conjecture:

Conjecture: *Let H be a Kimura Hadamard matrix of order $8n + 4$. Then its automorphism group has order $32n$.*

Proof of this conjecture would of course imply a negative answer to Horadam's problem.

Appendix A

Testing for cocyclic development

Here we provide a series of Magma programs that determine the cocyclic development properties of a Hadamard matrix. The theory supporting this appendix may be found in Chapter 4. The procedure `IsCocyclic` calls `AssociatedDesign` which in turn calls `ExpandedDesign`. Otherwise, we make use of existing Magma functions. Note that we do not calculate the automorphism group of a Hadamard matrix explicitly, but rather calculate the automorphism group of the associated design, which is isomorphic by Theorem 4.10. Magma's inbuilt function for calculating regular subgroups only checks that they act regularly on the points of a design. We check that all blocks lie in a single orbit also. These are reported as regular subgroups. Our proofs require also that the regular subgroups contain the central involution $\langle\zeta\rangle$; we test all regular subgroups for this property and return the number of centrally regular subgroups. This gives us the information we require about the cocyclic development properties of a Hadamard matrix. This procedure was used to compute the data given in Chapter 5, and to check that the matrices produced in Chapter 7 were not cocyclic. Our procedure also investigates our conjecture that the equality given in (4.3) holds for all cocyclic Hadamard groups. In the case that it is found to fail, the procedure will produce an error message. This can be circumvented by changing the definition of c to be the central involution $\langle\zeta\rangle$.

```
ExpandedDesign := function(H); \\
    z := Integers(); \\
    n := NumberOfRows(H);\\
    B := MatrixAlgebra(z, 2)![1,-1,-1,1];\\
  return TensorProduct(B,H);\\
end function;\\

AssociatedDesign := function(H);
    EH := ExpandedDesign(H);
    n := NumberOfRows(EH);
      for i in [1..n] do;
        for j in [1..n] do;
            EH[i,j] := (EH[i,j] + 1) / 2;
        end for;
      end for;
```

```
  return EH;
end function;


IsCocyclic := procedure(H);
    AH := AssociatedDesign(H);
    n := NumberOfRows(AH);
    d := IncidenceStructure<n|AH>;
    p := Points(d);
    b := Blocks(d);
    aut := AutomorphismGroup(d);
    c := Centre(aut);

    print "Order of automorphism group:", #(aut);
    print "Automorphism group has centre of order:", #c;

    reg := RegularSubgroups(aut);
    m := #(reg);
    reg1 := [];

      for i in [1..m] do;
          reg1 := Append(reg1, reg[i]`subgroup);
      end for;

    A := [];
    B := [];

    for i in [1..m] do;
        if #(p[1]^reg1[i]) eq n then
            if #(b[1]^reg1[i]) eq n then
                A := Append(A, reg1[i]);
            end if;
        end if;
    end for;

    q := #(A);

    print "Number of regular subgroups:", q;

    for i in [1..q] do;
        if c subset A[i] then
            B := Append(B, A[i]);
        end if;
    end for;

    r := #B;
    print "Number of centrally regular subgroups:", r;

    C := [];
```

```
    for i in [1..r] do;
        C := Append(C, (B[i]/c));
    end for;

    print "Expanded design is group developed
              /Matrix is cocyclic over the following groups:";

    for i in [1..r] do;
        IdentifyGroup(B[i]), IdentifyGroup(C[i]);
    end for;
end procedure;
```

Appendix B

Hadamard matrix constructions

In this Appendix we give some of the code that we used to derive the results of Chapter 7. In particular, we provide programs to construct Hadamard matrices of Kimura type, as well as Twin Prime Power Hadamard matrices. These are the more intricate of the programs that we wrote in preparing the material of Chapter 7. Many of the methods for the construction Two circulant cores Hadamard matrices and Goethals-Seidel Hadamard matrices may be seen here also. We give only the code itself with minimum additions in this Appendix, the reader is directed to Chapter 7 for details of the constructions.

