Automorphisms of Pairwise Combinatorial Designs

Padraig Ó Catháin

December 15, 2011

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
School of Mathematics, Statistics and Applied Mathematics
The National University of Ireland, Galway
Supervised by Dr. Dane Flannery

Contents

Abstract

In this thesis, we investigate group actions on certain families of pairwise combinatorial designs, in particular Hadamard matrices and symmetric 2-$(4t-1, 2t-1, t-1)$ designs.

A Hadamard matrix H is called cocyclic if a certain quotient of the automorphism group contains a subgroup acting regularly on the rows and columns of H. Cocyclic Hadamard matrices (CHMs) were first investigated by de Launey and Horadam in the early 1990s.

We develop an algorithm for constructing all CHMs of order $4t$ based on a known relation between CHMs and relative difference sets. This method is then used to produce a classification of all CHMs of order less than 40. This is an extension and completion of work of de Launey and Ito.

Non-affine groups acting doubly transitively on a Hadamard matrix have been classified by Ito. Implicit in this work is a list of Hadamard matrices with non-affine doubly transitive automorphism group. We give this list explicitly, in the process settling an old research problem of Ito and Leon.

We then use our classification to show that the only cocyclic Hadamard matrices with non-affine automorphism group are those that arise from the Paley Hadamard matrices. As a corollary of this result, we show that twin prime power difference sets and Hall sextic residue difference sets each give rise to a unique CHM.

If H is a CHM developed from a difference set then the automorphism group of H is doubly transitive. We classify all difference sets which give rise to Hadamard matrices with non-affine doubly transitive automorphism group. A key component of this is a complete list of difference sets corresponding to the Paley Hadamard matrices. As part of our classification we uncover a new triply infinite family of skew-Hadamard difference sets. To our knowledge, these are the first skew-Hadamard difference sets to be discovered in non-abelian p-groups with no exponent restriction.

Acknowledgments

I acknowledge the help and support of my collaborators Marc Röder and Richard M Stafford, who introduced me to new areas of mathematics[1].

I acknowledge the hospitality, generosity and support of Warwick de Launey, who provided inspiration for much of the work contained in this thesis.

I thank the staff (especially Kevin Jennings, John McDermott, Rachel Quinlan, Claas Röver, Jerome Sheahan and James Ward) and students (especially Marcus Bishop, Liam Naughton and Tobias Rossmann) of the School of Mathematics, Statistics and Applied Mathematics for many helpful discussions over the years and for providing an environment conducive to mathematical research.

I acknowledge the financial support of College of Arts, Social Sciences and Celtic Studies, which awarded me a fellowship. I express my gratitude to the Department of Mathematics, Statistics and Applied Mathematics at NUIG, Science Foundation Ireland (08/RFP/MTH1331), RISC Linz and the Centro Internazionale per la Ricerca Matematica Trento for covering travel expenses I incurred during my studies.

I thank my family and friends for their support over the past three years.

Last but not least, I acknowledge my supervisor Dane Flannery. Without his encouragement and guidance this thesis would not have been possible.

[1] All lists of people in these acknowledgments are alphabetical.

1 Introduction

This thesis is concerned with existence and classification problems for balanced incomplete block designs, Hadamard matrices and related algebraic and combinatorial objects. These topics were first explored in the mid-nineteenth century, yet retain a central importance in the field of design theory up to the present day. We begin this Introduction with a historical overview of the area, continue with a summary of our objectives and achievements and conclude with an outline of the thesis.

1.1 Historical overview

The origins of the study of combinatorial designs lie in the nineteenth century. A paucity of primary sources (and a near absence of secondary sources) makes investigation of this topic problematic. The first reference of which we are aware is the Prize Question posed by the editor of *The Lady's and Gentleman's diary* in 1844.

Problem 1.1 (Woolhouse, 1844)**.** *Determine the number of combinations that can be made of n symbols, p symbols in each; with this limitation, that no combination of q symbols which may appear in any one of them shall be repeated in any other.*

Remarkably, the description of Woolhouse is almost identical in substance to the definition of a (balanced incomplete block) design as given by Ryser some 120 years later.[1] Unfortunately, it does not seem that a record of the investigations which led to the posing of this question has been preserved, though in a personal communication R. J. Wilson has suggested that the problem may have been suggested to Woolhouse by Sylvester, based on work by Plücker on projective planes.

Definition 1.2 (Ryser, [69])**.** Let X be a v-set of elements, and let $X_1, X_2, \ldots, X_b$ be b distinct subsets of X. These subsets are called a *balanced incomplete block design* provided they satisfy the following requirements.

[1] In fact Ryser only defines 2-designs; we modify this to a definition of t-designs.

- Each X_i is a k-subset of X.
- Each t-subset of X is a subset of exactly λ of the sets $X_1, X_2, \ldots, X_b$.
- The integers v, k and λ satisfy $0 < \lambda$ and $k < v - 1$.

We refer to a balanced incomplete block design with parameters (t, v, k, λ) as a t-(v, k, λ) design. It is clear that a maximal solution to Woolhouse's problem is given by the number of blocks in a q-$(n, p, 1)$ design, if such a design should exist. His problem thus splits into the determination of the parameters for which a q-$(n, p, 1)$ design exists, and the determination of the number of blocks in a maximal partial design in the remaining cases. Both of these questions, reformulated more generally for t-(v, k, λ) designs, remain unanswered and are central to modern design theory. Thus it is unsurprising that while Woolhouse and others made some progress on these problems, a general solution escaped them.

A special case of the original problem was later posed, obtained by setting $q = 2$ and $p = 3$. Such 2-$(n, 3, 1)$ designs later came to be known as Steiner triple systems. Indeed by 1846, Kirkman [51] was able to show that a 2-$(n, 3, 1)$ design exists if and only if $n \equiv 1$ or $n \equiv 3 \mod 6$. This is probably the first substantial result in design theory. Kirkman [52] later investigated what are now called *affine planes* over $\mathbb{F}_q$ and *projective planes* over $\mathbb{F}_p$, as well as more general projective geometries over $\mathbb{F}_2$. Relevant also to this thesis is Kirkman's introduction of *difference circles* (now known as cyclic difference sets), which he constructs in groups of orders $7, 13, 21, 31$ and 73 (see [53]). He establishes necessary conditions for existence of a cyclic difference set and observes that in certain cases the difference set consists of the powers of 2 modulo n. His treatment of the subject is quite sophisticated, and involves what he and later contributors term *multipliers*. He concludes this remarkable paper with a comment that he has been unable to find a difference set in the cyclic group of order 43, and considers it unlikely that one exists. On the other hand, he believes that such difference sets exist in the cyclic groups of orders 57 and 91. Inspection of the tables in Baumert's book [4] proves him correct on all three counts.

Unfortunately, Kirkman's legacy has been largely ignored: we became aware of his work only through the survey paper of Biggs [6]. The study of combinatorial designs flourished again in America in the middle of the twentieth century, spurred by Hall, Ryser, Bruck and others.

In the meantime, block designs had become of interest to statisticians, notably R.A. Fisher, who studied them in connection with problems in the design of experiments. We will not consider the applications of block designs here or in the

thesis: we restrict our attention to the study of combinatorial designs as a branch of combinatorics.

In later years, infinite families of designs were constructed, and new restrictions on the parameters of a design were found, most notably those provided by the Bruck-Ryser-Chowla theorem. Automorphism groups of designs were formalised and difference sets in arbitrary finite groups were defined. Relations with many other combinatorial structures were also discovered and formalised. The most important of these for our purposes is the relationship with Hadamard matrices, which derive their appellation from Hadamard's celebrated determinantal inequality.

Theorem 1.3 (Hadamard, 1893, [26])**.** *Let M be a matrix of order n with complex entries satisfying $\|m_{i,j}\| \leq 1$. Then*

$$\|\det(M)\| \leq n^{\frac{n}{2}}.$$

A real matrix whose determinant meets this bound is called a *Hadamard matrix*. It turns out that a Hadamard matrix necessarily has order $1, 2$ or $4n$ for some $n \in \mathbb{N}$, that all its entries lie in $\{\pm 1\}$ and that the existence of a Hadamard matrix of order $4n$ is equivalent to the existence of a 2-$(4n-1, 2n-1, n-1)$ design.

As is the case with most objects of study in design theory, the biggest open question about Hadamard matrices concerns their existence.

Problem 1.4. *Prove the Hadamard conjecture: there exists a Hadamard matrix of order $4n$ for all $n \in \mathbb{N}$.*

Hadamard himself constructed matrices of orders 12 and 20. He also observed that a family of matrices of orders 2^n, for all $n \in \mathbb{N}$, constructed by Sylvester satisfy his bound and that the Kronecker product of two Hadamard matrices is again Hadamard. Thus Hadamard matrices exist for all orders of the form 2^n, $2^x 3^y$, $2^x 5^y$, with $x \geq 2y$.

In light of Sylvester's construction, it suffices to find a Hadamard matrix of order $4n$ for all odd n to prove the Hadamard conjecture. The first important step in this direction was made by Paley in 1933, who constructed Hadamard matrices of orders $4n = p^a + 1$ and $4n = 2(q^b + 1)$ where p^a and q^b are prime powers congruent to 3 and 1 mod 4 respectively [62]. The Hadamard conjecture is properly attributed to Paley.

Many constructions of Hadamard matrices have been discovered, and all of these may be divided into two types: algebraic and combinatorial. An algebraic construction takes an algebraic object as its starting point and constructs a Hadamard matrix

or a 2-$(4n-1, 2n-1, n-1)$ design in a canonical way. For example, in the paper referenced above, Paley obtains designs from the quadratic residues of finite fields. Algebraic constructions typically require detailed information about their base objects and careful algebraic and combinatorial arguments. A combinatorial construction typically describes a set of simple combinatorial objects, the existence of which is equivalent to the existence of a Hadamard matrix. Thus, the well-known Williamson construction asserts that the existence of four symmetric $\{\pm 1\}$-circulant matrices A, B, C, D of order n satisfying the equation $AA^\top + BB^\top + CC^\top + DD^\top = 4nI_n$ implies the existence of a Hadamard matrix of order $4n$ (see [75]). Computer searches are often used to find these simple combinatorial objects.

While the study of combinatorial designs is a branch of combinatorics, it has always had close ties to abstract algebra, in particular the theories of finite permutation groups and of finite fields. Already with the contribution of Kirkman, we see the introduction of groups of automorphisms of a combinatorial design. Informally, a difference set corresponds to a regular subgroup of the automorphism group of a symmetric 2-(v, k, λ) design. The study of finite projective planes seems to have been a spur for the development of the theory of difference sets: Singer's seminal work on Singer cycles and Hall's introduction of multipliers being the earliest contributions of which we are aware. Originally Hall introduced multipliers for finite projective planes, that is difference sets associated with symmetric 2-$(n^2 + n + 1, n + 1, 1)$ designs. This was later generalised to (v, k, λ)-difference sets in arbitrary cyclic groups, and then to abelian groups. We note that in 1955 Bruck [9] defined difference sets in an arbitrary finite group. This general theory of difference sets awaits further refinement. A theory of multipliers for non-abelian groups has not yet been developed, for example.

In a pioneering paper [27] of 1962, Marshall Hall defined the automorphism group of a Hadamard matrix H as the group of all pairs of signed permutation matrices (P, Q) satisfying

$$PHQ^\top = H.$$

This allows the introduction of algebraic techniques to the study of Hadamard matrices. Hall also showed that all Hadamard matrices of order 12 are equivalent and that the full automorphism group of such a matrix is a central extension of the Mathieu group M_{12}.

The automorphism group of a Hadamard matrix has a homomorphic image that is a permutation group acting on the rows of the matrix. The kernel of this action

consists of automorphisms (P, Q) such that P is a diagonal matrix. In the 1970s and 1980s, Kantor, Ito and others studied this action in considerable detail. A major problem in this area was the following:

Problem 1.5 (p.9, [28])**.** *Are the Sylvester matrices and the Hadamard matrix of order* 12 *the only Hadamard matrices on which triply transitive permutation groups act?*

The (positive) solution of this problem is a direct result of Kantor's [48] classification of the symmetric designs on which a doubly transitive group acts. This result relies on the classification of finite simple groups. A proof independent of the classification was obtained by Ito and Kimura [39] for the affine case. Ito also achieved a classification of the non-affine doubly transitive permutation groups which act on a Hadamard matrix. We use this in Chapter 4 to classify Hadamard matrices with non-affine doubly transitive automorphism groups.

More recently, in the 1990s, de Launey and Horadam introduced cocyclic development for Hadamard matrices [34]. A precise definition will be given in Chapter 3, but essentially this theory relates to 'almost regular' actions on Hadamard matrices. One of our goals in this thesis is to show that the action considered by Kantor and Ito provides a natural setting in which to explore cocyclic development.

1.2 Pairwise Combinatorial Designs

The theory of pairwise combinatorial designs generalises and unifies many disparate structures in design theory. It is closely related to the theory of cocyclic development for Hadamard matrices, from which it has grown. While we will not consider PCDs in their full generality in this thesis, we use much of this framework implicitly. This may be visible in our attempts to discuss automorphisms of Hadamard matrices, 2-designs and other structures in a unified manner. We paraphrase de Launey and Flannery [16]:

Definition 1.6. Let $\mathcal{A}$ be a non-empty finite set such that $0 \notin \mathcal{A}$. Let Γ be a set of $2 \times b$ $(0, \mathcal{A})$-arrays that is closed under row and column permutations. Suppose also that no array in Γ has a repeated row. Then we call Γ an *orthogonality set*.

We observe that this definition is purely combinatorial: neither $\mathcal{A}$ nor 0 possess any algebraic qualities. As the theory is developed, it is often convenient to embed $\mathcal{A}$ into a ring (where the symbol 0 becomes the zero of the ring). Perhaps the

prototypical example of an orthogonality set is one defined by a condition on the inner product of rows of a matrix.

Definition 1.7. Let Δ be a $v \times b$ array with entries in $\mathcal{A} \cup \{0\}$. Then Δ is a Γ-*pairwise combinatorial design* if and only if every pair of distinct rows of Δ belongs to Γ.

It is clear that any standard definition of orthogonality arises as a special case of Definition 1.6. We refer the reader to Chapter 2 of [16] for an extensive list of examples of pairwise combinatorial designs.

1.3 Objectives, accomplishments and applications

Our original objective was a deeper investigation of cocyclic development than was achieved in the author's M.Litt. thesis [58]. This topic led eventually to theoretical and computational work on classifying cocyclic Hadamard matrices of small orders. As a byproduct of this investigation, we developed an interest in the various permutation actions of the automorphism group of a Hadamard matrix. There are many open questions concerning Hadamard matrices and their related combinatorial objects. We list some of these to which we have been able to contribute here.

- Research Problem 43 of [33] asks: *For $t > 5$, are there cocyclic matrices in each equivalence class of Hadamard matrices of order $4t$? If not, what proportion of the equivalence classes are cocyclic?* We answer the first question in the negative, and provide several infinite families of non-cocyclic Hadamard matrices. For the second part, we classify all cocyclic Hadamard matrices of order $4t$ for $t \leq 9$.

- Deciding if Hadamard matrices from twin prime power difference sets are cocyclic. This is Research Problem 39 of [33]. We completely solve this problem, and further we classify all cocyclic Hadamard matrices with non-affine doubly transitive automorphism groups developed from difference sets.

- Classifying skew Hadamard difference sets. This is Open Problem 13 of [44]. We describe a new triply infinite family of skew Hadamard difference sets in groups of order q^{nq^e}, parametrised by a prime power q, an odd integer n and an integer e.

- Proving the uniqueness of the Hadamard matrix of order 36 described in [40].

Our classification of cocyclic Hadamard matrices of small order may be used for the testing of conjectures. For example, a counterexample to the conjecture made by the author in [58], that the centre of the automorphism group of a cocyclic Hadamard matrix has order 2, is immediately obtained. It should be noted that enumeration of Hadamard matrices is an important open problem in design theory. The enumeration of the (not necessarily cocyclic) Hadamard matrices of order 32 is ongoing: currently there remain only two subcases of a major classification problem to be resolved; see [49].

Horadam observes in [33] that at the time of publication there were no families of Hadamard matrices which were known to not be cocyclic. We provide two families here, both derived from difference sets. Our classification result for skew Hadamard difference sets shows that a cocyclic Hadamard matrix derived from a skew Hadamard difference set is a Paley Type I Hadamard matrix. This result will provide more families of potentially non-cocyclic Hadamard matrices as more families of skew Hadamard difference sets are discovered.

Skew Hadamard difference sets have been the object of intensive research over the past several years, since the discovery by Ding and Yuan [20] of skew Hadamard difference sets inequivalent to those of Paley. Our result gives a new infinite family. More importantly, it lists all difference sets sharing the same underlying 2-design as the Paley difference sets. It is to be hoped that this work eases the hurdle of proving that a new family of skew Hadamard difference sets is inequivalent to the Paley difference sets.

1.4 Outline of the thesis

In Chapter 2 we introduce all of the algebraic and combinatorial objects that will be discussed in this thesis. We include an overview of theory of permutation groups, with an emphasis on doubly transitive groups. We introduce symmetric balanced incomplete block designs, their automorphism groups and difference sets. We then relate these to Hadamard matrices. All of this material is well known. We conclude the chapter with an original introduction to the theory of cocyclic development, building on the material already introduced.

In Chapter 3 we discuss the classification of cocyclic Hadamard matrices. This was the topic of the author's M. Litt thesis [58]. We prove a well-known result relating cocyclic Hadamard matrices to relative difference sets. We then describe an algorithm for classifying relative difference sets. These results then allow us to

classify the cocyclic Hadamard matrices of orders 32 and 36, a result not previously known. Some of this work was carried out jointly with Marc Röder, and has appeared in [59].

In Chapter 4 we discuss the Hadamard matrices which support the structure of both a difference set and a relative difference set (as set out in Chapters 2 and 3). We observe that a permutation group associated with such a matrix is necessarily doubly transitive. We then use a result of Ito, which classifies such permutation groups, to derive a classification of all Hadamard matrices with non-affine doubly transitive automorphism groups. Our main result is that a Hadamard matrix which is both cocyclic and developed from a difference set either has order 2^n for some n, or is equivalent to a Paley type I Hadamard matrix. In the rest of the chapter we describe the central extensions, relative difference sets and difference sets associated with each of these matrices.

Finally, in Chapters 5 and 6 we give some consequences of the classification of Chapter 4. It is known that the Hadamard matrices developed from Paley difference sets and from Singer difference sets are cocyclic. We show that the Hadamard matrices developed from twin prime power difference sets and Hall sextic residue difference sets are each cocyclic in precisely one instance. We conclude with a discussion of skew Hadamard difference sets. We use our classification to determine all skew Hadamard difference sets for which the corresponding Hadamard matrix is cocyclic. In accomplishing this, we describe a new three parameter family of skew Hadamard difference sets. Chronologically, this work was preceded by the result on twin prime power difference sets, which was obtained in collaboration with Richard Stafford and published in [60]. Chapters 4, 5 and 6 constitute an extensive generalisation of this work.

2 Preliminaries

Combinatorial objects can have many definitions, which need not be obviously equivalent. Furthermore, they generally exist in a web of closely related but distinct objects. It is the purpose of this chapter to define and distinguish between Hadamard matrices and their related 2- and 3-designs. It is possible to associate to each of these objects a group of automorphisms, from which more combinatorial objects may be derived. In this vein we introduce difference sets and cocyclic development. We also include a brief overview of the aspects of the theory of permutation groups which are necessary to this thesis. Sections 2.1 and 2.2 are necessary for Chapters 4 and 5. Section 2.4 is necessary for Chapter 3. Section 2.3 finds use throughout.

2.1 Permutation groups

We assume a familiarity with basic group theory, but recall some definitions for the sake of completeness. Our notation is standard. References for this material are [21, 36, 63, 74].

Definition 2.1. We denote the *symmetric group* on the finite set Ω by $\mathrm{Sym}(\Omega)$. We write α^g for the image of $\alpha \in \Omega$ under $g \in \mathrm{Sym}(\Omega)$. We will often identify Ω with the set $\{1, 2, \ldots, n\}$, in which case we denote the symmetric group by $\mathrm{Sym}(n)$.

Definition 2.2. We say that G is a *permutation group* of degree n if $G \leq \mathrm{Sym}(\Omega)$ for some set Ω of size n. The group G is *transitive* if for any $\alpha, \beta \in \Omega$, there exists some $g \in G$ such that $\alpha^g = \beta$. We say that G is *regular* if there exists a unique $g \in G$ with this property for every $\alpha, \beta \in \Omega$.

Definition 2.3. Given a permutation group G on Ω, the *orbit* of $\alpha \in \Omega$ is the set $\{\alpha^g \mid g \in G\}$, denoted α^G. The *stabiliser* of α is the subgroup G_α of G with the property $\alpha^g = \alpha$ if and only if $g \in G_\alpha$. The Orbit-Stabiliser theorem asserts that $|G| = \left|\alpha^G\right| |G_\alpha|$.

As finite simple groups are the building blocks of finite groups, so primitive permutation groups are the building blocks of permutation groups.

Definition 2.4. Let $G \leq \mathrm{Sym}(\Omega)$ and let $\Lambda \subseteq \Omega$. We say that Λ is a *block* of G if for all $g \in G$, either $\Lambda^g = \Lambda$ or $\Lambda \cap \Lambda^g$ is empty.

Of course Ω and the singleton sets $\{\alpha\}$ for any $\alpha \in \Omega$ are blocks of G: these are called *trivial blocks*.

Definition 2.5. A permutation group which has only trivial blocks is called *primitive*.

Primitivity imposes strong conditions on the structure of a permutation group.

Definition 2.6. Let G be a finite group. A normal subgroup of G is *minimal normal* if it contains no non-trivial normal subgroup of G. The *socle* of G, denoted $\mathrm{Soc}(G)$, is the subgroup generated by all minimal normal subgroups of G.

Theorem 2.7 ([21], Theorem 4.3B)**.** *Suppose that G is a primitive subgroup of $\mathrm{Sym}(\Omega)$, and that K is a minimal normal subgroup of G. Then one of the following holds.*

- *For some prime p and some integer d, K is a regular elementary abelian group of order p^d and $\mathrm{Soc}(G) = K$.*
- *K is a regular nonabelian group, the centraliser $C_G(K)$ of K in G is isomorphic to K and $\mathrm{Soc}(G) = K \times C_G(K)$.*
- *K is non-abelian, $C_G(K) = 1$, and $\mathrm{Soc}(G) = K$.*

As a consequence, $\mathrm{Soc}(G)$ is a direct product of isomorphic simple groups.

A stronger form of this result is the O'Nan-Scott theorem, which gives a partial classification of primitive permutation groups.

An abstract group G acts on the set of right cosets of a subgroup H by right multiplication. In this action, the stabiliser of a point is a subgroup conjugate to H. Every transitive permutation action of G arises in this way. The primitive permutation actions of G are described by the following result.

Lemma 2.8. *Let G be a transitive permutation group on Ω. Then G is primitive if and only if G_α is a maximal subgroup of G for each $\alpha \in \Omega$.*

In fact we want to consider a special class of primitive permutation groups: the doubly transitive permutation groups. These were historically important in the classification of finite simple groups.

Definition 2.9. Let G be a permutation group acting on Ω. Then G is *doubly transitive group* if it is transitive on the set of ordered pairs of distinct elements of Ω. That is, for any pairs (α, β) and (γ, δ) with $\alpha, \beta, \gamma, \delta \in \Omega$, $\alpha \neq \beta$ and $\gamma \neq \delta$, there exists $g \in G$ such that $\alpha^g = \gamma$ and $\beta^g = \delta$.