B.1 Kimura construction

The main function here is `KimuraMatrices`, which takes a Dihedral group as its argument. It calls `KimuraComponentMatrices` twice to produce component matrices with appropriate parameters. It selects all 4-subsets of matrices that satisfy the necessary equation, then uses `KimuraStructure` to form the relevant Hadamard matrices. `RegularRep` and `ElementRep` together give a simple method of finding a permutation representation of a group. They are called by `KimuraComponentMatrices`. All other functions are inbuilt in Magma.

```
yInvariants := function(n, G, y); //Constructs n-element y-Invariant subsets
    n := Integers()!n;
    m := Order(G);
    f := NumberingMap(G);
    g := Inverse(f);
    A := Subsets({1..m}, n);
    B := [];
    for i in A do;
        B := Append(B, SetToSequence(i));
    end for;
    B := g(B);
    C := B;
    p := #B;
    for i in [1..p] do;
        for j in [1..n] do;
```

```
            C[i,j] := y*C[i,j]*y;
        end for;
    end for;
    D := [];
    for i in [1..p] do;
        if C[i] subset B[i] then;
            D := Append(D, B[i]);
        end if;
    end for;
  return D;
end function;

ElementRep := function(a, G); //Constructs a permutation matrix from a
    B := [];      //group element, note that it is not normalised
    for i in G do;
        for j in G do;
            if i*j eq a then;
                B := Append(B, 1);
            else;
                B := Append(B, 0);
            end if;
        end for;
    end for;
  return Matrix(Order(G), B);
end function;

RegularRep := function(G);    //Computes a matrix representation of a group
    z := ElementRep(Identity(G), G)^-1;
    B := [];
    for x in G do;
        B := Append(B, ElementRep(x, G)*z);
    end for;
  return MatrixGroup<Order(G),Integers()|B>;
end function;

KimuraComponentMatrices := function(k, G);
    z := Generators(G);   //We find a suitable y to create Invariant subsets
    for i in z do;
        if Order(i) eq 2 then;
            b := i;
        end if;
    end for;

    A := yInvariants(k, G, b);
    a := #A;
    h1, h2 := IsIsomorphic(G, RegularRep(G)); // h2 is a homomorphism
    A1 := [];           //from G to its matrix representation
    for i in [1..a] do;
        Z := Matrix(h2(A[i,1]));    //We add the matrix reps of the elements
        for j in [2..k] do;   //to form the required Kimura components
```

```
            Z := Z + Matrix(h2(A[i,j]));
        end for;
        A1 := Append(A1, Z);
    end for;
  return A1;
end function;

KimuraStructure := function(A,B,C,D); //This function takes the components and
    n := NumberOfRows(A);     //inserts them into the template
    A1 := ZeroToOne(A);
    B1 := ZeroToOne(B);
    C1 := ZeroToOne(C);
    D1 := ZeroToOne(D);
    R1 := HorizontalJoin([A, B, C, D]);
    R2 := HorizontalJoin([B1, A, D, C1]);
    R3 := HorizontalJoin([C1, D1, A, B]);
    R4 := HorizontalJoin([D, C1, B, A1]);
    Core := VerticalJoin([R1, R2, R3, R4]);
    j0 := [];
    j1 := [];
    for i in [1..n] do;
        j0 := Append(j0, 0);
        j1 := Append(j1, 1);
    end for;
    r1 := j1 cat j1 cat j0 cat j0;
    r2 := j1 cat j0 cat j1 cat j0;
    r3 := j0 cat j1 cat j1 cat j0;
    c1 := [1,0,0] cat r1;
    c2 := [0,1,0] cat r2;
    c3 := [0,0,1] cat r3;
    S1 := Vector(r1);
    S2 := Vector(r2);
    S3 := Vector(r3);
    V := VerticalJoin(S3, Core);
    V1 := VerticalJoin(S2, V);
    V2 := VerticalJoin(S1, V1);
    T1 := Matrix(4*n+3, 1, c1);
    T2 := Matrix(4*n+3, 1, c2);
    T3 := Matrix(4*n+3, 1, c3);
    V3 := HorizontalJoin(T3, V2);
    V4 := HorizontalJoin(T2, V3);
    H := HorizontalJoin(T1, V4);
    M := AdjoinBorder(H);
    M1 := M - ZeroToOne(M);
  return M1;
end function;

KimuraMatrices := function(G);
    n := Order(G);
    a := n/2-1;   //These are the parameters given
```

```
    b := n/2;     //in the construction.
    E := [];
    F := [];
    A := KimuraComponentMatrices(a, G);
    B := KimuraComponentMatrices(b, G);
    p := #A;
    q := #B;
    J := [2*n-1];
    for i in [2..n] do;
        J := Append(J, n-2);
    end for;
    I := Circulant(J);
    for i in [1..p] do;
        for j in [1..q] do;
            for k in [j..q] do;
                for l in [k..q] do;
                    if A[i]*Transpose(A[i]) + B[j]*Transpose(B[j]) +
                     B[k]*Transpose(B[k]) + B[l]*Transpose(B[l]) eq I then;
                          E := Append(E, [A[i], B[j], B[k], B[l]]);
                    end if;
                end for;
            end for;
        end for;
    end for;
    e := #E;
    for i in [1..e] do;
        F:= Append(F, KimuraStructure(E[i,1], E[i,2], E[i,3], E[i,4]));
    end for;
  return F;
end function;
```