The following is a well known characterisation of doubly transitive permutation groups.

Lemma 2.10 (Proposition 3.6, [63])**.** *Suppose that G acts transitively on Ω, and let $\alpha \in \Omega$. Then G is doubly transitive if and only if the action of G_α on $\Omega - \{\alpha\}$ is transitive.*

Burnside's theorem on the socle of a doubly transitive group may be regarded as a special case of Theorem 2.7.

Theorem 2.11 ([10], Sect.154)**.** *Let G be a doubly transitive group. Then the socle of G is either regular and elementary abelian, or a non-regular non-abelian simple group.*

A permutation group with regular elementary abelian socle is said to be *of affine type*, while a group with non-abelian simple socle is of *almost simple type* (often referred to as *non-affine type*). As a consequence of the classification of finite simple groups [25], a classification of doubly transitive groups has been obtained. Since the classification of doubly transitive groups is used extensively in Chapters 3 and 4, we include an overview of it here. We begin by introducing two classical families of doubly transitive groups in their natural actions on (finite) affine and projective geometries.

2.1.1 Automorphisms of affine and projective geometries

In this short section, we introduce affine and projective spaces and their automorphism groups. The automorphism groups of these spaces give two infinite families of doubly transitive permutation groups. This material is standard, and contained in [2], for example. We begin by recalling the definitions of some important families of linear groups.

Definition 2.12. Let $\mathbb{F}$ be a field, K the group of field automorphisms of $\mathbb{F}$, and let V be a vector space of finite dimension n over $\mathbb{F}$. We denote by $GL_n(\mathbb{F})$ the *general linear group* of all invertible $n \times n$ matrices over $\mathbb{F}$. Any subgroup $G \leq GL_n(\mathbb{F})$ is

a *linear group*. The *special linear group*, $SL_n(\mathbb{F})$, is the kernel of the determinant map

$$\det : GL_n(\mathbb{F}) \to \mathbb{F}^*,$$

where $\mathbb{F}^*$ is the multiplicative group of $\mathbb{F}$. We may extend $GL_n(\mathbb{F})$ by field automorphisms to form the group $\Gamma L_n(\mathbb{F}) = GL_n(\mathbb{F}) \rtimes K$, where K acts entrywise on elements of V. This is the *general semilinear group*. Any subgroup of $\Gamma L_n(\mathbb{F})$ is a *semilinear group*. The *special semilinear group* is given by the restriction of the action of K to $SL_n(\mathbb{F})$, and is denoted $\Sigma L_n(\mathbb{F})$.

We denote by V the natural module of $GL_n(\mathbb{F})$. Suppose that $\mathbb{F}$ is a finite field of order q. Then $GL_n(\mathbb{F})$ and V are both finite, and $GL_n(\mathbb{F})$ has a faithful permutation action on the q^n points of V. This gives an injective map $GL_n(\mathbb{F}) \hookrightarrow \mathrm{Sym}(V)$. Note that every element of $GL_n(\mathbb{F})$ fixes the 0 vector of V, so $GL_n(\mathbb{F})$ is intransitive. For each $v \in V$, let $t_v : V \to V$ be given by $t_v : u \mapsto u + v$. Then $R = \{t_v \mid v \in V\}$ is a regular subgroup of $\mathrm{Sym}(V)$.

Definition 2.13. Let $G \leq \Gamma L_n(\mathbb{F})$ be a semilinear group. Then the *affine group of* G is the permutation group $\langle R, G\rangle \leq \mathrm{Sym}(V)$, and is denoted AG. In particular, $A\Gamma L_n(\mathbb{F})$ is the full normaliser of R in $\mathrm{Sym}(V)$. Thus any affine semilinear group normalises R in $\mathrm{Sym}(V)$.

Definition 2.14. Let $\mathbb{F}$ be a field, and let V be an n-dimensional vector space over $\mathbb{F}$. Then the n-dimensional affine geometry over $\mathbb{F}$, $AG_n(\mathbb{F})$, is constructed as follows.

- *Points* are elements of V.
- An *affine subspace* is a subset of V of the form $\{u + a \mid u \in U\}$ where U is a subspace of V and $a \in V$ is fixed.
- Incidence of affine subspaces is given by set-theoretic inclusion.

Remark 2.15. An *automorphism* of $AG_n(\mathbb{F})$ is a bijection on points which preserves incidence. In fact, the full automorphism group of $AG_n(\mathbb{F})$ is $A\Gamma L_n(\mathbb{F})$. We observe that the subgroup R of $A\Gamma L_n(\mathbb{F})$ is transitive on points, and that $\Gamma L_n(\mathbb{F})$ is transitive on non-zero points. Hence by Lemma 2.10, the action of $A\Gamma L_n(\mathbb{F})$ is doubly transitive on the points of $AG_n(\mathbb{F})$.

In Section 4.3.2, we will see that $A\Gamma L_n(\mathbb{F}_2)$ is a quotient of the automorphism group of the Sylvester matrix of order 2^n.

We continue with the definition of some important subgroups of $A\Gamma L_n(\mathbb{F})$. These preserve either a *symplectic* or *orthogonal* geometry on a vector space. We will not need any more than the definition of these groups in the remainder of this thesis.

Definition 2.16. Let $\phi : V \times V \to \mathbb{F}$ be a non-degenerate alternating bilinear form on V. Then the dimension of V is even, $2n$ say. The *symplectic group of* V, $Sp_{2n}(\mathbb{F})$, is the group of all matrices preserving ϕ. That is $g \in GL_{2n}(\mathbb{F})$ is in $Sp_{2n}(\mathbb{F})$ if and only if $\phi(gu, gv) = \phi(u, v)$ holds for all $u, v \in V$. The definition of $Sp_{2n}(\mathbb{F})$ is independent of the choice of ϕ.

Now let V have dimension n (not necessarily even). The *orthogonal group* $O_n(\mathbb{F})$ is the group of matrices preserving a non-degenerate symmetric bilinear form on V.[1] Collectively, the general linear, special linear, symplectic and orthogonal groups are known as *classical groups*.

We conclude this section with some definitions relevant to projective geometry.

Definition 2.17. Let $\mathbb{F}$ be a field and V a vector space of dimension $n+1$ over $\mathbb{F}$. Then the *n-dimensional projective geometry* over $\mathbb{F}$, $PG_n(\mathbb{F})$, is constructed as follows.

- *Projective points* are 1-dimensional affine subspaces (lines) of V.
- A *projective subspace* of dimension k is a subspace of dimension $k+1$ of V.
- Incidence is given by set-theoretic inclusion.

Definition 2.18. The group $\Gamma L_{n+1}(\mathbb{F})$ has an induced action on $PG_n(\mathbb{F})$, given by its action on the underlying vector space. The kernel of this action consists of scalar matrices. Its image is the *projective general semilinear group*, $P\Gamma L_n(\mathbb{F})$. More generally, any subgroup of $H \leq \Gamma L_{n+1}(\mathbb{F})$ has a projective quotient denoted PH.

As in the affine case, when both the order of $\mathbb{F}$ and the dimension of the projective space are finite, a projective linear group has an induced permutation action on the projective points of $PG_n(\mathbb{F})$. We note that the action of $PSL_n(\mathbb{F})$ is always doubly transitive, on $\frac{q^n-1}{q-1}$ points.

In Section 4.3.1, we will see that $P\Sigma L_2(\mathbb{F}_q)$ is a quotient of the automorphism group of the Paley matrix of order $q+1$.

Remark 2.19. With a few exceptions at small parameter values, the projective special linear groups, projective symplectic groups, and projective orthogonal groups over finite vector spaces are three important families of finite simple groups.

[1] This definition needs to be refined in characteristic 2: see Chapter 5 of [2], for example.

Finally, since all finite fields of order q are isomorphic, we generally substitute q for $\mathbb{F}_q$ in our notation for linear and associated groups.

2.1.2 Classification of doubly transitive groups

We now return to the classification of doubly transitive groups. We begin with the groups of affine type: these are doubly transitive subgroups of $A\Gamma L_n(q)$. Suppose that $G \leq A\Gamma L_n(q)$ is doubly transitive. Then $G = RK$ where R is the elementary abelian socle of order q^n, and $K \leq \mathrm{Aut}(R) \cong \Gamma L_n(q)$ is transitive on the non-identity elements of R. There are two cases: K is either solvable or non-solvable.

Theorem 2.20 (Huppert, [36], Theorem XII.7.3)**.** *Let G be a doubly transitive solvable group of degree q^n. Then $G = R \rtimes K$ where $R = \mathrm{Soc}(G)$ and $K \leq \mathrm{Aut}(R)$ is similar to a group of semilinear transformations on $\mathbb{F}_{q^n}$, or $q^n \in \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\}$.*

The non-solvable case is a deeper result, and requires the classification of finite simple groups. (The list of groups is given in Section 5 of [31] and proved to be exhaustive in [32].)

Theorem 2.21 (Hering, [31, 32])**.** *Let $G = RK$ be an non-solvable doubly transitive group of affine type. Then K is non-solvable and up to isomorphism one of the following occurs:*

- $SL_n(q) \trianglelefteq K \leq \Gamma L_n(q)$,
- $Sp_{2n}(q) \trianglelefteq K$,
- $O_n(q) \trianglelefteq K$ *and* $q = 2^n$,
- K *is on a finite list of known groups, and* $q \in \{9^2, 11^2, 19^2, 29^2, 59^2, 2^4, 2^6, 3^6\}$.

Thus, with the exception of some sporadic groups of small degree, an affine doubly transitive group is either a subgroup of $A\Gamma L_1(q)$, or the stabiliser of a point contains a classical group as a normal subgroup.

We now consider the case that G is almost simple. The classification here is necessarily a case by case analysis of the classification of finite simple groups.

Theorem 2.22 ([25])**.** *Let G be a finite simple group. Then G is isomorphic to one of the following.*

- *A cyclic group of prime order C_p.*

- *An alternating group* A_n, $n > 4$.
- *A Chevalley group* $A_n(q), B_n(q), C_n(q), D_n(q), E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$.
- *A Steinberg group* ${}^2A_n(q), {}^2D_n(q), {}^2E_6(q), {}^3D_4(q)$.
- *A Suzuki-Ree group* ${}^2B_2(2^{2n+1}), {}^2G_2(3^{2n+1}), {}^2F_4(2^{2n+1})$, $n \geq 1$.
- *The Tits group,* ${}^2F_4(2)'$.
- *One of* 26 *sporadic groups.*

The alternating group A_n is a subgroup of index 2 in $\mathrm{Sym}(n)$. A_n is $(n-2)$-transitive in its natural action on n points (i.e. the action of A_n on ordered $(n-2)$-tuples of distinct points is transitive). In particular, A_n is doubly transitive in its natural action on n points for $n \geq 4$.

Theorem 2.23 (Section 5, [11])**.** *Suppose that G is a doubly transitive group with $\mathrm{Soc}(G) = A_n$, $n \geq 5$. Then $G = A_n$ or $\mathrm{Sym}(n)$ in its natural action, or $\mathrm{Soc}(G)$ acts as one of the following.*

- $n = 5$ *and* $\mathrm{Soc}(G)$ *acts as* $PSL(2,5)$ *on* 6 *points.*
- $n = 6$ *and* $\mathrm{Soc}(G)$ *acts as* $PSL(2,9)$ *on* 10 *points.*
- $n = 7$ *and* $\mathrm{Soc}(G)$ *acts exceptionally on* 15 *points.*
- $n = 8$ *and* $\mathrm{Soc}(G)$ *acts as* $PSL(4,2)$ *on* 15 *points.*

Theorem 2.24 (Curtis, Kantor & Seitz, [15])**.** *Let G be a Chevalley group, and suppose that $G \leq G^* \leq \mathrm{Aut}(G)$. Suppose that G has a doubly transitive permutation representation. Then one of the following occurs.*

- $PSL_n(q) \leq G^* \leq P\Sigma L_n(q)$, *and the action of G^* is its usual action on $\frac{q^n-1}{q-1}$ points.*
- $G = PSL_2(q), PSU_3(q), Sz(q)$ *or* ${}^2G_2(q)$ *and the stabiliser of a point is a Borel subgroup.*
- $G^* \cong Sp(2n,2)$ *acting on* $2^{n-1}(2^n \pm 1)$ *points.*
- G^* *is isomorphic to* A_5, $\mathrm{Sym}(5)$, A_6, $\mathrm{Sym}(6)$, A_8, *or* $\mathrm{Sym}(8)$ *in a non-standard action.*

- *G^* is $PSL_2(11)$, $PSL_2(7)$ or $PGL_2(7)$ in a non-standard action.*
- *G is $P\Sigma L_2(8) \cong {}^2G_2(3)$.*
- *G^* is $G_2(2)$ or $\mathrm{Aut}(G_2(2))$.*

Note that the first three cases of Theorem 2.24 refer to infinite families of doubly transitive groups, while the remaining cases are exceptional actions of small groups. The doubly transitive actions of the exceptional groups of Lie type are described in the following result, for which we refer to [21, 76].

Theorem 2.25. *Let G be an exceptional group of Lie type with a doubly transitive permutation representation. Then G is one of the following.*

- *${}^2A_2(q) = U_3(q)$ acting on the $q^3 + 1$ points of the corresponding unital.*
- *${}^2B_2(q) = Sz(q)$ in its natural doubly transitive action on $q^2 + 1$ points, $q = 2^{2n+1}$.*
- *${}^2G_2(q) = R(q)$ in its natural doubly transitive action on $q^3 + 1$ points, $q = 3^{2n+1}$.*

Sufficient portions of the character tables of the sporadic finite simple groups are known (see [12]) that it is elementary to write down a list of their multiply transitive permutation representations.

Group	Degree	Transitivity
M_{11}	11	4
M_{11}	12	3
M_{12}	12	5
M_{22}	22	3
M_{23}	23	4
M_{24}	24	5
HS	176	2
Co_3	276	2

Table 2.1: Transitive permutation representations of sporadic simple groups

Thus problems about doubly transitive permutation groups are reduced to questions about alternating groups, a list of groups of Lie type, and finitely many sporadic doubly transitive groups.

2.2 Balanced incomplete block designs and difference sets

Designs are incidence structures with special properties. Many of the concepts that we treat for designs may be defined for an arbitrary incidence structure. The material in this section is standard for the most part, and may be found in Chapter 1 of [5], for example.

2.2.1 Incidence structures

Definition 2.26. Let V and B be finite sets, and let $I \subseteq V \times B$. We refer to the elements of V as *points* and the elements of B as *blocks*. If $(v, b) \in I$, then we say that the point v is *incident* with the block b. We say that $\Delta = (V, B, I)$ is an *incidence structure*.

Definition 2.27. Let $\Delta_1 = (V_1, B_1, I_1)$ and $\Delta_2 = (V_2, B_2, I_2)$ be incidence structures. We say that Δ_1 and Δ_2 are *equivalent* if there exist bijections $\phi : V_1 \to V_2$ and $\psi : B_1 \to B_2$ such that $(\phi(v), \psi(b)) \in I_2$ if and only if $(v, b) \in I_1$. This is clearly an equivalence relation on the class of incidence structures.

Definition 2.28. Let $\Delta = (V, B, I)$ be an incidence structure, and suppose there exist bijections $\phi : V \to V$ and $\psi : B \to B$ such that $(\phi(v), \psi(b)) \in I$ for all $(v, b) \in I$. Then (ϕ, ψ) is an *automorphism* of Δ.

The set of all automorphisms of $\Delta = (V, B, I)$ forms a group, $\mathrm{Aut}(\Delta)$. Indeed, $\mathrm{Aut}(\Delta)$ is the stabiliser of Δ under the action of $\mathrm{Sym}(V) \times \mathrm{Sym}(B)$ on the set of all incidence structures with point set V and block set B. Often we will find it desirable to work with concrete representations of incidence structures and their automorphisms.

Definition 2.29. Let $\Delta = (V, B, I)$ be an incidence structure. Define $\chi : V \times B \to \{0, 1\}$ by $\chi(v, b) = 1$ if $(v, b) \in I$ and $\chi(v, b) = 0$ otherwise. Let M be a matrix with rows indexed by the elements of V, and columns indexed by the elements of B, whose entry in row v and column b is $\chi(v, b)$. Then M is an *incidence matrix* of Δ. We will often write

$$M = [\chi(v, b)]_{v \in V, b \in B}.$$

This notation presupposes an arbitrary but fixed ordering of the sets V and B.

Remark 2.30. This procedure works both ways: any $(0, 1)$-matrix determines an incidence structure up to labeling of rows and columns.

We will frequently identify Δ with M. We observe that M may be considered a matrix over any unital ring, with additive identity 0 and multiplicative identity 1.

Lemma 2.31. *Let $\Delta = (V, B, I)$ be a design with incidence matrix M. Then* $\mathrm{Aut}(\Delta)$ *has induced faithful actions on both the rows and the columns of M, whose combined effect preserves M.*

Proof. Suppose that $(\phi, \psi) \in \mathrm{Sym}(V) \times \mathrm{Sym}(B)$ is an automorphism of Δ. Then ϕ has an induced action on the rows of M, given by its action on the row labels. Since ϕ permutes the rows of M, it has a representation as a permutation matrix, P. Similarly, ψ permutes the columns of the matrix, and has a representation as a permutation matrix $Q^\top$. The action is clearly faithful. Furthermore, (ϕ, ψ) preserves I, so $\chi(v, b) = \chi(\phi(v), \psi(b))$ for all $v \in V$, $b \in B$. Thus $PMQ^\top = M$ as required. □

Definition 2.32. Let M be a matrix over a unital ring R. The *permutation automorphism group* of M is the group of all pairs of permutation matrices (P, Q) such that $PMQ^\top = M$. It is denoted $\mathrm{PermAut}(M)$.

Lemma 2.33. *Let Δ be an incidence structure and M an incidence matrix for Δ. Then* $\mathrm{Aut}(\Delta) \cong \mathrm{PermAut}(M)$.

Proof. By Lemma 2.31, $\mathrm{Aut}(\Delta)$ embeds in $\mathrm{PermAut}(M)$. So it suffices to show that every permutation automorphism of M induces an automorphism of Δ. But this is clear: if $PMQ^\top = M$, then P induces a permutation on the labels of the rows, $\phi \in \mathrm{Sym}(V)$. Similarly, Q induces a permutation of the column labels, $\psi \in \mathrm{Sym}(B)$. We have that $\chi(v, b) = \chi(\phi(v), \psi(b))$ for all $v \in V$ and $b \in B$, so (ϕ, ψ) is an automorphism of Δ as required. □

Remark 2.34. For a given incidence structure Δ, any two incidence matrices M and M' for Δ are equivalent up to permutation of rows and columns. Thus $M' = UMV^\top$ for some permutation matrices U and V. But this means that $(P, Q) \in \mathrm{PermAut}(M)$ if and only if $(UPU^{-1}, VQV^{-1}) \in \mathrm{PermAut}(M')$. Thus it is easily seen that the automorphism groups of any two incidence matrices for Δ are permutation isomorphic. By Lemma 2.33, we will often identify $\mathrm{Aut}(\Delta)$ and $\mathrm{PermAut}(M)$ for any incidence matrix of M.

Incidence structures in general have precisely as much structure as $(0, 1)$-matrices. We restrict to a class of incidence structures with special properties, defined below, for which the study of existence and classification problems is meaningful.

Definition 2.35. Let $\Delta = (V, B, I)$ be an incidence structure with $|B| > 1$, and suppose that for any distinct $b_1, b_2 \in B$ there exists some $v \in V$ such that $(v, b_1) \in I$ but $(v, b_2) \notin I$. Then Δ is called *reduced*.

Suppose that $\Delta = (V, B, I)$ is reduced. Then for distinct $b_1, b_2 \in B$, the sets $\{v \in V \mid (v, b_1) \in I\}$ and $\{v \in V \mid (v, b_2) \in I\}$ are distinct. Thus we may suppress I from our notation, and consider B as a set of subsets of V. Henceforth, all incidence structures that we consider will be reduced.

Lemma 2.36. *Suppose that $\Delta = (V, B, I)$ is a reduced incidence structure. Then the action of $\mathrm{Aut}(\Delta)$ is faithful on V.*

Proof. Define $\pi : \mathrm{Aut}(\Delta) \to \mathrm{Sym}(V)$ by $\pi(\phi, \psi) = \phi$, and let $N = \mathrm{Ker}(\pi)$. Suppose that N is nontrivial. Then there exist blocks b_0 and b_1 such that $b_0^{\psi_0} = b_1$ for some $(1, \psi_0) \in N$. But then $\{v \mid (v, b_0) \in I\} = \{v \mid (v, b_1) \in I\}$, against our assumption that Δ is reduced. □

By Lemma 2.36, given a reduced incidence structure $\Delta = (V, B, I)$ there is an obvious identification of $\mathrm{Aut}(\Delta)$ with a subgroup of $\mathrm{Sym}(V)$ which allows us to apply permutation group theory to the study of $\mathrm{Aut}(\Delta)$. Given the isomorphism of Lemma 2.33, we may apply these results also to $\mathrm{PermAut}(M)$ for any incidence matrix M of Δ. In this case, we can consider $\mathrm{PermAut}(M)$ as a permutation group acting on the rows of M (whose elements are no longer automorphisms of M).

2.2.2 Designs, symmetric designs and difference sets

Definition 2.37. Let $\Delta = (V, B)$ be a reduced incidence structure. Then we say that Δ is a t-(v, k, λ) design if the following hold:

- $|V| = v$,
- $|b| = k$ for all $b \in B$,
- for any t-subset T of V, $|\{b \mid T \subseteq b\}| = \lambda$.

We call a t-(v, k, λ) design *non-trivial* if $v - 1 > k > \lambda > t \geq 0$.

Remark 2.38. It is clear that the requirements for a t-design become more stringent as t increases. In fact, every t-design is necessarily an s-design for all $0 \leq s \leq t$. Arguably the main problem in modern design theory remains the determination of the sets of parameter quadruples (t, v, k, λ) for which a t-(v, k, λ) design exists.

Definition 2.39. Consider a 2-(v, k, λ) design $\mathcal{S}$ with $|V| = |B|$. We say that $\mathcal{S}$ is *symmetric* in this case. An incidence matrix M of $\mathcal{S}$ is square.[2] Note that $M^\top$ is also the incidence matrix of a 2-(v, k, λ) design, which may or may not be equivalent to $\mathcal{S}$.

Remark 2.40. A design is defined in terms of properties of subsets of points. In the case of symmetric designs, certain dual statements hold. A 2-(v, k, λ) design $\mathcal{S}$ is symmetric if and only if the intersection of any two blocks has fixed size λ. It is elementary to show that there are no symmetric t-(v, k, λ) designs for $t > 2$: the number of blocks is necessarily larger than the number of points.

These 'duality' statements have implications for the automorphism group of a symmetric design. We will use the following result, which relates the (induced) action of $\mathrm{Aut}(\mathcal{S})$ on points to its induced action on blocks.

Theorem 2.41 (Theorem III.4.1, [5])**.** *Let $\mathcal{S}$ be a non-trivial symmetric design, and let $G \leq \mathrm{Aut}(\mathcal{S})$. Then the number of orbits of G on points is equal to the number of orbits of G on blocks.*

Difference sets are algebraic objects closely related to symmetric 2-(v, k, λ) designs. For finite sets $Y \subseteq X$ we denote by $X - Y$ the set $\{x \mid x \in X, x \notin Y\}$.

Definition 2.42. Let G be a group of order v, and let $\mathcal{D}$ be a k-subset of G. We say that $\mathcal{D}$ is a (v, k, λ)-difference set in G if for each $g \neq 1 \in G$, there exist precisely λ pairs $(d_i, d_j) \in \mathcal{D}$ such that $d_i d_j^{-1} = g$. We say that $\mathcal{D}$ is nontrivial if $v - 1 > k > \lambda > 0$. If $\mathcal{D}$ is a difference set, then so too is $G - \mathcal{D}$. So, up to replacing $\mathcal{D}$ by its complement in G, we can assume that $k \leq \frac{v}{2}$.

We often identify a difference set $\mathcal{D} = \{d_1, \ldots, d_k\}$ in G with the sum $\sum_{i=1}^{k} d_i$ in the group ring $\mathbb{Z}G$.

Definition 2.43. We call a map $\vartheta : G \to G$ an *antiendomorphism* of G if $\vartheta(gh) = \vartheta(h)\,\vartheta(g)$, for all $g, h \in G$. An *antiautomorphism* is a bijective antiendomorphism.

We denote the group consisting of all automorphisms and antiautomorphisms of G by $\mathrm{AntiAut}(G)$. We observe that $\mathrm{Aut}(G)$ is a normal subgroup of index at most 2 in $\mathrm{AntiAut}(G)$, and that this group is generated by $\mathrm{Aut}(G)$ and the inversion map. (Thus $\mathrm{AntiAut}(G) = \mathrm{Aut}(G)$ if and only if G is abelian.)

[2] In general M is **not** a symmetric matrix.

Definition 2.44. We say that difference sets $\mathcal{D}_1$ and $\mathcal{D}_2$ in G are *equivalent* if there exist $g \in G$ and $\sigma \in \mathrm{AntiAut}(G)$ such that $\mathcal{D}_1 = \mathcal{D}_2^\sigma g$.

Remark 2.45. We observe that $\mathcal{D}$ is equivalent to $g\mathcal{D}$ for any $g \in G$. In fact $g\mathcal{D} = \mathcal{D}^\sigma g$, where σ is the inner automorphism of G induced by g^{-1}.

Remark 2.46. A well known family of difference sets is given by the Paley construction. One takes $G = (\mathbb{F}_q, +)$ and $\mathcal{D} = \left\{g^2 \mid g \in \mathbb{F}_q^*\right\}$, where $q \equiv 3 \mod 4$. $\mathcal{D}$ then has parameters $(4t-1, 2t-1, t-1)$. For a proof that this construction yields difference sets, see [72, p.30].

The following theorem is well known, being essentially contained in [4, pp.5-6] or [5, p.300] for example. We include the proof as an example of the type of phenomena in which we are interested, and as an illustration of many of the ideas developed thus far.

Theorem 2.47. *Suppose G contains a (v,k,λ)-difference set $\mathcal{D}$. Then there exists a symmetric 2-(v,k,λ) design on which G acts regularly. Conversely, a symmetric 2-(v,k,λ) design on which G acts regularly corresponds to a (v,k,λ)-difference set in G.*

Proof. Set $V = \{g \mid g \in G\}$ and $B = \{g\mathcal{D} \mid g \in G\}$, and let $\mathcal{S} = (V, B)$. By the 'duality' of Remark 2.40, $\mathcal{S}$ is a 2-(v,k,λ) design if and only if every pair of blocks intersect in λ points.

We consider the equation $gd_i = hd_j$ for $d_i, d_j \in \mathcal{D}$, and $g, h \in G$. Suppose $g \neq h$, and rewrite the equation as $d_i d_j^{-1} = g^{-1}h$. Since $\mathcal{D}$ is a difference set, there are precisely λ solutions. Hence $|g\mathcal{D} \cap h\mathcal{D}| = \lambda$ as required.

In the other direction, suppose that $\mathcal{S}$ is a symmetric 2-(v,k,λ) design with $G \leq \mathrm{Aut}(\mathcal{S})$ acting regularly on points. Identify the points of $\mathcal{S}$ with the elements of G. Blocks of $\mathcal{S}$ become subsets of G. By Theorem 2.41, G acts regularly on blocks. Then one finds that all blocks are of the form gb_0 for some fixed block b_0. But $|gb_0 \cap hb_0| = \lambda$ for arbitrary $g, h \in G$, $g \neq h$ implies that $x_i x_j^{-1} = g^{-1}h$ has precisely λ solutions with $x_i, x_j \in b_0$. So b_0 is a (v,k,λ)-difference set in G as required. □

Remark 2.48. If $\mathcal{S}_1$ and $\mathcal{S}_2$ are equivalent designs and G acts regularly on $\mathcal{S}_1$, then G acts regularly on $\mathcal{S}_2$. Furthermore, any difference set in G obtained from $\mathcal{S}_1$ via the construction of Theorem 2.47 is equivalent to some difference set obtained in the same way from $\mathcal{S}_2$. Conversely, equivalent difference sets give rise to equivalent symmetric designs via the construction of Theorem 2.47.

Note that $\mathrm{Aut}(\mathcal{S})$ can contain many conjugacy classes of regular subgroups which are isomorphic as abstract groups. Let R_i $(i = 1, 2)$ be regular subgroups of $\mathrm{Aut}(\mathcal{S})$, and let $\mathcal{D}_i$ be the difference set in R_i constructed as in the proof of Theorem 2.47. If R_1 and R_2 are $\mathrm{Aut}(\mathcal{S})$-conjugate, then there is an isomorphism $\alpha : R_1 \to R_2$ such that $\alpha(\mathcal{D}_1)$ is equivalent to $\mathcal{D}_2$. Conversely, if R_1 and R_2 are isomorphic but not $\mathrm{Aut}(\mathcal{S})$-conjugate, then there need not be such an isomorphism α.

We next give an example of a symmetric 2-(v, k, λ) design $\mathcal{S}$ for which $\mathrm{Aut}(\mathcal{S})$ contains many conjugacy classes of regular subgroups, and hence corresponds to many inequivalent difference sets, some of which occur in isomorphic groups. We denote the all 1s matrix of order n by J_n.

Theorem 2.49 (Kantor [47])**.** *Denote by H the n^{th} Kronecker power of the matrix $J_4 - 2I_4$ [3]. Then*

$$M = \frac{1}{2}(H + J_{2^{2n}})$$

is the incidence matrix of a 2-$(2^{2n}, 2^{2n-1}-2^{n-1}, 2^{2n-2}-2^{n-1})$ design $\mathcal{S}$. Furthermore $\mathrm{Aut}(\mathcal{S}) \cong V.Sp_{2n}(2)$, where V is an elementary abelian normal subgroup acting regularly on the points of $\mathcal{S}$ and $Sp_{2n}(2)$ is the symplectic group on V.

Remark 2.50. We consider the 2-$(16, 6, 2)$ design $\mathcal{S}$ constructed via Theorem 2.49. The designs with these parameters have been extensively studied by Assmus and Salwach [3]. In particular, they describe all of the following results which we have verified computationally. The regular subgroups of $V.Sp_4(2)$ are easily computed, using for example Magma [7]. We find that twelve of the fourteen groups of order 16 act regularly on $\mathcal{S}$. Dillon [19] refers to this as the *Jordan miracle*. We also find that $\mathrm{Aut}(\mathcal{S})$ contains 3 conjugacy classes of regular subgroups isomorphic to $C_4 \times C_4$. The difference sets these groups contain are inequivalent: this may be tested with the GAP package *rds* [68]. This shows that the distinctions of Remark 2.48 are necessary.

There is an extensive literature on difference sets. The main question here is similar to the main question of design theory: to describe the parameter sets for which a (v, k, λ)-difference set exists. One may refine this question to ask in which groups of order v such a difference set exists, or how many inequivalent difference sets exist in a given group. Identifying the points of a symmetric design $\mathcal{S}$ with the elements of a regular subgroup of $\mathrm{Aut}(\mathcal{S})$ allows for the introduction of algebraic

[3] this is equivalent to the Sylvester matrix of order 2^{2n}; see Section 4.3.2

techniques: constructions and non-existence results for difference sets in abelian groups generally make use of character theory and algebraic number theory. The existence question here is far from settled even for cyclic groups [4]. For non-abelian groups, the theory is less well developed. It is known, for example, that (v, k, λ)-difference sets exist at parameters where no abelian difference set can exist [70].

2.3 Hadamard matrices

As noted in Chapter 1, Hadamard's determinantal inequality is our starting point.

Theorem 2.51 (Hadamard, 1893, [26])**.** *Let M be a $n \times n$ matrix with complex entries satisfying $\|m_{i,j}\| \leq 1$. Then*

$$\|\det(M)\| \leq n^{\frac{n}{2}}.$$

Definition 2.52. Let H be a $n \times n$ matrix with real entries satisfying $|h_{i,j}| \leq 1$. We say that H is *Hadamard* if and only if $|\det(H)| = n^{\frac{n}{2}}$.

Remark 2.53. It is well known that a Hadamard matrix of order n necessarily has entries drawn from $\{\pm 1\}$, and that $n = 1, 2$ or $4 \mid n$. The following conditions are sufficient for a matrix H to be Hadamard.

- Every entry of H is drawn from $\{\pm 1\}$, and $HH^\top = nI_n$.
- Every entry of H is drawn from $\{\pm 1\}$, and the dot product of distinct rows of H is 0.

The definition of a Hadamard matrix does not specify the ring over which H is defined. In most cases this is irrelevant, but where not stated, we generally consider H as a matrix over $\mathbb{Z}$. This makes the standard definition of the automorphism group of a Hadamard matrix coincide with Definition 2.63. Occasionally, we may need to invert H, in which case it is considered as a matrix over $\mathbb{Q}$.

Now, it is clear that for any matrix M over $\mathbb{C}$, the quantity $\|\det(M)\|$ is preserved by permutation of rows and columns of M, and multiplication of rows and columns of M by complex numbers of absolute value 1. In fact these are precisely the operations which preserve orthogonality of rows. This motivates the definitions of equivalence and automorphisms of Hadamard matrices.

Definition 2.54. We say that Hadamard matrices H and H' of order n are *equivalent* if $PHQ^\top = H'$, for some monomial $\{\pm 1\}$-matrices P and Q. If $\mathrm{Mon}(n, \langle -1 \rangle)$

denotes the group of all $n \times n$ monomial $\{\pm 1\}$-matrices, then $\mathrm{Mon}(n, \langle -1 \rangle) \times \mathrm{Mon}(n, \langle -1 \rangle)$ acts on the set of all $n \times n$ Hadamard matrices via $(P, Q)H = PHQ^\top$. The *automorphism group* of a Hadamard matrix H is the stabiliser of H under this action. Its elements are *automorphisms* of H. We denote the automorphism group of H by $\mathrm{Aut}(H)$. If $(P, Q) \in \mathrm{Aut}(H)$ and P and Q are both $\{0, 1\}$-matrices, we say that (P, Q) is a *permutation automorphism* of H. Note that $\mathrm{PermAut}(H) \leq \mathrm{Aut}(H)$.

The following action will allow us to apply deep results from the theory of permutation groups to the study of $\mathrm{Aut}(H)$.

Definition 2.55. Let X be a $\{\pm 1\}$-monomial matrix of order n. Then X has a unique factorization $D_X E_X$ where D_X is a diagonal matrix and E_X is a permutation matrix. For a Hadamard matrix H, and $(P, Q) \in \mathrm{Aut}(H)$, define $\nu(P, Q) = E_P$.

In this way each permutation automorphism (P, Q) of a Hadamard matrix H induces a permutation of the rows of H. In fact, ν is a homomorphism and gives a permutation representation of $\mathrm{Aut}(H)$ in the symmetric group on the rows of H. For ease of notation, we will refer to $\mathcal{A}(H) = \nu(\mathrm{Aut}(H))$ as a permutation group on $\{1, 2, \ldots, n\}$ where i represents the i^{th} row of H. We use standard permutation group terminology for $\mathcal{A}(H)$. Henceforth, when $\mathcal{A}(H)$ has a permutation group property, we will say that $\mathrm{Aut}(H)$ has this property.

Definition 2.56. We say that a Hadamard matrix $H = [h_{i,j}]_{1 \leq i,j \leq n}$ is *normalised* if and only if $h_{i,1} = h_{1,j} = 1$ for all $1 \leq i, j \leq n$. Every Hadamard matrix is monomially equivalent to a normalised Hadamard matrix.

Any statements regarding Hadamard matrices (such as claims of uniqueness, classification etc.) are made only up to equivalence.

The following lemma is standard; see e.g. Lemma I.9.3 of [5], though our proof is different from the one given there.

Lemma 2.57. *Let $\mathcal{S}$ be a symmetric 2-$(4n-1, 2n-1, n-1)$-design with incidence matrix M. Define J to be the $(4n-1) \times (4n-1)$ all 1s matrix, and T to be $2M - J$. Let $\overline{1}$ be the all 1s vector of length $4n-1$. Then*

$$H = \begin{pmatrix} 1 & \overline{1} \\ \overline{1}^\top & T \end{pmatrix}$$

is a Hadamard matrix.

Proof. First, we observe that $MM^\top = nI + (n-1)J$. It follows that

$$\begin{aligned} TT^\top &= (2M - J)(2M^\top - J) \\ &= 4MM^\top - 2MJ - 2JM^\top + J^2 \\ &= 4(nI + (n-1)J) - (4n-2)J - (4n-2)J + (4n-1)J \\ &= 4nI - J. \end{aligned}$$

Thus, adding an initial row and column of +1s to T gives a Hadamard matrix. □

Remark 2.58. So a Hadamard matrix of order $4n$ exists if a symmetric 2-$(4n-1, 2n-1, n-1)$ design exists. The converse is also true: one obtains an incidence matrix for a symmetric 2-$(4n-1, 2n-1, n-1)$ design from the core of a normalised Hadamard matrix by replacing every occurrence of -1 by 0. Notice that a symmetric 2-$(4n-1, 2n-1, n-1)$ design corresponds to a unique equivalence class of Hadamard matrices via the construction of Lemma 2.57. But the equivalence operations for 2-designs are finer than the equivalence relations for Hadamard matrices. So a single equivalence class of Hadamard matrices can give rise to many inequivalent 2-designs.

Lemma 2.59. *Let $\mathcal{S}$ be a symmetric* 2-$(4n-1, 2n-1, n-1)$ *design, and let H be the Hadamard matrix constructed from $\mathcal{S}$ as in Lemma 2.57. Then* $\mathrm{Aut}(\mathcal{S}) \cong \mathrm{PermAut}(H)$.

Proof. We extend $(P, Q) \in \mathrm{Aut}(\mathcal{S})$ to an automorphism

$$\left(\begin{pmatrix} 1 & \overline{0} \\ \overline{0}^\top & P \end{pmatrix}, \begin{pmatrix} 1 & \overline{0} \\ \overline{0}^\top & Q \end{pmatrix} \right)$$

of H, which fixes the first row and column and acts as (P, Q) on the submatrix T. Thus $\mathrm{Aut}(\mathcal{S})$ embeds in $\mathrm{PermAut}(H)$. In the other direction: $(P, Q) \in \mathrm{PermAut}(H)$ must fix the unique first row and first column of 1s, and hence restricts to an automorphism of $\mathcal{S}$. So $\mathrm{PermAut}(H) \cong \mathrm{Aut}(\mathcal{S})$. □

We observe that Theorem 2.47 can be combined with Lemma 2.57 to obtain a Hadamard matrix from a difference set.

Definition 2.60. Let H be a Hadamard matrix, $\mathcal{D}$ a difference set in a group G and $\mathcal{S}$ a symmetric design. If $\mathcal{D}$ and $\mathcal{S}$ are related as in Theorem 2.47, then we say that $\mathcal{S}$ *underlies* $\mathcal{D}$, or that $\mathcal{D}$ *is over* $\mathcal{S}$. If H is a Hadamard matrix related to $\mathcal{S}$ as in Lemma 2.57, then we say that H *is developed from* $\mathcal{S}$, or that $\mathcal{S}$ *corresponds*

to H. We use the same terminology for the relationship between $\mathcal{D}$ and H as for $\mathcal{S}$ and H.

So by Lemma 2.57 and Theorem 2.47, we see that a $(4n-1, 2n-1, n-1)$-difference set in a group G corresponds in a natural way to a Hadamard matrix H such that G is a regular subgroup of the stabiliser $\mathcal{A}(H)_1$ of the first row of H in $\mathcal{A}(H)$.

Definition 2.61. A symmetric 2-$(4t-1, 2t-1, t-1)$ design is called *Paley-Hadamard*. Likewise a $(4t-1, 2t-1, t-1)$-difference set is called *Paley-Hadamard*. This terminology acknowledges both the relation to Hadamard matrices and the role of R.E.A.C. Paley in describing one of the best known families of $(4t-1, 2t-1, t-1)$-difference sets. We emphasise: *Paley-Hadamard* refers to any difference set with parameters $(4t-1, 2t-1, t-1)$, whereas a *Paley* difference set belongs to a specific family with these parameters (see Remark 2.46).

Remark 2.62. Paley-Hadamard designs are not to be confused with designs with parameters 2-$(4t^2, 2t^2-t, t^2-t)$, which give rise to Hadamard matrices via a different construction. We do not consider such designs per se in this thesis (they form a special case of certain relative difference sets discussed in Chapter 3). Where necessary we refer to them as *Menon-Hadamard*. Note that the term *Hadamard design* is inconsistently used in the literature to refer to a design of either type: different authors have different conventions. For this reason we avoid it entirely. We direct the reader to a further discussion in the footnote to p.366 of [5].

2.4 Cocyclic development

Most of the ideas in this section can be traced back to work by Warwick de Launey and by de Launey and Horadam in the early 1990s. These ideas were further extended to general pairwise combinatorial designs in the book [16]. Our treatment of the topic is perhaps more closely related to the theory of permutation groups than the standard accounts [16, 33].

In Theorem 2.47, we described a relation between symmetric 2-designs and difference sets. In the following theorem, we extend this to a relation between an arbitrary matrix M over a commutative ring, regular subgroups of $\mathrm{PermAut}(M)$ and distinguished sets of elements of a group G. This is the base case for a generalisation of the theory developed by Horadam and de Launey for Hadamard matrices in [34], termed *cocyclic development*.

We begin with a definition of the automorphism group of a matrix over a commutative ring. This generalises the definitions of $\mathrm{PermAut}(M)$ for the incidence matrix of a t-(v, k, λ) design, and $\mathrm{Aut}(H)$ for a Hadamard matrix H, for example.

Definition 2.63. Let R be a commutative unital ring with unit group U. Let M be an R-matrix. Then the *full automorphism group* of M, denoted $\mathrm{Aut}(M)$ consists of all pairs of monomial U-matrices (P, Q) such that $PMQ^\top = M$.

We observe that $\mathrm{Aut}(M)$ contains a central subgroup of diagonal matrices of the form $(uI, u^{-1}I)$ which is isomorphic to the unit group U of R. We denote this subgroup by Θ. We note also that $\mathrm{PermAut}(M) \leq \mathrm{Aut}(M)$.

2.4.1 Group development

From the remainder of this chapter, we will restrict our attention to square matrices.

Definition 2.64. Let M be an $n \times n$ matrix with entries in a commutative ring R, and let G be a group of order n. We say that M is *group developed over* G if there exists a function $\mu : G \to R$ such that $M = \left[\mu(gh^{-1})\right]_{g,h\in G}$ for a fixed but arbitrary labeling of the rows and columns of M by the elements of G. We say that M is *group developed* if it is group developed over G for some group G.

Remark 2.65. It is perhaps more usual to define a group developed matrix to be of the form $M = [\mu(gh)]_{g,h\in G}$. The two forms are equivalent up to a suitable permutation of the columns of M. Our choice of the above was motivated by the discussion of skew Hadamard matrices and skew difference sets in Chapter 5. In particular, our notation has the following advantages when the labeling of rows and columns is identical.

- The main diagonal of a group developed matrix is constant, consisting of the entries $\mu(gg^{-1}) = \mu(1)$.
- The transpose of M takes a particularly nice form: $M^\top = \left[\mu(gh^{-1})\right]^\top_{g,h\in G} = \left[\mu(hg^{-1})\right]_{g,h\in G} = \left[\mu((gh^{-1})^{-1})\right]_{g,h\in G}$.

As an example, let π be a regular permutation matrix representation of G over some unital ring R. Then any matrix of the form $M = \sum_{g\in G} \alpha_g \pi(g)$, where the α_g are drawn from R, is group developed. Up to permutation of rows and columns, every group developed matrix is obtained in this way (see Lemma 3.7.4 of [16]).

Remark 2.66. As previously mentioned, a standard technique in the theory of difference sets is to identify a difference set with the sum of its elements in the group ring. Under this identification, we see the correspondence between difference sets and symmetric 2-designs as part of a more general phenomenon. There are many similar results which relate group developed matrices of particular types to group ring elements with special properties. (Such constructions are common in coding theory, for example.)

In the following results, we describe necessary and sufficient conditions on the group $\mathrm{PermAut}(M)$ for a matrix M to be group developed over G. We recall the Kronecker δ_g^h function, which is 1 if $g = h$ and 0 otherwise.

Lemma 2.67 (Cf. Theorem 3.7.5 of [16])**.** *Let M be a matrix of order n with entries in a commutative unital ring R, and G a group of order n. Fix an ordering of the elements of G, and use this to index the rows and columns of M. Define T_x to be $[\delta_a^{gx}]_{g,a\in G}$. Then M is group developed over G if and only if $(T_x, T_x) \in \mathrm{PermAut}(M)$ for all $x \in G$.*

Proof. Write $M = \left[\mu\left(g, h^{-1}\right)\right]_{g,h\in G}$, and observe that $T_x^\top = T_x^{-1} = T_{x^{-1}}$. Now

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

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

$$\mu\left(g, h^{-1}\right) = \mu\left(gx, x^{-1}h^{-1}\right) \quad \forall g, h, x \in G. \tag{2.1}$$

If M is group developed, then $\mu\left(g, h^{-1}\right) = \phi\left(gh^{-1}\right)$ for some set map $\phi : G \to R$, and (2.1) is certainly satisfied:

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

Conversely, suppose that (2.1) is satisfied, and define $\phi(g) = \mu(g, 1)$. Then

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

Hence M is group developed over G. □

The following theorem gives an effective procedure to determine if M is group developed, under the assumption that there exist effective algorithms for the determination of $\mathrm{PermAut}(M)$ and the regular subgroups of a permutation group.

Theorem 2.68. *An R-matrix M is group developed over the group G if and only if* $\mathrm{PermAut}(M)$ *contains a subgroup isomorphic to G, acting regularly on the rows and columns of M.*

Proof. Suppose that M is group developed. Then by Lemma 2.67, for all $x \in G$, $(T_x, T_x) \in \mathrm{PermAut}(M)$. The map $x \mapsto (T_x, T_x)$ defines an isomorphism from G onto a subgroup of $\mathrm{PermAut}(M)$. Furthermore, this subgroup acts regularly on the rows and columns of M.