B.2 TPP construction

The main function here is `TPPMatrix`, which takes as its arguments a pair of twin prime powers. It generates the Galois fields for each of these prime powers. Then for each field, it forms an elementary Abelian group isomorphic to the additive group of the field, and creates an isomorphism between this and the respective additive group. The group G is formed from the direct sum of the two elementary Abelian groups. This is necessary as Magma does not allow any such operations on subgroups of a finite field. Quadratic residues and non-residues are determined in each field, using the functions `Squares` and `NonSquares`, and mapped into G using the isomorphisms mentioned previously and canonical inclusion maps. As per the construction, we form the Hadamard difference set as a series of products of elements from the two subgroups. We then iterate over a multiplication table of the group, in list form, to create the core of the Hadamard matrix. The function `AdjoinBorder` adds a row and column of 1's, producing a Hadamard matrix, as required by the construction.

```
AdjoinBorder := function(M);
    n := NumberOfRows(M);
    a := [];
    b := [1];
    for i in [1..n] do;
        a := Append(a, 1);
        b := Append(b, 1);
    end for;
    a1 := Matrix(1, n, a);
    b1 := Matrix(n+1, 1, b);
    M1 := VerticalJoin(a1, M);
    M2 := HorizontalJoin(b1, M1);
  return M2;
end function;

Squares:= function(GF);
    A := [];
    for i in GF do;
        if IsZero(i) eq false then;
            if IsSquare(i) eq true then;
                A := Append(A, i);
            end if;
        end if;
    end for;
  return A;
end function;

NonSquares := function(GF);
    A := [];
    for i in GF do;
        if IsSquare(i) eq false then;
            A := Append(A, i);
        end if;
    end for;
  return A;
end function;


AppendSum := function(X, I, J);
    for i in I do;
        for j in J do;
            X := Append(X, i+j);
        end for;
    end for;
  return X;
end function;

TPPMatrix := function(p,q);
    GFp := GF(p);
```

```
GFq := GF(q);
p1 := Factorization(p)[1,1];    //The characteristic of GFp
q1 := Factorization(q)[1,1];
Ap, phi := AdditiveGroup(GFp);
Aq, psi := AdditiveGroup(GFq);
Phi := Inverse(phi);      // A map from (GFp, +) to GFp
Psi := Inverse(psi);

G := DirectSum(Ap, Aq);   // The group over which we develop the H-matrix
Gp := SylowSubgroup(G, p1);   //A subgroup isomorphic to GFp
Gq := SylowSubgroup(G, q1);
a, alpha := IsIsomorphic(Ap, Gp);
b, beta := IsIsomorphic(Aq, Gq);

Sp := Squares(GFp);
Spi := Phi(Sp);       //We coerce the squares into (GFp, +)
Spii := alpha(Spi);   //We coerce the squares into a subgroup of G
NSp := NonSquares(GFp);
NSpi := Phi(NSp);
NSpii := alpha(NSpi);   //We coerce the non squares into a subgroup of G

Sq := Squares(GFq);
Sqi := Psi(Sq);
Sqii := beta(Sqi);
NSq := NonSquares(GFq);
NSqi := Psi(NSq);
NSqii := beta(NSqi);


I := [];
J := [];
for i in Spii do;
    I := Append(I, G!i);    // We coerce the squares into G itself
end for;
for i in Sqii do;
    J := Append(J, G!i);
end for;

K := [];
L := [];
for i in NSpii do;
    K := Append(K, i);    //We coerce the non squares into G itself
end for;
for i in NSqii do;
    L := Append(L, i);
end for;

X := [];    //We form the list of elements described in the construction
X := AppendSum(X, I, J);
X := AppendSum(X, K, L);
```

```
    for i in Gp do;
        X := Append(X, i);
    end for;

    Z := [];
    for i in G do;
        for j in G do;    //We iterate over a Cayley table of G
            if i+j in X then;   // to form the required matrix
                Z := Append(Z, 1);
            else;
                Z := Append(Z, -1);
            end if;
        end for;
    end for;

    TPPcore := Matrix(p*q, p*q, Z);
    TPPmatrix := AdjoinBorder(TPPcore); //We adjoin a border of +1's
    return TPPmatrix;
end function;
```

Bibliography

[1] K. J. Horadam. *Hadamard matrices and their applications*. Princeton University Press, Princeton, NJ, 2007. ISBN 978-0-691-11921-2; 0-691-11921-X.