Conversely, suppose that $\mathrm{PermAut}(M)$ contains a subgroup isomorphic to G acting regularly on the rows and columns of M. We may write this subgroup as $\{(P_x, Q_x) \mid x \in G\}$ for permutation matrices P_x, Q_x, such that $P_x M Q_x^\top = M$. As is well known, up to similarity, there is a single faithful regular permutation representation of G. This means that there exist permutation matrices U and V such that $UP_xU^\top = T_x$ and $VQ_xV^\top = T_x$ for all $x \in G$. Thus $UMV^\top$ is group developed over G by Lemma 2.67. Group development is preserved by permutation equivalence, so M is also group developed over G. □

Remark 2.69. It was consideration of factorization of the determinant of an arbitrary group developed matrix with entries in $\mathbb{C}$ which originally led Frobenius to the invention of character theory [14]. While his work is not directly relevant here, we observe that his results lead to efficient methods to calculate the determinant of a group developed matrix $\left[\phi(gh^{-1})\right]_{g,h\in G}$ directly from knowledge of the group development function ϕ. It is reasonable to consider that these results may be generalised to cocyclic matrices, possibly by inducing characters to the extension group.

Now we generalise these results to cocyclic development.

2.4.2 Cocyclic development

Our cocycles are a very special case of the general definition of a cocycle as used in e.g. algebraic topology.

Definition 2.70. Let G be a finite group, and let W be a finite abelian group. A *(2-)cocycle* is a map $\psi : G \times G \to W$ which obeys the following identity for all $g, h, k \in G$.

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

Similarly, a *(2-)coboundary* is a map $\delta\phi : G \times G \to W$ such that

$$\delta\phi(g,h) = \phi(g)\phi(h)\phi(gh)^{-1}$$

for some map $\phi : G \to W$.

Remark 2.71. Every coboundary is a cocycle. The set of cocycles forms an abelian group under (pointwise) multiplication, normally denoted $Z^2(G,W)$. The set of coboundaries forms a subgroup, denoted $B^2(G,W)$. The quotient group is the *second cohomology group of G with coefficients in W*, $H^2(G,W)$. We say that two cocycles ψ_1 and ψ_2 are *cohomologically equivalent* if there exists a coboundary $\delta\phi$ such that $\psi_2 = \psi_1\delta\phi$.

Higher cohomology groups are defined analogously, but currently play no part in the theory of cocyclic development. The following material on second cohomology is standard; a more comprehensive account may be found in Chapter 11 of [65].

Definition 2.72. A group Γ is an *extension* of W by G if there exist an injective map $\iota : W \to \Gamma$ and a surjective map $\pi : \Gamma \to G$ such that the sequence

$$1 \to W \xrightarrow{\iota} \Gamma \xrightarrow{\pi} G \to 1$$

is exact. We say that the extension is *central* if $\iota(W) \leq Z(\Gamma)$.

From now on, all extensions we consider are central. Given a cocycle $\psi \in Z^2(G,W)$, define a multiplication on the Cartesian product of the underlying sets of W and G by

$$(u,g)(v,h) = (uv\psi(g,h), gh).$$

where the multiplications in the first and second components are the group operations of W and G respectively. It is routine to verify that the group Γ_ψ so formed

is in fact an extension of W by G. Note that the trivial cocycle corresponds to the direct product of W by G. In fact every central extension of W by G gives rise to a central extension Γ_ψ for some $\psi \in Z^2(G,W)$, that is equivalent to the original extension in the following sense.

Definition 2.73. Two extensions of W by G are *equivalent* if and only if the following diagram commutes, where γ_0 and γ_2 are identity maps. Note that if the

$$\begin{array}{ccccccccc} 1 & \to & W & \xrightarrow{\iota} & \Gamma_\psi & \xrightarrow{\pi} & G & \to & 1 \\ & & \downarrow \gamma_0 & & \downarrow \gamma_1 & & \downarrow \gamma_2 & & \\ 1 & \to & W & \xrightarrow{\iota'} & \Gamma_\varphi & \xrightarrow{\pi'} & G & \to & 1 \end{array}$$

extensions are equivalent then γ_1 is necessarily an isomorphism. However, if Γ_ψ and Γ_φ are isomorphic then the extensions need not be equivalent.

Now, we have introduced equivalence relations on both the set of extensions of W by G and the set of set of cocycles $Z^2(G,W)$. In fact these notions of equivalence coincide. Cohomologically equivalent cocycles give rise to equivalent extensions, and conversely. Thus $H^2(G,W)$ gives the structure of an abelian group to the set of equivalence classes of extensions of W by G.

Definition 2.74. Let R be a commutative unital ring with unit group U, and let $W \leq U$ be finite. Let M be an $n \times n$ matrix with entries in R, and G a group of order n. Then M is *cocyclic* over G if and only if there exist a cocycle $\psi : G \times G \to W$ and a set map $\phi : G \to R$ such that M is equivalent to the matrix

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

up to permutation of rows and columns and multiplication of rows and columns by elements of U. We say that ψ *is a cocycle of* M, that M is *cocyclic over* G, and that the extension of W by G determined by ψ is an *extension group of* M.

This definition is broader than that given by Horadam in Definition 6.3 of [33], where a cocyclic matrix over an abelian group C is defined as one that is equivalent to $[\psi(g,h)]_{g,h\in G}$ for some cocycle ψ. In Chapter 13 of [16], de Launey and Flannery give a definition, broader than ours, in which the equivalence relations on rows and columns need not coincide. Inclusion of the function $\phi : G \to R$ allows us to consider a broader class of matrices. We give an example.

Example 2.75. Let $C = \langle c \mid c^3 = 1 \rangle$, and ω be a primitive complex cube root of unity. Let $\rho(1) = 1$ and $\rho(c) = \rho\left(c^2\right) = \omega$. Define the cocycle $\psi : C \times C \to \langle\omega\rangle$ by

$\psi\left(c^i, c^j\right) = \rho\left(c^i\right)\rho\left(c^j\right)\rho\left(c^{i+j}\right)^{-1}$. Indexing row i and column i by c^{i-1}, we obtain the pure cocyclic matrix

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

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

The following lemma is an example of restrictions on the permutation automorphism group of a normalised matrix.

Lemma 2.76. *Suppose that the R-matrix M is invertible and normalised. Define G to be the stabiliser in* $\mathrm{Aut}(M)$ *of the first column and the first row of M. Then* $\mathrm{PermAut}(M)$ *is a complement of* Θ *in G.*

Proof. Suppose that (P,Q) is a permutation automorphism of M. Then (P,Q) fixes the first row and column of M. So it is contained in G. Conversely, suppose that (P,Q) is in G. Then the first row and column of M are fixed. So $(uP, u^{-1}Q)$ is a permutation automorphism for any unit u of R. In particular, we observe that G splits over Θ. □

Our goal is to develop a characterisation of cocyclic matrices in terms of their automorphism groups analogous to Lemma 2.67 for group developed matrices. We will also explore some properties of cocyclic matrices which will be of use in later chapters. Assuming that each matrix M discussed is invertible over an implicit ring, and that all entries of M are non-zero, we introduce some important quotients of $\mathrm{Aut}(M)$.

We observe that a monomial matrix P has a unique decomposition $P = D_P E_P$ into diagonal and permutation parts.

Definition 2.77 (cf. Definition 2.55)**.** Let $(P,Q) \in \mathrm{Aut}(M)$ and define the projections $\mu : (P,Q) \mapsto (E_P, E_Q)$ and $\nu : (P,Q) \mapsto E_P$. We define $\mathcal{G}(M) = \mu(\mathrm{Aut}(M))$ and $\mathcal{A}(M) = \nu(\mathrm{Aut}(M))$. We consider $\mathcal{A}(M)$ a permutation group on the rows of M and $\mathcal{G}(M)$ a permutation group on the rows and columns of M. We observe that $\mathrm{Ker}(\mu) = \Theta$, and that $\mathrm{Ker}(\mu) \trianglelefteq \mathrm{Ker}(\nu)$. However these subgroups need not coincide.

Remark 2.78. Let ρ be the map that projects onto the first component, so that $\nu = \rho\mu$. In many cases ρ can be shown to be injective. For example this will happen if M is a $(0,1)$ matrix, so that $\mathrm{Aut}(M) = \mathrm{PermAut}(M)$. We are not aware of necessary and sufficient conditions for ρ to be injective in general. An example where $\mathrm{Ker}(\rho)$ is non-trivial (and even transitive) is given in Theorem 4.2. If one restricts to the case that ρ is injective, the statement of Theorem 2.86 below takes a much simpler form.

In particular, if we insist that M is a normalised matrix, then $\nu(\mathrm{PermAut}(M))$ is never transitive, and this excludes some interesting behaviour. The Hadamard matrix H constructed in Theorem 2.49 is not normalised and has $\mathrm{PermAut}(H) \cong V.Sp_{2n}(2)$, which is doubly transitive. H is cocyclic in the sense of Definition 2.74.

Definition 2.79. Suppose that G is a subgroup of $\mathcal{G}(M)$ such that the action of G on the rows of M is regular, and the action of G on the columns of M is regular. We say that the action of G on M is *totally regular*.

Remark 2.80. We recall that M is group developed if and only if $\mathrm{PermAut}(M)$ contains a subgroup G which acts regularly on both rows and columns of M. In this case $\mathcal{G}(M)$ contains a totally regular subgroup. Furthermore, ΘG is a direct product, and $\mu(\Theta G) = G$.

A group developed matrix is a special kind of cocyclic matrix (i.e. one with trivial cocycle) on which a group acts regularly. We next show that $\mathcal{G}(M)$ contains a totally regular subgroup if M is cocyclic.

Lemma 2.81. *Suppose that M is cocyclic over G. Then $\mathcal{G}(M)$ contains a totally regular subgroup isomorphic to G.*

Proof. Suppose that ψ is a cocycle of M. Define the following monomial matrices for all $a \in G$:

$$P_a = [\psi(x,a)\delta_y^{xa}]_{x,y\in G}, \quad Q_a^\top = [\psi(a,a^{-1}w^{-1})^{-1}\delta_w^{za^{-1}}]_{z,w\in G}.$$

The cocycle equation can be written as $\psi(g,h) = \psi(g,hk)\psi(h,k)\psi(gh,k)^{-1}$, from which we derive the identity

$$\psi(x,a) = \psi(x,w^{-1})\psi(a,a^{-1}w^{-1})\psi(xa,a^{-1}w^{-1})^{-1},$$

which is used in the argument below. We show that (P_a, Q_a) is an automorphism of M for all $a \in G$:

$$\begin{aligned}
P_a M Q_a^\top &= \left[\psi(x,a)\delta_y^{xa}\right]_{x,y\in G}\left[\psi(y,z^{-1})\phi(yz^{-1})\right]_{y,z\in G}[\psi(a,a^{-1}w^{-1})^{-1}\delta_w^{za^{-1}}]_{z,w\in G}\\
&= \left[\sum_y \delta_y^{xa}\psi(x,a)\psi(y,z^{-1})\phi(yz^{-1})\right]_{x,z\in G}[\psi(a,a^{-1}w^{-1})^{-1}\delta_w^{za^{-1}}]_{z,w\in G}\\
&= \left[\psi(x,a)\psi(xa,z^{-1})\phi(xaz^{-1})\right]_{x,z\in G}[\psi(a,a^{-1}w^{-1})^{-1}\delta_w^{za^{-1}}]_{z,w\in G}\\
&= \left[\sum_z \delta_w^{za^{-1}}\psi(x,a)\psi(xa,z^{-1})\psi(a,a^{-1}w^{-1})^{-1}\phi(xaz^{-1})\right]_{x,w\in G}\\
&= \left[\psi(x,a)\psi(xa,(wa)^{-1})\psi(a,a^{-1}w^{-1})^{-1}\phi(xa(wa)^{-1})\right]_{x,w\in G}\\
&= \left[\psi(x,w^{-1})\phi(xw^{-1})\right]_{x,w\in G}\\
&= M.
\end{aligned}$$

Now, to conclude it suffices to observe that the subgroup

$$\left\{\left(\left[\delta_y^{xa}\right]_{x,y\in G},\left[\delta_y^{xa}\right]_{x,y\in G}\right) \mid a\in G\right\} \cong G$$

of $\mathcal{G}(M)$ is totally regular (cf. Lemma 2.67: $\left[\delta_y^{xa}\right]_{x,y\in G} = T_a$ in the notation of that result). □

We now show that a matrix M for which $\mathcal{G}(M)$ contains a totally regular subgroup with a preimage in $\mathrm{Aut}(M)$ of a specified type is cocyclic. To do this, we introduce the expanded matrix of M.

Definition 2.82. Let M be an $n\times n$ R-matrix, and W a finite subgroup of the group of units of R. Then

$$\mathcal{E}_M = [vwm_{i,j}]_{v,w\in W,1\le i,j\le n}$$

is an *expanded matrix* of M. That is, $\mathcal{E}_M$ is the Kronecker product of M with a Cayley table for W.

The following result allows us to embed $\mathrm{Aut}(M)$ in $\mathrm{PermAut}(\mathcal{E}_M)$. We omit the proof (it is elementary but long). For the rest of this section, M is a matrix with entries in a ring R with finite unit group W.

Lemma 2.83 (Lemma 3.14, [58]; and cf. Theorem 9.6.11 of [16])**.** *Define* $\epsilon_w(M) = \left[\delta^w_{m_{i,j}}\right]_{1\le i,j\le n}$. *Then the homomorphism* $\iota : \mathrm{Aut}(M)\to\mathrm{PermAut}(\mathcal{E}_M)$ *given by* $\iota(P,Q) = (\left[\epsilon_{vw^{-1}}(P)\right]_{v,w\in W},\left[\epsilon_{vw^{-1}}(Q)\right]_{v,w\in W})$ *is injective.*

Corollary 2.84. *The group $G \leq \mathcal{G}(M)$ is totally regular on M if and only if the full preimage Γ of G in $\mathrm{Aut}(M)$ under μ (see Definition 2.77) has an induced regular action on the rows of $\mathcal{E}_M$ and an induced regular action on the columns of $\mathcal{E}_M$.*

Proof. First, the preimage Γ of G in $\mathrm{Aut}(M)$ is a central extension of the group $\overline{W} = \{(wI, w^{-1}I) \mid w \in W\}$ by G.

Let ι be as in Lemma 2.83. Suppose that G is totally regular. We claim the action of $\iota(\Gamma)$ on the rows and columns of $\mathcal{E}_M$ is fixed-point-free. By hypothesis, a non-trivial element $(P, Q) \in G$ is fixed-point-free on the rows and columns of M. So all diagonal entries of P and Q are zero. Thus every element in $\Gamma - \overline{W}$ has all diagonal entries zero. So certainly every element of $\iota(\Gamma - \overline{W})$ is fixed-point-free on rows and columns of $\mathcal{E}_M$. But the action of $\iota\overline{W}$ is specified in Definition 2.82, and is easily seen to be fixed-point-free.

So $\iota(\Gamma)$ is fixed-point-free on the rows and columns of $\mathcal{E}_M$. But $|\iota(\Gamma)| = |G|\,|W|$, which is equal to the dimension of $\mathcal{E}_M$. So $\iota(\Gamma)$ is regular on the rows and regular on the columns of $\mathcal{E}_M$. □

Lemma 2.85. *Suppose that $G \leq \mathcal{G}(M)$ acts totally regularly on M. Then M is cocyclic over G.*

Proof. By Theorem 2.68 and Corollary 2.84, $\mathcal{E}_M$ is group developed over the central extension $\Gamma = \Gamma_\psi$, for some cocycle $\psi : G \times G \to W$. So $\mathcal{E}_M$ can be expressed as follows.

$$\mathcal{E}_M = \left[\phi((v,g)(w,h)^{-1})\right]_{(v,g),(w,h)\in\Gamma}.$$

In fact, we can say more: the action of $\overline{W} \trianglelefteq \Gamma$ is specified by Definition 2.82. So $\phi(w, g) = w\phi(1, g)$ for all $w \in W$ and all $g \in G$. We observe that M is a submatrix of $\mathcal{E}_M$ with rows and columns labelled by $(1, g)$ and $(1, h^{-1})$ respectively:

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

Define $\overline{\phi} : G \to R$ by $\overline{\phi}(g) = \phi(1, g)$. Then $M = \left[\psi(g, h^{-1})\overline{\phi}(gh^{-1})\right]_{g,h\in G}$ is a cocyclic matrix as required. □

Theorem 2.86 (cf. Theorem 14.7.1 of [16])**.** *The matrix M is cocyclic over the group G if and only if $\mathcal{G}(M)$ contains a totally regular subgroup isomorphic to G.*

Proof. One direction follows from Lemma 2.81, the other from Lemma 2.85. □

Remark 2.87. We note that Chapter 14 of [16] gives a full treatment of cocyclic development for pairwise combinatorial designs. There, a cocyclic design is characterised in terms of 'centrally regular' actions on the expanded matrix of the design.

This concludes our discussion of cocyclic development. In Chapter 3, we apply much of the theory developed in this chapter to classify the cocyclic Hadamard matrices of orders less than 40.

3 Classification of cocyclic Hadamard matrices

In Chapter 2, we defined cocyclic development for certain matrices over a commutative ring. The author's M. Litt. thesis [58] contains an extensive discussion of the theory of cocyclic development for Hadamard matrices. It also contains an algorithm for determining the cocycles of a given Hadamard matrix. We begin this chapter with a proof of the well-known fact that a cocyclic Hadamard matrix of order $4t$ corresponds to a $(4t, 2, 4t, 2t)$-relative difference set. (This has been shown by de Launey, Flannery and Horadam in [17]. Also cf. [43], and Ito's series of papers beginning with [38]. Note that a Hadamard group is precisely an extension group of a cocyclic Hadamard matrix; see [23].) Then we give an algorithm for the computation of all such relative difference sets in a given group. Running this algorithm for all groups of orders 64 and 72 yields all cocyclic Hadamard matrices of orders 32 and 36. We collect and summarize the results obtained in the final section. Some of this work was carried out jointly with Marc Röder, and has appeared in print in [59].

3.1 Cocyclic Hadamard matrices and relative difference sets

We begin with an overview of cocyclic development for Hadamard matrices. Since all entries in a Hadamard matrix are drawn from $\langle -1 \rangle$, the theory is simpler than in the general case.

Remark 3.1. Suppose that $\psi : G \times G \to \langle -1 \rangle$ is a cocycle. Then $\psi(g, h^{-1}) = \psi(g, h^{-1})^{-1}$ for all $g, h \in G$. This allows us some liberty in rearranging identities involving cocycles.

Suppose that the Hadamard matrix H is cocyclic over the group G. That is

$$H = \left[\psi(g, h^{-1})\phi(gh^{-1})\right]_{g,h \in G}$$

for some cocycle ψ and set map $\phi : G \to \langle -1 \rangle$. Recall that a coboundary is defined by the equation $\delta\phi(g, h^{-1}) = \phi(gh^{-1})\phi(g)\phi(h^{-1})$.

Now consider the matrix

$$\overline{H} = \left[\psi(g, h^{-1})\phi(gh^{-1})\phi(g)^{-1}\phi(h^{-1})^{-1}\right]_{g,h\in G} = \left[\overline{\psi}(g, h^{-1})\right]_{g,h\in G}.$$

$\overline{H}$ differs from H only in the multiplication of rows and columns by scalars. Hence H and $\overline{H}$ are equivalent cocyclic Hadamard matrices. We say that $\overline{H}$ is a *pure cocyclic* matrix. We have the following result.

Lemma 3.2. *The Hadamard matrix H is cocyclic if and only if it is equivalent to a pure cocyclic Hadamard matrix.*

Remark 3.3. We again remark that Horadam [33] defines a cocyclic Hadamard matrix according to the statement of Lemma 3.2. Also, a cocycle of H under our definition may not be a cocycle of H under Horadam's definition.

In Theorem 2.47 we related the existence of a regular subgroup G in the automorphism group of a symmetric design $\mathcal{S}$ to the existence of a difference set in G. Now we relate the existence of a regular subgroup G in $\mathcal{A}(H)$ (satisfying some additional conditions) to the existence of a relative difference set in a group $\Gamma \leq \mathrm{Aut}(H)$ satisfying $\nu(\Gamma) = G$ (see Definition 2.55). Although a difference set is a relative difference set, we emphasise that these two sets of relationships are quite separate from each other; cf. Remark 2.62.

We first recall the definition of a relative difference set.

Definition 3.4. Let Γ be a finite group, with normal subgroup N. We say that $R \subset \Gamma$ is a relative difference set (RDS) with respect to N if in the multiset $\left\{r_1 r_2^{-1} \mid r_1, r_2 \in R\right\}$ every element of $\Gamma - N$ occurs exactly λ times (for some fixed λ), and no non-trivial element of N occurs.

We refer to N as the *forbidden subgroup*. If N is of order n, Γ is of order nm and the RDS contains k elements, then we speak of a (m, n, k, λ)-RDS. A group of order $8t$ containing a $(4t, 2, 4t, 2t)$-RDS is called a *Hadamard group* by Ito [38]. Following this usage, we call a $(4t, 2, 4t, 2t)$-relative difference set a *Hadamard relative difference set* (HRDS). The reason for this will become apparent in the remainder of this section.

If H is a Hadamard matrix, then the expanded matrix of H is

$$\mathcal{E}_H = \begin{pmatrix} H & -H \\ -H & H \end{pmatrix}.$$

We denote the subgroup of $\mathrm{PermAut}(\mathcal{E}_H)$ generated by the central involution

$$\left(\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}, \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}\right)$$

by Θ. Note that Θ is the image of $\langle(-I,-I)\rangle \leq \mathrm{Aut}(H)$ under the embedding ι of Lemma 2.83.

Lemma 3.5. *The Hadamard matrix H is cocyclic over G if and only if $\mathcal{E}_H$ is group developed over an extension $\Gamma \leq \mathrm{PermAut}(\mathcal{E}_H)$ of $\Theta \leq \Gamma$ by G.*

Proof. This is the restriction of Corollary 2.84 to the special case of Hadamard matrices, together with Theorem 2.68. Alternatively, see Section 16.2 of [16] or Theorem 3.24 of [58]. □

Lemma 3.6. *Suppose that H is a Hadamard matrix, and that $\Gamma \leq \mathrm{PermAut}(\mathcal{E}_H)$ contains Θ and acts regularly on $\mathcal{E}_H$. Then Γ contains a HRDS with forbidden subgroup Θ.*

Proof. Suppose that H has order $4t$. First, since Γ acts regularly on $\mathcal{E}_H$, we have that

$$\mathcal{E}_H = \left[\phi(gh^{-1})\right]_{g,h\in\Gamma}$$

for some function $\phi : \Gamma \to \langle -1\rangle$, where the first $4t$ rows and $4t$ columns of $\mathcal{E}_H$ are labelled by a set of representatives for the cosets of Θ in Γ. Let $R = \{g \in \Gamma \mid \phi(g) = 1\}$. We show that R is a HRDS.

Observe first that the inner product of the rows of $\mathcal{E}_H$ labelled by h and gh is

$$\sum_{k\in\Gamma} \phi(hk^{-1})\phi(ghk^{-1}) = \sum_{k\in\Gamma} \phi(k^{-1})\phi(gk^{-1}),$$

which is the inner product of the row labelled by g with the first row. Now, $\phi(k^{-1})\phi(gk^{-1}) = -1$ if exactly one of k^{-1} and gk^{-1} is in R, and $+1$ otherwise. The crucial observation here is that since $\mathcal{E}_H$ is the expanded matrix of a Hadamard matrix, any pair of distinct rows not of the form $\{r, -r\}$ is orthogonal. So $|R \cap gR| = 2t$, for $g \in \Gamma - \Theta$. But then the equation $r_i r_j^{-1} = g$ for $r_i, r_j \in R$ has precisely $2t$ solutions for $g \notin \Theta$.

Rows of $\mathcal{E}_H$ labelled by elements in the same coset of Θ have inner product $-8t$[1]. So $|gR \cap R| = 0$ for $g \in \Theta$, $g \neq 1$. Thus R is a HRDS as required. □

[1]This is the reason that we require $\Theta \trianglelefteq \Gamma$. Thus not every regular subgroup of $\mathrm{PermAut}(\mathcal{E}_H)$ corresponds to a cocycle of H.

In Lemma 3.6, we obtain a HRDS from a cocyclic Hadamard matrix. We can also proceed in the other direction.

Definition 3.7. Let R be a subset of a group Γ of order n. The *development* of R is the matrix

$$\mathrm{Dev}(R) = \left[\chi_R\left(ab^{-1}\right)\right]_{a,b\in\Gamma}$$

where $\chi_R(x) = 1$ if $x \in R$ and $\chi_R(x) = -1$ otherwise.

Theorem 3.8. *Suppose that R is a HRDS in a group Γ of order $8t$, with forbidden subgroup of order 2. Then $\mathrm{Dev}(R)$ is the expanded matrix of a cocyclic Hadamard matrix of order $4t$.*

Proof. The idea behind the proof is similar to that of Lemma 3.6.

Denote by z the unique non-trivial element in the forbidden subgroup. We have that $\Gamma = R \cup zR$. By definition, the rows and columns of $\mathrm{Dev}(R)$ can be labelled by the elements of Γ so that $\mathrm{Dev}(R) = \left[\phi(gh^{-1})\right]_{g,h\in\Gamma}$, where $\phi(gh^{-1}) = 1$ if $gh^{-1} \in R$ and $\phi(gh^{-1}) = -1$ otherwise.

For $r \in R$, the row labelled by zr is the negation of the row labelled by r: gh^{-1} is in R if and only if zgh^{-1} is not in R (since R is a transversal of $\langle z\rangle$ in Γ). Labelling the first $4t$ rows of $\mathrm{Dev}(R)$ with elements of R, and the first $4t$ columns with their inverses, we have that

$$\mathrm{Dev}(R) = \begin{pmatrix} M & -M \\ -M & M \end{pmatrix}.$$

By Lemma 3.6, it suffices to show that two rows of $\mathrm{Dev}(R)$ labelled by elements of R are orthogonal.

This is equivalent to showing that $|gR \cap hR| = 2t$ for any $g, h \in R$, $g \neq h$. But $|gR \cap hR|$ is the number of solutions of $r_i r_j^{-1} = g^{-1}h$, for $r_i, r_j \in R$, which by hypothesis is $2t$. The conclusion follows. □

So given a HRDS R in Γ of order $8t$, a cocyclic Hadamard matrix corresponds to a set of $4t$ linearly independent rows and columns in $\mathrm{Dev}(R)$. A canonical choice is the set of rows and columns labelled by the elements of R, in which case the Hadamard matrix so obtained is normalised. In any case, we state the result formally.

Theorem 3.9 (cf. Theorem 2.4 of [17])**.** *Let G be a group of order $4t$. Then there exists a Hadamard matrix cocyclic over G if and only if there exists a $(4t, 2, 4t, 2t)$-RDS in a central extension of $N \cong \mathrm{C}_2$ by G, with forbidden subgroup N.*

Proof. The 'if' direction follows from Theorem 3.8; the 'only if' from Lemmas 3.5 and 3.6. □

We have shown a relationship between cocyclic Hadamard matrices and relative difference sets. Unfortunately this relation is not well behaved in general: in the next section we deal with questions of equivalence.

Remark 3.10. Chapter 7 of [33] and Section 15.4 of [16] contain comprehensive discussions of relative difference sets corresponding to other kinds of cocyclic pairwise combinatorial designs.

3.2 Equivalence of HRDSs and Hadamard equivalence

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

Our definition of equivalence for RDSs differs from that in [33, p.164], in that we allow not just automorphisms, but antiautomorphisms (see Definition 2.43) of the containing group.

Definition 3.11 (cf. Definition 2.44)**.** Let $R, R' \subset G$ be (m, n, k, λ)-RDSs, with forbidden subgroups N and N' respectively. Then R is *equivalent* to R' if and only if there exist $g \in G$ and $\vartheta \in \mathrm{AntiAut}(G)$ such that $N^\vartheta = N'$ and $R' = R^\vartheta g$.

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

We write $M \approx M'$ if there exist permutation matrices P and Q such that $M = PM'Q^\top$.

Lemma 3.12. *Let $R \subset G$ be an RDS, $g \in G$ and $\zeta \in \mathrm{Aut}(G)$. Then*

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

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

For the second part, observe that $\mathrm{Dev}(R) = \left[\chi_R\left(gh^{-1}\right)\right]_{g,h\in G}$. Then $\mathrm{Dev}(R^{-1}) = \left[\chi_{R^{-1}}\left(g^{-1}h\right)\right]_{g,h\in G} = \left[\chi_R(hg^{-1})\right]_{g,h\in G} = \mathrm{Dev}(R)^\top$. (Note in particular that unless G is abelian, $\mathrm{Dev}(R)$ and its transpose need not be permutation equivalent.) □

Lemma 3.13. *Let H and H' be Hadamard matrices. Then $\mathcal{E}_H \approx \mathcal{E}_{H'}$ if and only if H and H' are equivalent as Hadamard matrices.*

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

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

This suffices for one direction of the proof.

Now, assume that $\mathcal{E}_H \approx \mathcal{E}_{H'}$. Then

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

where the first and third matrices are permutation matrices. Multiplying out these block matrices, we obtain four equations of the form

$$(P_\alpha - P_\beta)\, H \left(Q_\alpha^\top - Q_\beta^\top\right) = H'. \tag{3.1}$$

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

Note that this result can be extended in several directions. As an example, the equations (3.1) imply that $P_\alpha = P_\delta$, $P_\beta = P_\gamma$, $Q_\alpha = Q_\delta$ and $Q_\beta = Q_\gamma$, which imposes non-trivial restrictions on the automorphism group of an expanded matrix. In this chapter, we develop these ideas only enough for our purpose, which is the proof of Theorem 3.15.

Definition 3.14. Let $R \subset G$ be a HRDS with $\mathrm{Dev}(R) \approx \mathcal{E}_H$ for some cocyclic Hadamard matrix, H. We say that R is *associated with* H.

Theorem 3.15. *Suppose that R is a HRDS associated with H. If R is also associated with H' then H and H' are equivalent as Hadamard matrices. R is equivalent to a HRDS associated with $H^\top$. Furthermore, if R' is a HRDS equivalent to R then R' is equivalent to either H or $H^\top$.*

Proof. Immediate from Lemmas 3.12 and 3.13. □

Now, we have shown that a Hadamard matrix H is cocyclic if and only if $\mathcal{E}_H \approx \mathrm{Dev}(R)$ for some HRDS, R. Furthermore, any cocyclic Hadamard matrix, H', which is Hadamard equivalent either to H or $H^\top$ will have $\mathcal{E}_{H'} \approx \mathrm{Dev}(R')$, where R' is equivalent to R. Thus, to find representatives of all equivalence classes of cocyclic Hadamard matrices of order $4t$, up to transposition, it suffices to find all HRDSs in groups of order $8t$, up to equivalence. This list will not be irredundant in general, but can be made so using standard inequivalence tests for Hadamard matrices as implemented in Magma [7], for example.

3.3 Construction of relative difference sets

There is an extensive literature devoted to the study of difference sets in abelian groups. In contrast, difference sets in non-abelian groups have received relatively little attention. While multipliers have been defined for difference sets in non-abelian groups, there are no analogues of the multiplier theorems (see Section 5.2 for a discussion of multipliers). Likewise, results using characters and algebraic number theory fail to carry over to the non-abelian case.

It is unsurprising that there has been little attention paid to the theory of the more general relative difference sets. Our algorithm for the construction of RDSs in a group G is essentially a depth first backtrack search over the tree of all subsets of G. We outline some refinements to the search which make it feasible for the groups of order 64 and 72, as promised in the introduction to this chapter. The most important of these is a theorem of Bruck, generalised by Röder.

Theorem 3.16. *Let G be a group of order mn. Let R be a (m, n, k, λ)-RDS in G, with forbidden subgroup N, of order n. Let U be a normal subgroup of G, and denote by $T = \{g_1, g_2, \ldots, g_{|G:U|}\}$ a transversal of U in G. Furthermore, let $v_i = |R \cap g_i U|$ and $v_{ij} = |R \cap g_i g_j U|$. Then the following relations hold.*

$$\sum_{i \in T} v_i = k \tag{3.2}$$

$$\sum_{i \in T} v_i^2 = \lambda\left(|U| - |U \cap N|\right) + k \tag{3.3}$$

$$\sum_{j \in T} v_j v_{ij} = \lambda\left(|U| - |g_i U \cap N|\right) \text{ for } g_i \notin U. \tag{3.4}$$

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

canonical epimorphism of groups $\rho\colon G \to G/U$.

We have:

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

Hence

$$\vartheta(RR^{-1}) = \Big(\sum_{i=1}^{|G:N|} v_i g_i U\Big)\Big(\sum_{j=1}^{|G:N|} v_j g_j^{-1} U\Big) = \sum_{i=1}^{|G:N|}\Big(\sum_{j=1}^{|G:N|} v_j v_{ij}\Big) g_i U. \tag{3.5}$$

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

$$\vartheta(RR^{-1}) = k \cdot g_1 U + \lambda\Big(\sum_{g \in (G-N)} gU\Big) \tag{3.6}$$
$$= k \cdot g_1 U + \lambda\Big(\sum_{g_i \in T - \mathcal{N}} g_i U|U| - \sum_{g_i \in \mathcal{N}} g_i U|g_i U \cap N|\Big). \tag{3.7}$$

Comparing coefficients in (3.5) and (3.7), we get

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

and

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

□

We call $[v_i \mid 1 \leq i \leq |G:U|]$ a *signature* for R with respect to U. Note that the ordering of the signature depends on the ordering of the cosets of U.

A signature is entirely determined by the parameters of R and the index of U in G, so that we may speak of a signature for a given set of parameters in G, whether there exists a difference with these parameters or not. If the equations of Theorem 3.16 have no solution for a given group G, then there can be no relative difference set with the given parameters.

This result suggests the following algorithm for the construction of all (m, n, k, λ)-RDSs in the group G.

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

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

3. Calculate signatures (solutions of the equations of Theorem 3.16) with respect to every normal subgroup of index at most l for some suitable choice of l. (The signatures of subgroups of smaller index may be used in the reduction step.)
4. Find $U \trianglelefteq G$ with unique signature of the form $[i, \ldots, i]$ (all entries the same). Such a subgroup always exists in the cases we consider in Section 3.3.1.

Next, we generate all relative difference sets coset-wise.

Definition 3.17. We call $R \subset G$ a *partial relative difference set* (short: pRDS) with parameters $(4t, 2, 4t, 2t)$ relative to $N \trianglelefteq G$, if every element of $G - N$ can be written in at most $2t$ ways as a quotient in R, and no element of N can be expressed in this way. We say that a pRDS has *length* k if it contains k elements.

We start with the coset U and the set $P = \{\{1\}\}$ of partial difference sets (note that this can be done without loss of generality). For the reduction step (6) below, we use equivalence as defined in Definition 2.44 with a smaller automorphism group $A \leq (\mathrm{Aut}(G)_N)_U$ which acts trivially on G/U.

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

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

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

Remark 3.18. The choice of l, the maximal index of normal subgroups considered for generation of signatures, was determined by trial and error for the cases that we consider in Section 3.3.1. In general, the algorithm depends essentially on finding a normal subgroup with a suitable signature. Indeed, the algorithm may fail at Step 4 should it fail to find such a signature. In this case, the search branches in separate cases depending on the number of elements required in each of the cosets. We did not implement the algorithm in this more general setting: it was not necessary for the problem considered in this chapter.

3.3.1 Implementation for groups of order 64 and 72

We show there are only two signatures possible for a HRDS in a group of order 64. We consider a normal subgroup of order 16. This is permissible: a routine calculation shows that all groups of order 64 contain a normal subgroup of index 4.

Lemma 3.19. *Let G be a group of order 64 and let U be a normal subgroup of index 4. Suppose that R is a HRDS in G with forbidden subgroup N. Then the signature of R with respect to U is of one of two types:* $[6, 6, 10, 10]$, *or* $[8, 8, 8, 8]$. *Furthermore, signatures of the first kind occur only when $G/U \cong C_4$, and the non-trivial element of N lies in the unique coset of U of order 2.*

Proof. We simply apply the conditions of Theorem 3.16 to a HRDS in G. Now, from (3.2) we have that

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

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

- If $|U \cap N| = 1$, then by (3.3)

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

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

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

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

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

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

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

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

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

Remark 3.20. In fact every group of order 64 contains a normal subgroup with signature $[8, 8, 8, 8]$. So while some groups did contain normal subgroups with signature $[6, 6, 10, 10]$, it was not necessary for us to consider this case.

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

Lemma 3.21. *Let G be a group of order 72 and let U be a normal subgroup of index 6. Suppose that R is a HRDS in G with forbidden subgroup N. Then the signature of R is one of the following:*

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

The actual implementation of our algorithm uses Röder's GAP package 'rds' [68]. It differs slightly from the outline above, as we made use of the following heuristic methods.

1. The signatures calculated in step 3 can be used in the reduction step 6 as an invariant. See [66, 67] for details.
2. The reduction steps are very time-consuming, so steps 5 and 6 are not iterated i times, but a brute-force algorithm is used after fewer steps.

Also, steps 5 and 6 were not used for all cosets modulo U. Depending on the specific case, we used a brute-force method after a few cosets.

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

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

3.4 Classification of cocyclic Hadamard matrices of order less than 40

By 'classification' we mean a list of cocyclic Hadamard matrices which is complete and irredundant with respect to Hadamard equivalence. From these, the algorithm of Appendix A of [58] may be used to obtain cocycles. Relative difference sets, associated 2- and 3-designs or any other data of interest may also be recovered from this list using relatively standard techniques. As mentioned in the introduction to this chapter, a classification for Hadamard matrices of orders at most 28 was given in [58]. The methods of Section 3.3 were used to classify the cocyclic Hadamard matrices of orders 32 and 36, thus extending the classification to all cocyclic Hadamard matrices of order less than 40. The following table summarises our results. We list the number of cocyclic Hadamard matrices for all orders less than 40 (given as a fraction of the total number of Hadamard matrices where appropriate - these numbers are taken from [49] for order 32 and [61] for order 36). Likewise we list the number of indexing and extension groups at each order as a fraction of the total.

Order	Cocyclic	Indexing Groups	Extension Groups
2	1	1	2
4	1	2	3 / 5
8	1	3 / 5	9 / 14
12	1	3 / 5	3 / 15
16	5	13 / 14	45 / 51
20	3	2 / 5	3 / 14
24	16 / 60	8 / 15	14 / 52
28	6 / 487	2 / 4	2 / 13
32	$100/ \geq 13 \times 10^6$	49/51	261/267
36	$35 / \geq 18 \times 10^6$	12 /14	21 / 50

Table 1: Cocyclic Hadamard matrices of order less than 40.

All Hadamard matrices of order at most 20 are cocyclic. Beyond this, it seems that that the number of cocyclic Hadamard matrices is approximately proportional to the number of indexing groups. Results of Ito [38, Propositions 6,7] prove that a group of order $8t$ cannot contain a $(4t, 2, 4t, 2t)$-RDS if it has cyclic or dihedral type Sylow 2-subgroup. The existence of a cocyclic Hadamard matrix with cyclic indexing group of order greater than 4 would disprove the Circulant Hadamard conjecture. We observe that up to order 36, groups of lower exponent are more likely to be Hadamard groups.

The algorithm of Appendix A in [58] and the classification of Hadamard matrices in [71] were used to construct all cocyclic Hadamard matrices of order less than 30. The algorithm of Section 3.3 and information from the Small Groups Library, available in MAGMA [7], were used to generate all $(4t, 2, 4t, 2t)$-RDSs in groups of orders $40, 48, 56, 64$ and 72, whence all cocyclic Hadamard matrices of orders $20, 24, 28, 32$ and 36 were obtained. Both classifications agreed on their intersection.

The classification of cocyclic Hadamard matrices of order 32 is, to our knowledge, entirely new. The classification of cocyclic Hadamard matrices of order 36 was begun by Ito and Okomoto [41], who found 15 matrices, but is completed here. We conclude this chapter with some more detailed information on the data generated at orders 32 and 36.

3.4.1 Selected data

In general, H and $H^\top$ need not be equivalent as Hadamard matrices. Their automorphism groups are isomorphic however, with an obvious bijection between regular subgroups. Thus the cocyclic development properties of H and $H^\top$ are the same, so for the purposes of this section we introduce the notion of *strong inequivalence*, where we add transposition to equivalence relations for Hadamard matrices.

Of the 100 classes of cocyclic Hadamard matrices of order 32, there are precisely 30 pairs of classes $\{H_i\}, \{H_j\}$ $i \neq j$ such that $H_i^\top$ is Hadamard equivalent to H_j. The remaining 40 equivalence classes are closed under transposition. Thus we obtained 70 strongly inequivalence classes of Hadamard matrices, of which 40 classes are equivalent to their transpose classes and 30 are not. We describe the automorphism groups of these matrices in the two tables following. Where we could not find a nice description of a group, we describe it as an extension K of a normal subgroup by a quotient group (represented as a truncated exact sequence). Note in particular, that K represents a different group in each line of the table. The dihedral, quasidihedral and quaternion groups of order n are denoted $D_{\frac{n}{2}}$, QD_n and Q_n respectively.

$\lvert\mathrm{Aut}(H)\rvert$	Description	Remarks
64	$C_{16} \rtimes C_4$	
64	Q_{64}	4 matrices
64	$C_2^3 \to G \to D_4$	
64	$C_4 \rtimes Q_{16}$	
128	$C_{16} \to G \to D_4$	
128	$C_8 \to G \to C_2 \times D_4$	3 matrices
128	$(C_{16} \times C_4) \rtimes C_2$	
128	$C_{32} \to G \to C_2^2$	2 matrices
128	$C_2^3 \to G \to C_2 \times D_4$	central extension
128	$C_2^3 \to G \to D_8$	2 matrices
128	$C_2 \to G \to D_4^2$	2 matrices, central extension
192	$C_2^3 \to G \to S_4$	$Z(Syl_2(G)) = C_2 \times C_4$
192	$C_2^3 \to G \to S_4$	$Z(Syl_2(G)) = C_2^3$, 2 matrices
256	$C_{16} \to G \to C_2 \times D_4$	SmallGroup 26854
256	$C_{16} \to G \to C_2 \times D_4$	SmallGroup 26843
256	$C_2^2 \to G \to C_2^3 \times D_4$	central extension, SmallGroup 54577
256	$C_2^2 \to G \to C_2^3 \times D_4$	central extension, SmallGroup 55556
256	$C_2^2 \to G \to C_2^3 \times D_4$	central extension, SmallGroup 55593
256	$C_8 \to G \to C_2^4 \rtimes C_2$	SmallGroup 26530
320	$(C_2 \times Q_8) \rtimes C_2 \to G \to D_5$	
512	$C_8 \to G \to D_4^2$	
512	$C_2^4 \to G \to (C_2 \times D_4) \rtimes C_2$	
512	$C_2^4 \to G \to D_{16}$	
512	$C_8 \to G \to K$	K a group of order 64, exponent 4
512	$C_2^4 \to G \to C_2^4 \rtimes C_2$	
512	$C_2^3 \to G \to D_4^2$	

Table 2: Automorphism groups of order ≤ 1000

It is notable that only the automorphism groups of the Sylvester and Paley matrices are doubly transitive on rows. We give an extended discussion of the Sylvester and Paley matrices later, in Chapter 4. Indeed, Chapters 4 and 5 are concerned with Hadamard matrices that have doubly transitive automorphism groups in general. We note also the relative paucity of Hadamard matrices with non-solvable automorphism groups. It is likely that each of these is built in some manner from Hadamard matrices of order 8: the non-solvable factors occurring all have distinguished actions on 8 points. If so, it would be interesting to learn if these constructions are known, and if they generalise to larger orders.

$\lvert\mathrm{Aut}(H)\rvert$	Description	Remarks
1024	$C_2^2 \to G \to K$	$C_2^3 \to K \to C_2^5$
1024	$C_2^2 \to G \to K$	$C_2^3 \to K \to C_2^5$
1024	$C_2 \to G \to K$	$C_2^4 \to K \to C_2^5$, two matrices
1024	$C_2 \to G \to K$	$C_2^4 \to K \to C_2^5$
1152	$C_2 \to G \to C_{36} \times D_8$	
1536	$C_2^6 \to G \to C_2 \times A_4$	
1536	$C_2^2 \times GL_2(3) \to G \to D_8$	
2048	$C_2^7 \to G \to D_8$	
3072	$C_2 \to G \to K$	$C_2^5 \to K \to D_4 \times S_3$, central
8192	$C_2^2 \times C_4^2 \to G \to C_2^6 \rtimes C_2$	
8192	$C_2^4 \times C_4^2 \to G \to C_2^4 \rtimes C_2$	
8192	$C_2^5 \to G \to K$	$\lvert K\rvert = 256$, exponent 8
8192	$C_2^7 \to G \to K$	$\lvert K\rvert = 64$, exponent 4
10752	$C_2^5 \to G \to PGL_2(7)$	
10752	$C_2^6 \to G \to C_2^3 \rtimes F_{21}$	F_{21} Frobenius of order 21
16384	$C_2^7 \to G \to D_4^2 \rtimes C_2$	
16384	$C_2^4 \to G \to K$	$\lvert K\rvert = 1024$, exponent 8
29760	$SL_2(31)$	Paley I Matrix
32768	$C_2^5 \to G \to K$	$C_2^5 \to K \to C_2^5$
32768	$C_2^5 \to G \to K$	$C_2^4 \times C_4 \to K \to C_2^4$
32768	$C_2^8 \to G \to K$	$C_2^4 \to K \to C_2^3$
98304	$C_2^5 \to G \to K$	$C_2^6 \to K \to D_4 \times S_3$
122880	$C_2^5 \to G \to K$	$C_2^5 \to K \to S_5$
131072	$C_2^{10} \to G \to D_4^2 \rtimes C_2$	
688128	$C_2^{10} \to G \to K$	$C_2 \to K \to PGL_2(7)$
688128	$C_2^{10} \to G \to K$	$C_2 \to K \to PGL_2(7)$, 2 matrices
786432	$C_2^6 \to G \to K$	$C_2^8 \to K \to D_4 \times S_3$, two matrices
786432	$C_2^4 \to G \to K$	$C_2^8 \to K \to (C_2 \times D_4 \times S_3) \rtimes C_2$
917504	$C_2^4 \to G \to K$	$C_2^{12} \to K \to C_{14}$
1048576	$C_2^{10} \to G \to K$	$C_2^6 \to K \to D_8$
18874368	$C_2^{12} \to G \to K$	$C_2^5 \to K \to S_3 \times S_4$
20478689280	$C_2^6 \rtimes AGL_5(2)$	Sylvester matrix

Table 3: Automorphism groups of order > 1000

We obtain 35 equivalence classes of cocyclic Hadamard matrices of order 36, of which 17 classes are self-transpose equivalent, and 18 are not. Thus there are 26 strongly inequivalent classes of cocyclic Hadamard matrices at order 36.

At order 36, all of the full automorphism groups act imprimitively on the rows of their corresponding matrices. Furthermore, the Paley II Hadamard matrix of this order has a non-solvable automorphism group, containing a subgroup isomorphic to $PSL_2(17)$. The occurrence of $SL_2(3)$ and $GL_2(3)$ suggests that some of these matrices may have natural constructions over $\mathbb{F}_9$. Again, it would be interesting to examine the matrices and their automorphism groups for possible new algebraic constructions of Hadamard matrices. Note that there are many matrices with full automorphism groups of order 72, i.e. the automorphism group acts regularly on the expanded matrix.