[2] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system. i. the user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[3] Ilias S. Kotsireas, Christos Koukouvinos, and Jennifer Seberry. Hadamard ideals and Hadamard matrices with two circulant cores. *European J. Combin.*, 27(5): 658–668, 2006. ISSN 0195-6698.

[4] D. R. Hughes and F. C. Piper. *Design theory*. Cambridge University Press, Cambridge, 1985. ISBN 0-521-25754-9.

[5] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *J. Combin. Des.*, 13(6):435–440, 2005. ISSN 1063-8539.

[6] Dean Crnković. A series of regular Hadamard matrices. *Des. Codes Cryptogr.*, 39 (2):247–251, 2006. ISSN 0925-1022.

[7] Noboru Ito. On Hadamard groups. *J. Algebra*, 168(3):981–987, 1994. ISSN 0021-8693.

[8] D. L. Flannery. Cocyclic Hadamard matrices and Hadamard groups are equivalent. *J. Algebra*, 192(2):749–779, 1997. ISSN 0021-8693.

[9] 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. ISSN 0166-218X. Coding, cryptography and computer security (Lethbridge, AB, 1998).

[10] Derek John Scott Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982. ISBN 0-387-90600-2.

[11] Iain T. Adamson. *Elementary rings and modules*. Barnes & Noble Books [A division of Harper & Row, Publishers, Inc.], New York, 1972. University Mathematical Texts.

[12] William P. Orrick. Switching operations for Hadamard matrices. *SIAM J. Discrete Math.*, 22(1):31–50, 2008. ISSN 0895-4801.

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

[14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.10*. http://www.gap-system.org, 2007.

[15] M. Röder. *RDS, Version 1.0*. http://www.maths.nuigalway.ie/ roeder/rds, 2008.

[16] Petteri Kaski and Patric R. J. Östergård. *Classification algorithms for codes and designs*, volume 15 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006. ISBN 978-3-540-28990-6; 3-540-28990-9. With 1 DVD-ROM (Windows, Macintosh and UNIX).

[17] John Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 11:65–81, 1944. ISSN 0012-7094.

[18] Solomon W. Golomb and Leonard D. Baumert. The search for Hadamard matrices. *Amer. Math. Monthly*, 70:12–17, 1963. ISSN 0002-9890.

[19] K. J. Horadam and W. de Launey. Cocyclic development of designs. *J. Algebraic Combin.*, 2(3):267–290, 1993. ISSN 0925-9899.

[20] A. Baliga and K. J. Horadam. Cocyclic Hadamard matrices over $Z_t \times Z_2^2$. *Australas. J. Combin.*, 11:123–134, 1995. ISSN 1034-4942.

[21] Warwick de Launey and Richard M. Stafford. On cocyclic weighing matrices and the regular group actions of certain Paley matrices. *Discrete Appl. Math.*, 102(1-2):63–101, 2000. ISSN 0166-218X. Coding, cryptography and computer security (Lethbridge, AB, 1998).

[22] Noboru Ito. On Hadamard groups. III. *Kyushu J. Math.*, 51(2):369–379, 1997. ISSN 1340-6116.

[23] Noboru Ito. Remarks on Hadamard groups. *Kyushu J. Math.*, 50(1):83–91, 1996. ISSN 1340-6116.

[24] Marcel J. E. Golay. Complementary series. *IRE Trans.*, IT-7:82–87, 1961.

[25] W. H. Holzmann and H. Kharaghani. A computer search for complex Golay sequences. *Australas. J. Combin.*, 10:251–258, 1994. ISSN 1034-4942.

[26] A. S. Hedayat, N. J. A. Sloane, and John Stufken. *Orthogonal arrays*. Springer Series in Statistics. Springer-Verlag, New York, 1999. ISBN 0-387-98766-5. Theory and applications, With a foreword by C. R. Rao.

[27] J.-M. Goethals and J. J. Seidel. Orthogonal matrices with zero diagonal. *Canad. J. Math.*, 19:1001–1010, 1967. ISSN 0008-414X.

[28] Roderick J. Fletcher, Marc Gysin, and Jennifer Seberry. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices. *Australas. J. Combin.*, 23:75–86, 2001. ISSN 1034-4942.

[29] Hiroshi Kimura and Takashi Niwasaki. Some properties of Hadamard matrices coming from dihedral groups. *Graphs Combin.*, 18(2):319–327, 2002. ISSN 0911-0119.