$\lvert\mathrm{Aut}(H)\rvert$	Description	Remarks
72	$C_3^2 \rtimes Q_8$	4 matrices
72	$C_3 \times SL_2(3)$	2 matrices
72	$C_3 \times (C_3 \rtimes Q_8)$	3 matrices
72	$C_3^2 \rtimes Q_8$	
144	$Q_8 \times D_9$	
144	$(C_3 \rtimes Q_8) \times S_3$	
144	$((C_{12} \times C_2) \rtimes C_2) \times C_3$	
216	$(C_9 \times Q_8) \rtimes C_3$	
216	$(C_3^2 \times Q_8) \rtimes C_3$	
432	$((C_9 \times Q_8) \rtimes C_3) \rtimes C_2$	
432	$C_3 \times S_3 \times SL_2(3)$	
432	$C_2 \times (C_6^2 \rtimes C_3) \rtimes C_2$	
1152	$C_6^2 \to G \to C_2 \times QD_{16}$	
1296	$C_3^4 \to G \to (C_2 \times C_4) \rtimes C_2$	
1728	$(Q_8 \times (C_3^2 \rtimes Q_8)) \rtimes C_3$	
1944	$C_3^4 \to G \to SL_2(3)$	
3456	$C_2 \times C_6^2 \to G \to GL_2(3)$	
3888	$C_3^4 \to G \to C_2 \times S_4$	
19584	$PSL_2(17) \to G \to Q_8$	Paley II Matrix
31104	$K \to G \to S_4$	$C_3^4 \to K \to C_2 \times Q_8$

Table 4: Automorphism groups of cocyclic Hadamard matrices of order 36

4 Cocyclic Hadamard matrices from difference sets

In this chapter we turn from the computational work of Chapter 3 to more theoretical work. For a Hadamard matrix H, we study the action of the permutation group $\mathcal{A}(H)$ on the rows of H. Detailed structural information is given in the special case that $\mathcal{A}(H)$ is a non-affine doubly transitive group. A corollary of this result is a partial classification of cocyclic Hadamard matrices H developed from difference sets (as per Definition 2.60).

4.1 The action of a permutation group on a Hadamard matrix

Let H be a Hadamard matrix. We described the permutation action of $\mathrm{Aut}(H)$ on the rows and columns of $\mathcal{E}_H$ in Lemma 2.83. It is clear that this action is never primitive on rows: a system of imprimitivity consists of the pairs of rows $\{r, -r\}$. In fact, this can be a maximal system of imprimitivity in the sense that the induced action of $\mathrm{Aut}(H)$ on the set of pairs $\{r, -r\}$ is primitive (even doubly transitive). This is the action considered by Kantor and by Ito in [46] and [37] respectively.

Equivalently, Kantor and Ito's action may be described in terms of Definition 2.55. We observe that this action no longer consists of automorphisms of any obvious incidence structure associated with H. We outline some of the properties of $\mathcal{A}(H)$ in the remainder of this section.

Lemma 4.1. *The kernel of the map $\nu : \mathrm{Aut}(H) \to \mathcal{A}(H)$ consists of matrices diagonal in the first component.*

Proof. Suppose that $(P, Q) \in \mathrm{Ker}(\nu)$. Then $E_P = I$, so P is a diagonal matrix. □

The next theorem is due to Ito. We give a proof that is somewhat less terse than the original.

Theorem 4.2 ([39], Lemma 1)**.** *Suppose that $\mathcal{A}(H)$ acts 2-transitively on the rows of H and that $\mathrm{Ker}(\nu)$ is not $\langle\zeta\rangle$, where $\zeta = (-I, -I)$. Then H is a Sylvester matrix*[1]*.*

Proof. An automorphism (P, Q) of H such that P is a diagonal matrix is called a *dilatation* by Kimberley [50]. A dilatation which is in $\langle\zeta\rangle$ or which does not fix any column is called a *translation*. Theorem 8 of [50] states that a Hadamard matrix H with a transitive group of translations is equivalent to a Sylvester matrix. We show that $\mathrm{Ker}(\nu)$ is such a transitive translation group for H.

First, we observe that $(P, Q) \in \mathrm{Ker}(\nu)$ implies that $P^2 = I$, so that every non-identity element of $\mathrm{Ker}(\nu)$ has order 2. Hence $\mathrm{Ker}(\nu)$ is an elementary abelian group containing ζ. Note that every element of $\mathrm{Ker}(\nu)$ is a dilatation.

We describe an incidence structure on which $\mathrm{Ker}(\nu)$ has non-trivial action. Suppose that $H = [h_{i,j}]_{i,j}$ has order $4n$. Define a set $P = \{1, 2, \ldots, 4n, 1^*, 2^*, \ldots, 4n^*\}$ of points and a set of blocks $B = \{b_1, b_2, \ldots, b_{4n}, b_1^*, b_2^*, \ldots, b_{4n}^*\}$ with i incident to b_j if $h_{i,j} = 1$, and i^* incident to b_j otherwise. Set $b_j^* = P - b_j$ and $\Delta = (P, B)$. For any $x, y \in B$ we observe that $x \cap y = 2n$ if $y \neq x, x^*$. The elements of P are identified with the rows of H and their negations, which induces an action of $\mathrm{Aut}(H)$ on Δ. We denote by $\overline{P}$ the system of imprimitivity given by the blocks $\overline{x} = \{x, x^*\}$ for $x \in P$. Then the induced action of $\mathrm{Aut}(H)$ on $\overline{P}$ is permutation isomorphic to the action of $\mathcal{A}(H)$ on the rows of H.

Now, choose $\sigma \in \mathrm{Ker}(\nu) - \langle\zeta\rangle$. Then there exist i and j in P such that $i^\sigma = i^*$ and $j^\sigma = j$. Hence the action of σ on B is fixed-point-free: σ is a translation. Now $\mathrm{Ker}(\nu)$ is semiregular on B, so $|\mathrm{Ker}(\nu)| \leq 8n$.

Let b be an arbitrary block. Then $(b \cap b^\sigma) \cup (b^* \cap (b^*)^\sigma)$ is the fixed point set of σ. Now, $|(b \cap b^\sigma)| = |(b^* \cap (b^*)^\sigma)| = 2n$. Thus σ fixes $4n$ points in total. Let $F(\sigma) = \{\overline{x} \mid x^\sigma = x\}$. Then $|F(\sigma)| = 2n$, and $F(\sigma)$ uniquely determines σ.

Denote by u the number of distinct sets $F(\sigma)$, so $u = |\mathrm{Ker}(\nu)| - 2$. Let $\overline{x}$ and $\overline{y}$ be distinct elements of $\overline{P}$, and denote by v the number of distinct $F(\sigma)$ which contain both $\overline{x}$ and $\overline{y}$. By hypothesis, the action of $\mathcal{A}(H)$ on $\overline{P}$ is doubly transitive. It follows that v is independent of the choice of $\overline{x}$ and $\overline{y}$:

$$\begin{aligned} v\binom{4n}{2} &= u\binom{2n}{2} \\ \Rightarrow v &= (2n-1)\frac{u}{2(4n-1)} \end{aligned}$$

But v is an integer, so $2(4n-1)$ divides u. The action of $\mathrm{Ker}(\nu)$ is semiregular, so

[1] We describe the Sylvester matrices in detail in Section 4.3.2.

$|\mathrm{Ker}(\nu)| = u + 2 \leq 8n$. Hence $u = 8n - 2$, and $\mathrm{Ker}(\nu)$ is transitive on the columns of H, and H is equivalent to a Sylvester matrix. □

In particular, if H is a Hadamard matrix with non-affine doubly transitive automorphism group (recall: we mean here that $\mathcal{A}(H)$ is non-affine doubly transitive), then $\mathrm{Ker}(\nu) = \langle\zeta\rangle$.

Suppose that H is a Hadamard matrix developed from a symmetric design $\mathcal{S}$. Then $\mathrm{Aut}(\mathcal{S}) \cong \mathrm{PermAut}(H)$ by Lemma 2.59. We show that $\mathcal{A}(H)$ contains a subgroup isomorphic to $\mathrm{Aut}(\mathcal{S})$.

Lemma 4.3. *Let H be a Hadamard matrix. Then* $\mathrm{PermAut}(H) \cong \nu(\mathrm{PermAut}(H))$.

Proof. By Lemma 4.1, $\mathrm{Ker}(\nu) \cap \mathrm{PermAut}(H) = (I, I)$: a diagonal permutation matrix is necessarily the identity. □

By Lemma 2.59, $\mathrm{PermAut}(H) \cong \mathrm{Aut}(\mathcal{S})$ where $\mathcal{S}$ is the underlying 2-design of H. We denote $\nu(\mathrm{PermAut}(H))$ by $\mathcal{A}(\mathcal{S})$ and bound the index of $\mathcal{A}(\mathcal{S})$ in $\mathcal{A}(H)$.

Lemma 4.4. *Let H be a normalised Hadamard matrix of order $4t$ developed from the symmetric design $\mathcal{S}$. Then $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| \leq 16t^2$.*

Proof. Note that $\mathcal{A}(\mathcal{S}) \leq \mathcal{A}(H)_1$, so

$$|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| = |\mathcal{A}(H) : \mathcal{A}(H)_1| \cdot |\mathcal{A}(H)_1 : \mathcal{A}(\mathcal{S})| .$$

By the Orbit-Stabiliser theorem $|\mathcal{A}(H) : \mathcal{A}(H)_1| \leq 4t$.

Consider the group $G = \{Q \mid \nu(P, Q) \in \mathcal{A}(H)_1\}$. If $Q \in G$ then either Q or $-Q$ is a permutation matrix. Denote by G^+ the subgroup of permutation matrices in G. We observe that $|G| = 2\,|\mathcal{A}(H)_1|$, hence $|G^+| = |\mathcal{A}(H)_1|$.

Suppose that $Q \in G^+$ fixes the first column of H. Then $(P, Q) \in \mathrm{PermAut}(H)$ and so induces an automorphism of $\mathcal{S}$. Thus G_1^+ is isomorphic to a subgroup of $\mathrm{PermAut}(H)$. But it is easily seen that $\mathrm{PermAut}(H) \leq G_1^+$, hence $\mathrm{PermAut}(H) \cong G_1^+$.

So $|\mathcal{A}(\mathcal{S})| = \left|G_1^+\right|$, from which it follows that $|\mathcal{A}(H)_1 : \mathcal{A}(\mathcal{S})| = \left|G^+ : G_1^+\right| \leq 4t$. □

Known restriction on the orders of automorphisms of both Hadamard matrices and Paley-Hadamard designs could be used to improve the bound of Lemma 4.4. We do not explore this topic; instead, we impose some further conditions on $\mathcal{A}(H)$ and $\mathrm{Aut}(\mathcal{S})$.

Lemma 4.5. *Let H be a normalised Hadamard matrix of order $4t$ developed from the symmetric design $\mathcal{S}$. Suppose that* $\mathrm{Aut}(\mathcal{S})$ *is transitive on the points of $\mathcal{S}$. Then* $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| \in \{1, 4t, 16t^2\}$.

Proof. By Theorem 2.41, $\mathrm{Aut}(\mathcal{S})$ is transitive on the blocks of $\mathcal{S}$. Then, using the notation in the proof of Lemma 4.4, we observe that $|\mathcal{A}(H) : \mathcal{A}(H)_1|$ and $\left|G^+ : G_1^+\right|$ are each $4t$ or 1 depending on whether $\mathcal{A}(H)$ and G^+ are transitive or intransitive. Since $|\mathcal{A}(H)_1 : \mathcal{A}(\mathcal{S})| = \left|G^+ : G_1^+\right|$, the lemma follows. □

Clearly, if $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| = 1$, then $\mathcal{A}(H)$ is isomorphic to $\mathrm{Aut}(\mathcal{S})$, in which case we do not gain any further information on either $\mathcal{S}$ or H. The situation is quite different in the other two cases of Lemma 4.5. We begin with a technical lemma, and a statement of a theorem of Ito.

Lemma 4.6. *Let G be an affine doubly transitive permutation group of degree $n = 2^k$ with character $\chi_1 + \chi_\rho$, where χ_1 is the trivial character, ρ is irreducible of degree $n - 1$. Consider the natural permutation representation of G in $GL_n(\mathbb{C})$ whose ordinary character is $\chi_1 + \chi_\rho$.*

Suppose further that ρ is monomial, so $\rho(g) = D_g E_g$ for diagonal and permutation matrices D_g and E_g respectively. Then the permutation representation $\pi : \rho(g) \mapsto E_g$ is not faithful.

Proof. First: G is of affine type, so $G = VH$ where V is an elementary abelian normal subgroup, and H is a point stabiliser. Let $\rho(G)$ act on the $n-1$-dimensional $\mathbb{C}$-vector space W. Since ρ is monomial by hypothesis, W decomposes as a direct sum of 1-dimensional subspaces, which are permuted by ρ under ordinary matrix multiplication.

We observe that $\chi_{\rho(v)} = -1$ for any $v \in V$. But V is the socle of G, so ρ is faithful.

Now, $\rho(u) = \rho(v) = -1$ for arbitrary $u, v \in V$. So there exist subspaces W_u and W_v of W such that $x_u^u = -x_u$ and $x_v^v = -x_v$ for $x_u \in W_u$ and $x_v \in W_v$. These subspaces may be chosen to be distinct: otherwise $x_u^{uv} = x_u$, but $\rho(uv) = -1$, so there is a third subspace negated by exactly one of u and v.

Suppose that $W_u^v = X \neq W_u$. Then $W_u^{uv} = W_u^{vu}$, which implies that $X^u = -X$. But v was arbitrary, so we see that u fixes every 1-dimensional subspace of W. And v is conjugate to u in G: so it must also fix every 1-dimensional subspace.

Diagonal matrices commute, so because V is self-centralising in G, we have that $\mathrm{Ker}(\rho) = V$, and the projection $\pi(\rho(G))$ is isomorphic to H. □

The next theorem is truly fundamental for our purposes in this chapter.

Theorem 4.7 (Ito, [37]). *Let H be a Hadamard matrix such that $\mathcal{A}(H)$ is non-affine and doubly transitive. Then the action of $\mathcal{A}(H)$ is one of the following.*

- $\mathcal{A}(H) \cong M_{12}$ *in its natural action on* 12 *points.*
- $PSL_2(p^k) \trianglelefteq \mathcal{A}(H)$ *acting naturally on* $p^k + 1$ *points, for* $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.
- $\mathcal{A}(H) \cong Sp_6(2)$ *acting on* 36 *points.*

Theorem 4.8. *Let H be a normalised Hadamard matrix of order $4t$ developed from the symmetric design $\mathcal{S}$. Suppose that* $\mathrm{Aut}(\mathcal{S})$ *is transitive and $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| \geq 4t$. Then $\mathcal{A}(H)$ is doubly transitive. If $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| = 16t^2$ then H is a Sylvester matrix, or H is of order* 12.

Proof. First, $\mathcal{A}(H)_1$ is transitive on the remaining rows of H, and G_1^+ is transitive on the remaining columns of H. If $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| \geq 4t$, then either $\mathcal{A}(H)$ is transitive on the rows of H, in which case $\mathcal{A}(H)$ is doubly transitive by Lemma 2.10; or else G^+ is doubly transitive on the columns of H, in which case we replace H by $H^\top$ without loss of generality.

Continuing with the notation of Lemma 4.4, we see that $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| = 16t^2$ precisely when G^+ is a doubly transitive permutation group on the columns of H. Now, observe that G^+ is the projection of a subgroup of $\mathrm{Aut}(H)$ onto one of its components. So G^+ is isomorphic to a section of $\mathrm{Aut}(H)$.

Consider the group $K = \langle P \mid (P, Q) \in \mathrm{Aut}(H) \text{ for some } Q \in G^+ \rangle$. Since $Q = H^{-1}PH$, we have that K and G^+ are similar as matrix groups, though K is not a permutation group. Note that every element of K fixes the first row of H, so that each element decomposes as a direct sum of the trivial representation of G^+ and a faithful monomial representation ρ of G^+ of degree $4t - 1$. Note that ρ is not a permutation matrix representation: G contains a fixed-point-free element, so some element $\rho(g)$ has trace -1.

Now, consider the projection $\pi : P \mapsto E_P$, restricted to ρ. In the case that G^+ is of affine type, the kernel of π is non-trivial by Lemma 4.6. Since every element of $\mathrm{Ker}(\pi)$ lifts to an element of $\mathrm{Ker}(\nu)$, we have that $\mathrm{Ker}(\nu)$ is larger than $\langle (-I, -I) \rangle$. By Theorem 4.2, H is a Sylvester Hadamard matrix.

In the case that G^+ is almost simple, we have the following.

- $\mathcal{A}(H)$ is 2-transitive on $4t$ points.
- G^+ is a subgroup of index $4t$ of $\mathcal{A}(H)$, and is 2-transitive on $4t$ points.

- $\mathrm{Ker}(\pi)$ is trivial, and so G^+ also has a transitive permutation representation on $4t-1$ points.

It is possible to determine the non-affine doubly transitive groups satisfying these conditions. We use Theorem 4.7 and the classification of doubly transitive permutation groups to conclude the proof.

Suppose that K is almost simple. But then $K \leq \mathcal{A}(H^\top)$ is doubly transitive on the rows of a Hadamard matrix and Theorem 4.7 applies. We consider each case in turn. The point stabiliser of $P\Sigma L_2(q)$ is a subgroup of $A\Gamma L_1(q)$, which cannot have a transitive action on $q+1$ points. So this case does not yield an example. The point stabiliser of $Sp_6(2)$ is S_8, but S_8 has no doubly transitive permutation representation on 36 points. Finally, the stabiliser of a point in M_{12} is M_{11}, which has an induced 3-transitive action on 12 points. It can be verified that this is indeed the action of K on the columns of the Hadamard matrix of order 12. Hence $\mathrm{Aut}(\mathcal{S}) \cong PSL_2(11)$ in this case, which is of index 144 in M_{12}. □

Corollary 4.9. *Let H be a Hadamard matrix developed from a symmetric design $\mathcal{S}$ with $\mathcal{A}(H)$ non-affine doubly transitive and $\mathrm{Aut}(\mathcal{S})$ transitive. Then H is of order 12, or $\mathrm{Aut}(\mathcal{S}) \cong \mathcal{A}(H)_1$.*

Proof. If H is not of order 12, then by Theorem 4.8 and hypothesis, $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| = 4t$. By transitivity of $\mathcal{A}(H)$, $|\mathcal{A}(H) : \mathcal{A}(H)_1| = 4t$. Since $\mathcal{A}(\mathcal{S}) \leq \mathcal{A}(H)_1$, the result follows. □

4.2 Cocyclic Hadamard matrices from difference sets

Suppose that H is a cocyclic Hadamard matrix which is also developed from a difference set. In this section we show that $\mathcal{A}(H)$ is necessarily a doubly transitive permutation group.

Lemma 4.10. *Let H be a (normalised) Hadamard matrix developed from a difference set $\mathcal{D}$. Then $\mathcal{A}(H)_1$ is transitive on the non-initial rows of H.*

Proof. Let $\mathcal{S}$ be the symmetric design underlying $\mathcal{D}$. Then $\mathrm{Aut}(\mathcal{S})$ is transitive on the points of $\mathcal{S}$ by Theorem 2.47. By Theorem 2.57, Lemma 2.59 and Lemma 4.3, the action of $\mathcal{A}(\mathcal{S})$ on the non-initial rows of H is permutation isomorphic to the action of $\mathrm{Aut}(\mathcal{S})$ on the points of $\mathcal{S}$. Thus $\mathcal{A}(H)_1$ is transitive on the non-initial rows of H. □

Lemma 4.11 (Cf. Lemma 6, [60]). *Let H be a cocyclic Hadamard matrix. Then $\mathcal{A}(H)$ is transitive.*

Proof. Let H be a cocyclic Hadamard matrix, with cocycle $\psi : G \times G \to \langle -1 \rangle$. The cocycle equation can be written as

$$\psi(g, hk) = \psi(g, h)\psi(gh, k)\psi(h, k). \tag{4.1}$$

Now define $\delta_y^{xa} = 1$ if $y = xa$, and 0 otherwise. Define the following monomial matrices for all $a \in G$:

$$P_a = [\psi(x, a)\delta_y^{xa}]_{x,y\in G}, \quad Q_a^\top = [\psi(a, a^{-1}y)\delta_{a^{-1}y}^x]_{x,y\in G}.$$

Then (P_a, Q_a) is an automorphism of H for all $a \in G$; the proof is as in Lemma 2.81.

Now, $\nu((P_a, Q_a)) = \left[\delta_y^{xa}\right]_{x,y\in G}$, and so we see that $\mathcal{A}(H)$ contains the subgroup $\left\{\left[\delta_y^{xa}\right]_{x,y\in G} \mid a \in G\right\} \cong G$ acting regularly on the rows of H. Thus $\mathcal{A}(H)$ is transitive on the rows of H. □

Theorem 4.12 (Cf. Lemma 11, [60]). *If H is a cocyclic Hadamard matrix developed from a $(4n-1, 2n-1, n-1)$-difference set as in Lemma 2.57 and Theorem 2.47, then $\mathcal{A}(H)$ is doubly transitive.*

Proof. This follows directly from Lemmas 2.10, 4.11 and 4.10. □

In the remainder of this Chapter, we classify the Hadamard matrices with non-affine doubly transitive permutation groups. We also classify extension groups and difference sets (if any) for each matrix.

4.3 Hadamard matrices with doubly transitive automorphism groups

As evidenced by Theorem 4.2 and Corollary 4.9, Hadamard matrices H with $\mathcal{A}(H)$ non-affine doubly transitive are well behaved, in some sense. We begin this section with two examples of families of Hadamard matrices with $\mathcal{A}(H)$ doubly transitive. In both cases, we define these matrices in terms of difference sets. These families of difference sets, along with others, will be discussed more fully in Section 5.1.

4.3.1 Paley matrices

Definition 4.13. Let $q \equiv 3 \mod 4$ be a prime power. As we noted in Remark 2.46 the quadratic residues of $\mathbb{F}_q$ form a difference set in the additive group of $\mathbb{F}_q$. Such a difference set is known as a *Paley difference set*. A *Paley design* is the underlying symmetric 2-design of a Paley difference set, and a *Paley matrix* is a Hadamard matrix developed from a Paley difference set (these are generally known as Type I Paley matrices.)

Remark 4.14. We caution the read that a Paley difference set belongs to the family described in Definition 4.13, while Paley-Hadamard is a generic term for any difference set with parameters $(4t-1, 2t-1, t-1)$.

The Paley matrices are well studied. In [27], Hall demonstrates that $PSL_2(q)$ is a subgroup of the automorphism group of the Paley matrix of order $q+1$. This result was later extended by Kantor, who determined the full automorphism group.

Theorem 4.15 ([46], [18])**.** *Let H be a Paley matrix of order $p^n + 1 > 12$. Then $\mathrm{Aut}(H)$ is an extension of C_2 by $P\Sigma L_2(p^n)$ (that is, $PSL_2(p^n)$ extended by field automorphisms).*

Thus for a Paley matrix H of order > 12, we have that $\mathcal{A}(H) \cong P\Sigma L_2(p^n)$ in its natural action. We begin with an investigation of the natural action of $PSL_2(q)$ on the projective line. We restrict attention to the case $q > 11$, $q \equiv 3 \mod 4$ to avoid the consideration of some exceptional small cases. (for example the exceptional action of $PSL_2(11)$ on 11 points, the isomorphism $PSL_2(4) \cong PSL_2(5)$, etc.)

We recall that the affine plane over $\mathbb{F}_q$ is simply a two dimensional vector space V over $\mathbb{F}_q$. Now, observe that the points $(0,0)$ and $(x,1)$ determine a unique line in V; hence the lines passing through the origin in V are in bijection with the non-zero elements of $\mathbb{F}_q$. Henceforth, we identify the line through $(0,0)$ and $(x,1)$ with x. We label the line $\langle(1,0)\rangle$ by ∞, and denote by $X = \mathbb{F}_q \cup \{\infty\}$ this set of lines in V.

Lemma 4.16. *The set X is closed under the induced action of $GL_2(q)$. The kernel of this action consists of scalar matrices, and the image is $PGL_2(q)$.*

Proof. First, $GL_2(q)$ fixes $(0,0)$, and by definition its action is linear, and so maps lines to lines. It is easily verified that $\mathbb{F}_q \cup \{\infty\}$ is a complete and irredundant list of the lines through the origin. A scalar matrix is easily seen to lie in the kernel. Conversely, if M is in the kernel then M fixes every line setwise, and thus is seen to be a scalar matrix. □

We describe the action of $PGL_2(q)$ on X. Consider the following matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax+b \\ cx+d \end{pmatrix}.$$

But the point $(ax+b, cx+d)$ lies on a unique line in X, given by $(\frac{ax+b}{cx+d}, 1)$, when $cx+d \neq 0$. If $cx+d=0$, then the image of x is ∞. Thus the action of $PGL_2(X)$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = \frac{ax+b}{cx+d}$$

for any $x \in X$. The rules for the manipulation of ∞ are easily obtained by referring to the action of $GL_2(q)$ on V. We observe that the action of $PGL_2(q)$ on X is transitive.

Lemma 4.17. *The stabiliser of a point in the action of $PGL_2(q)$ on X is isomorphic to $AGL_1(q)$.*

Proof. The stabiliser of ∞ has order $q(q-1)$. Observe that the matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

with $a \neq 0$ stabilise ∞, are $q(q-1)$ in number, and are closed under multiplication. Hence, they form the full stabiliser of a point. Observe that this is precisely the group of affine transformations of a 1-dimensional vector space over $\mathbb{F}_q$. □

Since the action of $AGL_1(q)$ on $\mathbb{F}_q$ is sharply 2-transitive, we have shown that $PGL_2(q)$ is in fact sharply triply transitive. We now consider $PSL_2(q)$.

Lemma 4.18. *Up to isomorphism the group $PSL_2(q)$ is a (simple) subgroup of $PGL_2(q)$ of index 2. Its action on X is 2-transitive, and the stabiliser of 2 points has 2 orbits on the remaining points of X, consisting of quadratic residues and quadratic non-residues respectively.*

Proof. First, we observe that the determinant of a scalar matrix aI_2 is necessarily a quadratic residue. Now construct a homomorphism $\pi : PGL_2(q) \to \langle -1 \rangle$ such that $\pi(g) = 1$ if and only if the determinant of a preimage of g in $GL_2(q)$ is a quadratic residue. Then $\ker(\pi) = PSL_2(q)$.

Now, the action of $PSL_2(q)$ on X is transitive, and the stabiliser of a point is a subgroup of index 2 in $AGL_1(q)$ (it is **not** $ASL_1(q)$!), given by matrices of the form

$$\begin{pmatrix} a^2 & b \\ 0 & 1 \end{pmatrix}.$$

This group remains transitive on $X - \{\infty\}$. Now observe that the pointwise stabiliser of $\{\infty, 0\}$ consists of matrices of the form

$$\begin{pmatrix} a^2 & 0 \\ 0 & 1 \end{pmatrix}.$$

It is clear that this group has two orbits on the remaining points of X, consisting of quadratic residues and non-residues respectively. □

We observe that the action of $PSL_2(q)$ on the Paley matrix of order $q+1$ induces a labelling of the rows of H with the elements of X. Without loss of generality, we may label the initial row of H with ∞, in which case we see that the core of the matrix is labelled by the elements of $\mathbb{F}_q$, and that the stabiliser of two points has two orbits on the remaining rows.

Finally, we observe that the Paley matrices of orders 4 and 8 are equivalent to the Sylvester matrices at those orders. While they are developed from Paley difference sets, their automorphism groups are of the type specified for the Sylvester matrices. The Paley matrix of order 12 has additional automorphisms besides those given by Kantor. Indeed in [27], Hall observes that all Hadamard matrices of order 12 are equivalent and demonstrates that a Hadamard matrix of order 12 has $\mathcal{A}(H)$ isomorphic to the Mathieu group M_{12}.

4.3.2 Sylvester Hadamard matrices

We have already encountered the Sylvester matrices in the proof of Theorem 4.2. These matrices are named after Sylvester, who constructed them as the Kronecker powers of the matrix

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

He also observed that the rows of such a matrix are orthogonal [73]. Indeed, Sylvester's construction seems to have been one of the motivations for Hadamard's work.

Like the Paley matrices, the Sylvester matrices have a natural construction from difference sets constructed from projective geometries. In this case, however, we fix the field to be $\mathbb{F}_2$, and allow the dimension of the projective space to vary. We begin with a well known theorem of Singer.

Theorem 4.19 (Singer, Theorem III.6.2, [5])**.** *The group $PGL_n(q)$ contains a cyclic subgroup of order $\frac{q^n-1}{q-1}$ acting regularly on the points and hyperplanes of the projective geometry $PG_n(q)$.*

Now, we specialise to the case $q = 2$. Then the groups $GL_n(q)$, $SL_n(q)$, $P\Gamma L_n(q)$ and $PSL_n(q)$ etc. all coincide. The point-hyperplane geometry over $PG_n(2)$ has parameters 2-$(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$. Combining Theorem 4.19 with Theorem 2.47, we see that the cyclic group of order $2^n - 1$ contains a $(4t - 1, 2t - 1, t - 1)$-difference set. In fact we can describe this difference set explicitly.

Definition 4.20. Let $\mathbb{F}_q$ be a finite field, $q = 2^n$. We define the *trace function* on $\mathbb{F}_q$ to be the map $x \mapsto \sum_{i=0}^{n-1} x^{2^i}$. The elements of $\mathbb{F}_q^*$ of trace zero form a difference set in $\mathbb{F}_q^*$. (See Theorem 2.1.1 of [64] for a proof.) Such a difference set is known as a *Singer difference set*. A *Singer design* is the underlying symmetric 2-design of a Singer difference set, and a *Sylvester Hadamard matrix* is a Hadamard matrix developed from a Singer difference set.

We recall the following result.

Theorem 4.21 (Fundamental Theorem of Projective Geometry, Theorem 2.26 [2])**.** *Let $\mathbb{F}$ be any field, and $n \geq 3$ a natural number. Then $P\Gamma L_n(q)$ is the full automorphism group of the projective geometry $PG_n(q)$.*

Now, from the description of a Singer design $\mathcal{S}$ on $2^n - 1$ points as a point-hyperplane design, it is clear from Theorem 4.21 that $\mathrm{Aut}(\mathcal{S}) = PSL_n(2)$.

Observe that a line over $\mathbb{F}_2$ consists of 2 points. Hence in this special case, it is possible to construct the affine geometry $AG_n(2)$ directly from $PG_n(2)$. To do this, we add a new point, 0, which is incident with all (projective) hyperplanes, and adjoin the translates of all of these hyperplanes. Notice that the hyperplanes occur in complementary pairs H_i and H_i^*, where every point of $AG_n(2)$ is incident to exactly one of H_i and H_i^*. Now, the i^{th} column of the Sylvester matrix of order 2^n has j^{th} entry $+1$ if point j is incident with H_i, and -1 otherwise. Thus we see that $AGL_n(2)$ has an induced action on the set of rows of H. In fact, this action is faithful, and since $AGL_n(2)$ is maximal in S_{2^n} (see [54]), it follows that

$\mathcal{A}(H) \cong AGL_n(2)$. By the proof of Theorem 4.2, the kernel of ν is a group acting regularly on the hyperplanes of $AG_n(2)$, of order 2^{n+1}. Thus we have the following theorem.

Theorem 4.22 (p.258, [16]). *Let H be a Sylvester Hadamard matrix of order 2^n. Then the full automorphism group of H is $Z(\mathrm{Aut}(H)) \times C_2^n \rtimes A\Gamma L_n(2)$.*

In fact, it can be shown that a Hadamard matrix with 3-transitive automorphism group is either a Sylvester matrix, or is of order 12. The proof is achieved by constructing a rudimentary geometry from the blocks of a nontrivial 2-(v, k, λ) design Δ.

Definition 4.23. Let u and v be two points of Δ. Then the *line* through u and v is the intersection of all blocks containing both u and v.

Trivially the cardinality of a line is bounded below by 2. An easy counting argument gives an upper bound on the cardinality of a line.

Lemma 4.24 (Lemma 2.23, [35]). *The cardinality of a line of Δ is bounded above by $\frac{b-\lambda}{r-\lambda}$ where b is the number of blocks in Δ and r is the number of blocks incident with a single point. This bound is achieved for a line l if and only if l meets every block.*

For a Hadamard 2-design, the upper bound of Lemma 4.24 is 3.

Definition 4.25. Three non-collinear points form a *triangle*. A *plane* is the intersection of all blocks containing a triangle.

The following theorem of Dembowski-Wagner characterises the designs that come from projective planes.

Theorem 4.26 (Dembowski-Wagner, Theorem 2.24, [35]). *Suppose that Δ is symmetric. Then the following are equivalent:*

- *$\Delta \cong P_n(q)$ for some $n \geq 2$ and prime power q, or Δ is a projective plane.*
- *every line meets every block.*
- *every line contains $\frac{v-\lambda}{k-\lambda}$ points.*
- *every plane is contained in the same number of blocks.*

We can now classify the Hadamard matrices with $\mathcal{A}(H)$ triply transitive. This proof may be compared to Proposition 2 of [39], which arrives at the same conclusion via arguments about primitive prime divisors of $|\mathcal{A}(H)|$.

Theorem 4.27. *Suppose that H is a Hadamard matrix such that $\mathcal{A}(H)$ is triply transitive. Then either H is a Sylvester matrix or H is of order* 12.

Proof. Let H be a Hadamard matrix with $\mathcal{A}(H)$ non-affine. Then by Theorem 4.7, H is of order 12. (Neither $PSL_2(q)$, $q > 11$, or $Sp_6(2)$ on 36 points are triply transitive.)

Suppose now that $\mathcal{A}(H)$ is affine. Thus H has order 2^n for some n. Then the underlying symmetric design $\mathcal{S}$ has the parameters of a projective space. Now if $\nu : \mathrm{Aut}(H) \to \mathcal{A}(H)$ is not faithful, H is already a Sylvester matrix by Theorem 4.2. So we assume that ν is faithful. In this case, $\mathrm{Aut}(\mathcal{S})$ is 2-transitive on the points of $\mathcal{S}$.

A line in $\mathcal{S}$ is uniquely determined by a pair of points: so $\mathrm{Aut}(\mathcal{S})$ has a single orbit on lines. By Lemma 4.24 and Theorem 4.26, it suffices to show that some line in $\mathcal{S}$ has length 3. This can be shown by elementary, but involved, counting arguments on the number of blocks meeting a distinguished line in a single point. We refer to the Theorem 12.2 of [45] for the full argument. Hence $\mathcal{S}$ is a projective space. By Remark 2.58, the Hadamard matrix constructed from a symmetric design is unique up to equivalence. So a Hadamard matrix with 3-transitive automorphism group is either of order 12 or arises from a projective space. The latter case is a Sylvester matrix by definition. □

4.3.3 A classification of Hadamard matrices with $\mathcal{A}(H)$ doubly transitive

We give a detailed classification of the Hadamard matrices with $\mathcal{A}(H)$ non-affine doubly transitive. Our main tool is Theorem 4.7, due to Ito.

We recall Burnside's Theorem on the socle of a doubly transitive group (Theorem 2.11): a doubly transitive group is either of affine type and contains an elementary abelian normal subgroup acting regularly, or it is almost simple. We consider only the non-affine case. The affine case requires methods different to those developed here and falls outside of the scope of this thesis. In light of Theorem 4.7, it is not difficult to list all Hadamard matrices H with $\mathcal{A}(H)$ non-affine doubly transitive. We consider each of the cases listed by Ito in turn: M_{12}, $Sp_6(2)$ and $PSL_2(q)$. The first case was considered by Marshall Hall.

Lemma 4.28 (M. Hall, [27])**.** *All Hadamard matrices of order* 12 *are (Hadamard) equivalent, and for any such matrix* H*,* $\mathcal{A}(H) \cong M_{12}$ *acting sharply* 5*-transitively.*

The action of $Sp_6(2)$ in Theorem 4.7 is not its natural action on a 6 dimensional $\mathbb{F}_2$-vector space; rather the stabiliser of a point is a maximal subgroup of index 36 isomorphic to S_8. This is the only action of $Sp_6(2)$ that we will consider. In this action, S_8 acts primitively on the 35 remaining points. In [28], Marshall Hall discusses (among other topics) the construction of Menon-Hadamard designs from strongly regular graphs. One example given is the construction of a $(36, 15, 6)$ design having $U_4(2)$ as its automorphism group. Hall observes that the corresponding Hadamard matrix has full automorphism group isomorphic to $Sp_6(2)$ in the action described above. Then in [40], Ito and Leon construct a Hadamard matrix H of order 36 with $\mathcal{A}(H) \cong Sp_6(2)$ as follows. Let ψ be a symplectic form on $\mathbb{F}_2^6$. Then the set of vectors satisfying $\psi(v, v) = 1$ has cardinality 35 (see pp. 245-247 of [21]). The stabiliser of a point in the action of $O_6^+(2)$ on these vectors has three orbits. Translates of the union of two of these orbits provide the blocks of a 2-$(35, 17, 8)$ design, from which a Hadamard matrix H with $\mathcal{A}(H) \cong Sp_6(2)$ is constructed. Ito and Leon (wrongly) state that this matrix has not previously been considered in the literature. They conjecture that up to equivalence, H is the unique Hadamard matrix of order 36 with $\mathcal{A}(H)$ doubly transitive. We now observe that this is the case.

Theorem 4.29. *Suppose that* H *is a Hadamard matrix with* $\mathcal{A}(H) \cong Sp_6(2)$ *in its doubly transitive action on* 36 *points. Then* H *is unique (up to Hadamard equivalence).*

Proof. By Theorem 4.2, $\mathrm{Ker}(\nu)$ has order 2. Thus $|\mathrm{Aut}(H)| = 2 \cdot |Sp_6(2)| = 2,903,040$. Now see Tables 8 and 9 of [8], where an exhaustive computer search shows that there is a unique Hadamard matrix of order 36 with automorphism group of order $2,903,040$. □

Remark 4.30. One may also prove uniqueness of the Hadamard matrix upon which $Sp_6(2)$ acts as follows. By Theorem 4.8, $|\mathcal{A}(H) : \mathcal{A}(\mathcal{S})| = 36$. But $Sp_6(2)$ has a unique conjugacy class of subgroups of index 36. So $\mathrm{Aut}(\mathcal{S}) \cong \mathrm{Sym}(8)$.

Theorem 2 of [13] states that there are four symmetric 2-$(35, 17, 8)$ designs with automorphisms of order 7. One of these has S_8 as its automorphism group; the others have automorphism groups of order at most 420. By Remark 2.58, this gives another proof of the uniqueness of H.

This resolves the two sporadic cases of Ito. We consider now the case that $PSL_2(p^k)$ acts on the rows of H. (We refer the reader to Section 4.3.1 for a discussion of this action. Also note that the proof below contains some forward references to Chapter 5.)

Theorem 4.31. *Let H be a normalised Hadamard matrix of order $q+1$, for a prime power $q \equiv 3 \mod 4$, $q > 11$. Then $PSL_2(q)$ in its natural doubly transitive action is a normal subgroup of $\mathcal{A}(H)$ if and only if H is equivalent to a Paley matrix.*

Proof. Suppose that $PSL_2(q)$ is a normal subgroup of $\mathcal{A}(H)$. Then the stabiliser of a point in $\mathcal{A}(H)$ contains a subgroup of index 2 in $AGL_1(q)$. This contains a normal elementary abelian subgroup R of order q acting regularly on the remaining points. It is clear that R fixes a point in its action on columns. Hence, R is a regular subgroup of $\mathrm{Aut}(\mathcal{S})$, where $\mathcal{S}$ is a symmetric design corresponding to H. Thus by Theorem 2.47, H is developed from a difference set $\mathcal{D}$ in R. We show that $\mathcal{D}$ is necessarily of Paley type: this guarantees that H is equivalent to a Paley matrix by Remarks 2.58 and 2.48.

Consider $\mathcal{A}(H)_{1,2}$, the stabiliser of a point in $\mathcal{A}(H)_1$. This has two orbits on the remaining rows, one labeled by quadratic residues and one by non-residues. By Bruck's characterisation of the multipliers of a difference set (Theorem 5.8), we have that the quadratic residues are multipliers of $\mathcal{D}$. Now, by Theorem 5.10, there exists a translate of $\mathcal{D}$ fixed by every multiplier. This translate either consists entirely of quadratic residues or of quadratic non-residues. In either case $\mathcal{D}$ is equivalent to a Paley difference set.

Conversely, if H is of order $q + 1 > 12$ and H is equivalent to a Paley matrix, it is clear by Theorem 4.15 that $PSL_2(q) \trianglelefteq \mathcal{A}(H)$. □

The previous results yield the following classification.

Corollary 4.32. *H is a Hadamard matrix such that $\mathcal{A}(H)$ is non-affine doubly transitive if and only if one of the following holds.*

- *H is of order 12.*
- *H is in the unique equivalence class of Hadamard matrices of order 36 on which $Sp_6(2)$ acts.*
- *H has order greater than 12 and is equivalent to a Paley matrix.*

Remark 4.33. The Hadamard matrices of order less than 12 are excluded from the list of Corollary 4.32 because their automorphism groups are affine doubly transitive rather than non-affine. Indeed, the Hadamard matrices of orders 4 and 8 are the only Hadamard matrices which are simultaneously of Paley and Sylvester type.

We note that an unpublished paper [55] of Moorhouse classifies all of the complex Hadamard matrices with doubly transitive automorphism groups. Our classification agrees with his in the special case considered here.

4.4 Cocyclic development

We know from Theorem 4.12 that a cocyclic Hadamard matrix H developed from a Paley-Hadamard difference set has $\mathcal{A}(H)$ doubly transitive. In this short section, we describe all the groups over which the Hadamard matrices of Corollary 4.32 are cocyclic. Recall that this can be achieved for any Hadamard matrix by using the techniques discussed in Chapter 3. We consider the sporadic cases first. The next two results were obtained using the computational techniques developed in [58] from ideas due to de Launey (as per Chapter 3).

Lemma 4.34 ([58], Section 5.3)**.** *A Hadamard matrix of order* 12 *is cocyclic over the alternating group A_4, the dihedral group of order* 12 *and $C_2 \times C_6$, with extension groups $SL_2(3)$, $C_3 \rtimes Q_8$ and $C_3 \times Q_8$ respectively.*

The cocyclic Hadamard matrices of order 36 are classified in Chapter 3. The Hadamard matrix of Ito and Leon is not contained in the classification. In fact the Paley Type II matrix is the only cocyclic Hadamard matrix at this order with a non-solvable automorphism group.

Lemma 4.35. *Let H be in the unique equivalence class of Hadamard matrices of order* 36 *with $\mathcal{A}(H) \cong Sp_6(2)$. Then H is not cocyclic over any group.*

This leaves only the Paley matrices to consider. The groups over which a Paley matrix is cocyclic have been described by de Launey and Stafford. This result is deep, and relies on detailed knowledge about the finite near-fields, amongst other things.

Theorem 4.36 ([18], Section 5)**.** *Let H be a Paley matrix of order $q+1$. Then H is cocyclic over the dihedral group of order $q+1$, with dicyclic extension group. There are additional extension groups only for $q \in \{3, 7, 11, 23, 59\}$.*

The additional extensions in Theorem 4.36 are described in Section 5 of [18]. The matrices of orders $4, 8, 12$ and 24 are also discussed in Chapter 5 of [58]. There is just one additional extension group for the Paley matrix of order 60, namely $SL_2(5)$.

Corollary 4.37. *Let H be a Hadamard matrix with $\mathcal{A}(H)$ non-affine doubly transitive. Then H is cocyclic if and only if H is of order 12 or H is equivalent to a Paley matrix. In both cases all groups over which H is cocyclic and all extension groups for H are known.*

4.5 A classification of $(4n-1, 2n-1, n-1)$-difference sets with 'transitive extensions'

In this section, we classify up to equivalence (in the sense of Definition 2.44) the $(4n-1, 2n-1, n-1)$-difference sets which correspond to the Hadamard matrices of Corollary 4.32.

Suppose that H is a Hadamard matrix such that $\mathcal{A}(H)$ is non-affine doubly transitive. Let $\mathcal{S}$ be a symmetric 2-$(4n-1, 2n-1, n-1)$ design underlying H. By Corollary 4.9, either H is of order 12 or $\mathrm{Aut}(\mathcal{S}) \cong \mathcal{A}(H)_1$. In particular $\mathrm{Aut}(\mathcal{S})$ is transitive on the points of $\mathcal{S}$. Then by Theorem 2.47, the difference sets corresponding to H are in bijection with the regular subgroups of $\mathcal{A}(H)_1$. Note that we do not describe all difference sets in these groups (a listing of all difference sets in elementary abelian groups is well beyond the bounds of existing techniques!), but only those for which the corresponding Hadamard matrix H has $\mathcal{A}(H)$ non-affine doubly transitive.

To summarise: for each of the doubly transitive groups identified by Ito, we classify the regular subgroups of a point stabiliser on the remaining points. We choose a representative from each conjugacy class of regular subgroups and describe the difference sets in these groups which correspond to the Hadamard matrices of Corollary 4.32.

Lemma 4.38. *Suppose that H is a Hadamard matrix of order 12. Let $\mathcal{S}$ be a symmetric design corresponding to H. Then $\mathrm{Aut}(\mathcal{S})$ has precisely one conjugacy class of regular subgroups, each of which contains the Paley difference set of that order.*

Proof. The stabiliser of a point in M_{12} is the simple group M_{11}, but the automorphism group of $\mathcal{S}$ is $PSL_2(11)$. This group has a unique conjugacy class of regular

subgroups. The First Multiplier Theorem (see Section 5.2, or Theorems VI.2.6 and VI.2.11 of [5]) allows us to settle this case by hand. We are searching for an $(11, 5, 2)$-difference set in $\mathbb{Z}_{11}$, so 3 is a multiplier. That is, any difference set in $\mathbb{Z}_{11}$ has a translate which is fixed by the automorphism $x \mapsto 3x$. The orbits of this automorphism are $\{1, 3, 4, 5, 9\}$, $\{2, 6, 7, 8, 10\}$ and $\{0\}$. But the first orbit consists precisely of the quadratic residues of $\mathbb{F}_{11}$, so is a Paley difference set. The second orbit also forms a difference set, which is equivalent to the first under the inversion automorphism. □

It is easy to show that S_8 does not contain a subgroup of order 35 (no element of order 5 commutes with an element of order 7 in S_8). Hence in its action on 35 points, S_8 does not contain a regular subgroup.

Lemma 4.39. *Suppose that H is a Hadamard matrix of order 36, and $\mathcal{A}(H) \cong Sp_6(2)$ acting doubly transitively. Then H is not developed from any difference set.*

Remark 4.40. Lemmas 4.35 and 4.39 may be compared to [60, Theorem 10].

By Corollary 4.32, all that remains to be considered are the Paley matrices. Let H be the Paley matrix of order $q + 1$. Then $\mathcal{A}(H) \cong P\Sigma L_2(q)$, by Theorem 4.15. Then by Corollary 4.9, we see that a symmetric 2-design corresponding to the Paley matrix of order $q + 1$ has a subgroup of index 2 in $A\Gamma L_1(q)$ as its automorphism group. Thus, our first task is to classify the regular subgroups of this automorphism group. For convenience, we now state the main results of our investigations.

Theorem 4.41. *Let H be the Paley matrix of order $q + 1$. Express q as p^{np^e} for a prime p, and n coprime to p. Then $\mathcal{A}(H)_1$ has $e + 1$ conjugacy classes of regular subgroups. One is normal and elementary abelian, the remainder are non-normal, non-abelian of exponents p^{2p^t} for $0 \leq t \leq e - 1$.*

The difference sets in the abelian regular subgroups are equivalent to the Paley difference sets. A description of the non-abelian difference sets corresponding to the Paley matrices is given in the proof of Theorem 6.6. This will complete the description of all difference sets for which the corresponding Hadamard matrix H has $\mathcal{A}(H)$ non-affine doubly transitive.

Corollary 4.42. *There exists a difference set corresponding to a Hadamard matrix H with $\mathcal{A}(H)$ non-affine doubly transitive if and only if H is a Paley matrix. All such difference sets are known.*

The rest of this section is devoted to a proof of Theorem 4.41.

4.5.1 The regular subgroups of $A\Gamma L_1(q)$

Let K/L be a Galois field extension of degree n, with Galois group G. Then the Normal Basis Theorem states that there exists an element of ω of K such that ω^G is a basis for K as an L-vector space. Recall that extensions of finite fields are always Galois, with cyclic Galois group.

We will consider $\mathbb{F}_q$ as a field extension of $\mathbb{F}_p$ for the moment. Extensions of intermediate fields are obtained by replacing the Frobenius automorphism σ by a suitable power, and will be considered later. We now determine the regular subgroups of $A\Gamma L_1(q)$ in its natural action.

Lemma 4.43. *Suppose that $q = p^n$ and p does not divide n. Then the only regular subgroup of $A\Gamma L_1(q)$ is elementary abelian and normal.*

Proof. The subgroup T consisting of the maps $x \mapsto x + a$ for $a \in \mathbb{F}_q$ is a regular normal subgroup of $A\Gamma L_1(q)$ and is easily seen to be elementary abelian. But a Sylow p-subgroup of $A\Gamma L_1(q)$ is of order q; hence T is the unique subgroup of order q in $A\Gamma L_1(q)$. □

We consider now the case that $q = p^p$. (The argument for the general case is almost identical, and is given later.) In this case, a Sylow p-subgroup of $A\Gamma L_1(q)$ has order p^{p+1}, and a regular subgroup has order p^p. By the Normal Basis Theorem, we may consider $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space V of dimension p, on which the Frobenius automorphism σ acts by cyclic permutation of co-ordinates. We fix some notation: $\{v_1, v_2, \ldots, v_p\}$ is a basis for V, $A\Gamma L_1(q) = \langle a_1, a_2, \ldots, a_p, \beta, \sigma\rangle$ where the action of each of the generators is given by

$$v^{a_i} = v + v_i, \qquad v^{\beta} = bv, \qquad v_i^{\sigma} = v_{i+1},$$

with subscripts interpreted modulo p, b is a primitive element of $\mathbb{F}_q^*$ and the action of σ is extended linearly to all of $V = \mathbb{F}_q$. The subgroup $G = \langle a_1, \ldots, a_p, \sigma\rangle$ is a Sylow p-subgroup of $A\Gamma L_1(q)$. We can determine a presentation of G with relative ease:

$$G = \langle a_1, \ldots, a_p, \sigma \mid a_i^p = \sigma^p = 1, [a_i, a_j] = 1, a_i^{\sigma} = a_{i+1}, 1 \le i, j \le p\rangle\,.$$

Remark 4.44. We observe that the prime subfield of $\mathbb{F}_q$ is fixed by σ; it is the subspace spanned by $v_1 + v_2 + \cdots + v_p$.

Lemma 4.45. *A non-trivial element of G is either fixed-point-free, or is conjugate to an element of $\langle\sigma\rangle$ and fixes p points.*

Proof. The element σ centralises p^2 elements of G (those of the form $a_1^x \cdots a_p^x \sigma^t$), so $|N_G(\langle\sigma\rangle)| = p^2$ and the number of distinct conjugates of $\langle\sigma\rangle$ in G is $p^{p+1}/p^2 = p^{p-1}$. Now σ fixes the prime subfield, so a non-trivial element in the union U of these conjugates fixes at least p points in V. Note that $|U| = p^{p-1}(p-1)+1$. Since G is transitive on V, it then follows from the Cauchy-Frobenius formula that each non-trivial element of U fixes precisely p points, and that $G \setminus U$ is the set of fixed-point-free elements of G. □

Definition 4.46. Let E be a multiplicatively written elementary abelian group of order p^k, with fixed minimal generating set $\{e_1, \ldots, e_k\}$. Then the *weight* of an element of E is given by

$$w(e_1^{x_1} \cdots e_k^{x_k}) = \sum_{i=1}^{k} x_i \mod p \quad (0 \le x_i \le p-1).$$

Definition 4.47. Each element g of G may be expressed uniquely in the form $a\sigma^t$ for some $a \in \langle a_1, \ldots, a_p\rangle$ and $0 \le t \le p-1$. Define the weight $w(g)$ of g to be $w(a)$. Also define the *class* of g to be t.

Lemma 4.48. *The weight and class of an element of G are invariant under conjugation by G.*

Proof. Each quantity is preserved under conjugation by the generators of G. □

Lemma 4.49. *All conjugates of σ have weight 0. Furthermore, an element of G of weight zero is conjugate to σ^t if and only if it has class t.*

Proof. The first part is immediate from Lemma 4.48. For the second, it suffices to show that an element of weight zero and class t is conjugate to σ^t.

By Lemma 4.45, σ^t has p^{p-1} conjugates. Each of these is an element of weight zero and class t. But there are precisely p^{p-1} elements in G with this property. The result follows. □

By definition $\langle a_1, \ldots, a_p\rangle$ acts transitively on V; hence it is a regular subgroup of G. As the next theorem shows, this is the only abelian regular subgroup.

Theorem 4.50. *Let $q = p^p$. Then $A\Gamma L_1(q)$ has two conjugacy classes of regular subgroups. In particular, all non-abelian regular subgroups are $A\Gamma L_1(q)$-conjugate.*

Proof. Consider the subgroup

$$T_k = \langle a_i \sigma^k,\ 1 \leq i \leq p \rangle$$

of G. Note that T_k is abelian if and only if $k = 0$. We claim that $T_k = \{a\sigma^{k \cdot w(a)} \mid a \in T_0\}$. To see this, let $g = a\sigma^{kt}$ and $h = b\sigma^{ks}$ for $a, b \in T_0$ have weights t, s respectively; then

$$gh = a\sigma^{kt} b\sigma^{ks} = ab^{\sigma^{-kt}} \sigma^{k(t+s)}$$

has weight $w(a) + w(b^{\sigma^{-kt}}) = t + s$ and class $k(t + s)$. Since T_k is generated by elements of weight 1 and class k, this implies by induction that the class of $g \in T_k$ is $k \cdot w(g)$, as required.

We show that each T_k is a regular subgroup of G. Let $g \in T_k$, $g \neq 1$. If $w(g) \neq 0$ then g is fixed-point-free by Lemmas 31 and 34. Suppose that $w(g) = 0$. Then the class of g is zero by the previous paragraph. By Lemmas 31 and 35, we see once again that g is fixed-point-free. But T_k has order p^p and acts on a set of this size: it is regular.

In the next part of the proof we establish that the T_k are the only regular subgroups of G. Since a regular subgroup R has index p in G, R must contain the normal subgroup

$$K = \langle a_1 a_2^{-1}, a_2 a_3^{-1}, \ldots, a_{p-1} a_p^{-1} \rangle$$

of G that lies in every T_k. Note that $|K| = p^{p-1}$, K consists of all elements of weight 0 in T_0, and $T_0 = \cup_{i=0}^{p-1} a_1^i K$. If $R \neq T_0$ then $R = \langle a_1^s \sigma^t, K \rangle$ for some $1 \leq s, t \leq p-1$. But $a_1^s \sigma^t = a_1^s \sigma^{rs}$ where $r \equiv ts^{-1} \mod p$, so that $R = T_r$.

Now choose any r, $1 < r \leq p-1$. Let $c \equiv r^{-1} \mod p$. Then there exists $\gamma \in \langle \beta \rangle$ such that $v^\gamma = cv$ for all $v \in V$. The equalities

$$v_i^{\gamma\sigma} = (cv_i)^\sigma = cv_i^\sigma = c(v_i^\sigma) = v_i^{\sigma\gamma}$$

and

$$v^{\gamma^{-1} a_i \gamma} = (c^{-1} v + v_i)^\gamma = v + cv_i = v^{a_i^c}$$

imply that $\sigma^\gamma = \sigma$ and $a_i^\gamma = a_i^c$. Therefore $T_1^\gamma = \langle a_i^c \sigma,\ 1 \leq i \leq p \rangle = T_r$.

Finally, since a regular subgroup of $A\Gamma L_1(q)$ is contained in some Sylow p-subgroup, and (as we just showed) all non-abelian regular subgroups of the Sylow p-subgroup G are conjugate, all non-abelian regular subgroups of $A\Gamma L_1(q)$ are conjugate. □

Corollary 4.51. *Suppose that F is a finite field of characteristic p and that K is*

an extension of F of finite index. Then $A\Gamma L_F(K)$, the group of semilinear transformations of K fixing F, contains one conjugacy class of regular subgroups for each power of p dividing the degree of the extension (including p^0).

Proof. In the case that K is an extension of degree mp where $p \nmid m$, it suffices to consider K as an extension of degree p over a suitable intermediate field. The argument in the proof of the previous theorem holds with minor modifications.

Now we consider field extensions of degree p^a. Here we construct a tower of extensions, each of degree p. It is then seen that one additional conjugacy class of regular subgroups is obtained at each level of the tower. □

We recall that the automorphism group of a symmetric Paley 2-design $\mathcal{S}$ is of index 2 in $A\Gamma L(1,q)$. So its Sylow p-subgroups are the same as those of $A\Gamma L(1,q)$. Thus the conjugacy classes of regular subgroups of $\mathrm{Aut}(\mathcal{S})$ are in bijection with those of $A\Gamma L(1,q)$. This completes the proof of Theorem 4.41.

5 Non-cocyclic Hadamard matrices from difference sets

In this chapter we apply the classification result Corollary 4.32. We decide when the Hadamard matrices developed from twin prime power and sextic residue difference sets are cocyclic. This occurs in precisely one case in each family. These results are original; the result on twin prime power Hadamard matrices was obtained in collaboration with Richard Stafford, and has appeared in print in [60]. Thus we provide two presumably infinite families of non-cocyclic Hadamard matrices in this chapter. (These constructions rely on the existence of infinitely many twin prime powers and the existence of infinitely many prime solutions to the polynomial $x^2 + 27$ over the integers respectively. Both of these are well known open problems in number theory.) We begin with a brief review and further discussion of the theory of $(4t-1, 2t-1, t-1)$-difference sets.

5.1 Paley-Hadamard difference sets

In Lemma 2.57 and Remark 2.58 we described the relation between a symmetric 2-$(4t-1, 2t-1, t-1)$ design $\mathcal{S}$ and the corresponding Hadamard matrix. Since a difference set corresponds to a regular subgroup of $\mathrm{Aut}(\mathcal{S})$, we have a relationship between Paley-Hadamard difference sets (i.e. $(4t-1, 2t-1, t-1)$ difference sets) and Hadamard matrices.

There are four classical families of Paley-Hadamard difference sets[1]; we describe each family in turn.

Definition 5.1. We recall from Definition 4.20 that the elements of trace zero in $\mathbb{F}_{2^n}^*$ form a *Singer difference set.*

The Singer difference sets correspond to Sylvester Hadamard matrices. We refer the reader to Section 4.3.2 for a discussion of the full automorphism group of a

[1] By 'classical' we mean the families of difference sets known in the 1960s as discussed in [4] and [29]. See also Remark VI.8.4 of [5].

Sylvester matrix, and for the full automorphism group of its underlying 2-design. We confine ourselves to observing that the cyclic regular subgroups of $\mathrm{Aut}(\mathcal{S}) \cong PSL_n(2)$ are called *Singer cycles*, and that they are all conjugate. Difference sets in Singer cycles of arbitrary projective geometries are said to have *classical parameters* (see Chapter 3 of [64] for example), and are among the best understood families of difference sets.

The Paley difference sets (see Definition 4.13) correspond to the (Type I) Paley matrices as defined in Section 4.3.1. The automorphism groups of the Paley matrices and their underlying 2-designs are well known, and are given in Section 4.3.1. In contrast, the following difference sets have received rather less attention in the literature.

By *twin prime powers*, we mean a pair of odd positive integers, q and $q+2$, each of which is a prime power. We note that twin prime power difference sets are a generalisation of twin prime difference sets, which were seemingly first discovered by Gruner in 1939. As Baumert observes, these difference sets 'seem to belong to that special class of mathematical objects which are prone to independent rediscovery'. They seem to be well understood, with Baumert giving a detailed description of their properties and generalisations in [4, pp. 131-142].

Definition 5.2. Let q and $q+2$ be twin prime powers, and let $4n-1 = q(q+2)$. Denote by χ the standard quadratic residue function. Then

$$\{(g,0) \mid g \in \mathbb{F}_q\} \bigcup \{(g,h) \mid g \in \mathbb{F}_q, h \in \mathbb{F}_{q+2}, \chi(g)\chi(h) = 1\}$$

is a $(4n-1, 2n-1, n-1)$-difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$. We refer to such a difference set as a *TPP difference set*. (Theorem VI.8.2 of [5] proves that this construction yields a difference set.)

We now come to the last of our classical families of difference sets.

Definition 5.3. Let p be a prime of the form $x^2 + 27$ for some integer x (there are no non-trivial prime powers of this form for $x \neq 0$). Denote by C the multiplicative group of $\mathbb{F}_p$. Let U be the unique subgroup of index 6 in C and denote by μ a preimage in $\mathbb{F}_p$ of a generator of C/U. Then $U \cup \mu U \cup \mu^3 U$ forms a difference set in $(\mathbb{F}_p, +)$, generally known as a *Hall sextic residue difference set* or HSR difference set for short. (Theorem 11.6.7 of [29] proves the existence of these difference sets, and characterises them, together with the Paley difference sets, as the only ones having the sextic residues as multipliers.)

To our knowledge, the automorphism groups of the underlying symmetric 2-designs have not been described for either the TPP difference sets or the HSR difference sets. Nor was it known if either family corresponded to cocyclic Hadamard matrices. In fact, we quote a research problem of Horadam.

Problem 5.4 (Research Problem 39, [33])**.** *Are the Hadamard matrices of order* ≥ 36*, constructed from twin prime power difference sets, cocyclic?*

We resolve this problem in the remainder of this chapter. We also answer the same question for the HSR difference sets, completing the analysis of the classical families of Paley-Hadamard difference sets.

Remark 5.5. We note that all of these families give rise to Hadamard matrices of order $4t$ where one of the following hold:

- $t = 2^n$ for some n. A difference set of this type has *classical parameters*.
- $4t - 1$ is a prime power. A difference set of this type has *prime power parameters*.
- $4t - 1 = (k + 1)(k - 1)$ where $k + 1$ and $k - 1$ are prime powers. A difference set of this type has *TPP parameters*.

Note that a HSR difference set has prime power parameters, and that prime power and classical parameters coincide precisely at Mersenne primes. It is conjectured that every Paley-Hadamard difference set has parameters of one of the listed types. (See [24] for an overview of the cyclic case.) In each case, there can exist multiple inequivalent difference sets of the same type. In some cases, infinite families of inequivalent difference sets are known with the same parameters.

5.2 Multipliers and cyclotomy

We introduce some tools from the theory of difference sets which will be needed later in this chapter. The material in this section is not new, but its presentation is somewhat non-standard. The standard exposition of the theory of multipliers is normally given in terms of abelian groups. Indeed many important results on multipliers rely on the isomorphism between an abelian group and its character group, and then use algebraic number theory to derive their conclusions. Such an approach is not valid with non-abelian groups. We give our exposition in terms of

certain automorphisms of the underlying symmetric design of a difference set. First we fix some notation.

Let $\mathcal{D}$ be a difference set in a finite group G, and let $\mathcal{S}$ be its underlying symmetric design, as in Theorem 2.47 and its proof. Then the rows of $\mathcal{S}$ are labelled by the elements of G, and G acts regularly via $x \mapsto xg$, and G acts regularly on the blocks of $\mathcal{S}$, which are of the form $\mathcal{D}g$ for $g \in G$.

Definition 5.6. The *(right) multiplier group* of $\mathcal{D}$, $M(\mathcal{D})$, is the subgroup of $\mathrm{Aut}(G)$ consisting of automorphisms ϕ such that $\mathcal{D}^\phi = \mathcal{D}g$ for some $g \in G$. The elements of $M(\mathcal{D})$ are called *multipliers* of $\mathcal{D}$.

Remark 5.7. We warn the reader that our definition of a multiplier is nonstandard! In particular, it falls halfway between the standard definitions. Let G be a group containing a difference set $\mathcal{D}$, and let $\phi \in \mathrm{Aut}(G)$. Hall ([29, Section 11.4]) defines a multiplier for an abelian group as in Definition 5.6: an automorphism of the group which induces an automorphism of the underlying symmetric design. By Hall's definition in the nonabelian case, ϕ is a multiplier of $\mathcal{D}$ if $\mathcal{D}^\phi = g\mathcal{D}h$ for some $g, h \in G$. Our definition then coincides with his definition of a *right multiplier*. Hall's multipliers need not, in general, be automorphisms of the underlying symmetric design. Since this is the primary case in which we are interested, we define our multipliers in those terms.

Theorem 5.8 (Theorem VI.2.18, [5])**.** *Let $\mathcal{S}$ be the underlying symmetric design of a difference set $\mathcal{D}$. Then, identifying G with its right regular representation in $\mathrm{Aut}(\mathcal{S})$, we have that $M(\mathcal{D}) \cong N_{\mathrm{Aut}(\mathcal{S})}(G)/G$.*

The multiplier groups of certain well known families of difference sets have been determined. We will need the following result in later sections.

Theorem 5.9 (Proposition 3.1.1, [64])**.** *Let $\mathcal{D}$ be a Singer difference set. Then the only multipliers of $\mathcal{D}$ are the powers of* 2.

The following result is of fundamental importance in the theory of difference sets. Note that we do *not* require that the group G is abelian.

Theorem 5.10 (Theorem VI.2.19, [5])**.** *Let $\mathcal{D}$ be a difference set in G and let $H \leq M(\mathcal{D})$. Suppose that $|H|$ is coprime to $|G|$. Then there exists a translate of $\mathcal{D}$ which is fixed by every multiplier in H.*

Theorem 5.10 states that, up to equivalence, $\mathcal{D}$ is the union of H-orbits of G. This result often allows us to construct difference sets with relative ease, given some suitable subgroup of H of $M(\mathcal{D})$.

Example 5.11. As a trivial example, we observe that the Paley difference sets have the quadratic residues as multipliers. It is easily seen that they are the only non-trivial difference sets in $(\mathbb{F}_q, +)$, $q \equiv 3 \mod 4$, with this property. Suppose that $\mathcal{D}$ is a non-trivial difference set in $(\mathbb{F}_q, +)$ (so $1 \leq |\mathcal{D}| \leq \frac{q-1}{2}$) for which $H = \langle x^2 \mid x \in \mathbb{F}_q^* \rangle \leq M(\mathcal{D})$. Observe that Theorem 5.10 applies, since $|H| = 2t - 1$ and $|G| = 4t - 1$ are coprime. Thus there exists a translate of $\mathcal{D}$, $\mathcal{D} + k$ say, which is fixed by H. Now, if $\mathcal{D} + k$ contains a quadratic residue, it contains all quadratic residues, and if it contains a quadratic non-residue, then it contains all the quadratic non-residues. Thus $\mathcal{D} + k$ either consists entirely of quadratic residues, or of quadratic non-residues. In either case $\mathcal{D}$ is equivalent to a Paley difference set.

The theory of *cyclotomy* is essentially a study of generalisations of the Paley difference sets. The main question of the theory is the determination of necessary and sufficient conditions on a prime power q for the e^{th} powers in $\mathbb{F}_q$ to form a difference set in $(\mathbb{F}_q, +)$. One may modify this problem to consider unions of cosets of e^{th} powers, or the e^{th} powers with 0, etc. There is also a theory of generalised cyclotomy, which considers more generally difference sets in direct sums of additive groups of fields. The general reference for this material is the monograph of Storer [72].

Definition 5.12. Let $\mathbb{F}_q$ be a finite field, $q = ef + 1$, and let α be a primitive element of $\mathbb{F}_q$. Then the (non-trivial) e^{th} powers of $\mathbb{F}_q$ are precisely those elements of $\mathbb{F}_q$ which lie in the unique subgroup U_0 of index e and order f in $\mathbb{F}_q^*$.

We denote by $(i, j)_e$ the number of solutions in $\mathbb{F}_q$ to the equation

$$\alpha^s + 1 = \alpha^t$$

where $s \equiv i \mod e$ and $t \equiv j \mod e$. Then $\{(i, j)_e \mid 0 \leq i, j \leq e\}$ is the set of *cyclotomic numbers* of $\mathbb{F}_q$ of order e.

Necessary and sufficient conditions for cosets of the e^{th} powers of $\mathbb{F}_q$ to form a difference set can be described entirely in terms of the cyclotomic numbers of order e. We restrict ourselves to listing some basic identities obeyed by cyclotomic numbers. Proofs of these claims may be found on pages $177 - 178$ of [29].

Theorem 5.13. *The e^{th} cyclotomic numbers of $\mathbb{F}_q$ obey the following identities.*

- $(i, j)_e = (i + k, j + k)_e$
- $(i, j)_e = (-i, j - i)_e$

- $\sum_{j=0}^{e-1}(i,j) = f - n_i$ *where* $n_0 = 1$ *if* f *is even,* $n_{\frac{e}{2}} = 1$ *if* f *is odd, and* $n_i = 0$ *otherwise.*

We note in particular that the Paley difference sets and HSR difference sets are most easily constructed via cyclotomy, while the TPP difference sets are a result of generalised cyclotomy.

Since both the Paley difference sets and HSR difference sets are formed from cosets of the sextic residues, it is clear that both families have the sextic residues as multipliers. The following result of Hall is far less trivial.

Theorem 5.14 (Theorem 11.6.7, [29])**.** *Suppose that* $\mathcal{D}$ *is a difference set in an elementary abelian group of order* $q \equiv 7 \mod 12$ *which admits the sextic residues as multipliers. Then either* $\mathcal{D}$ *is equivalent to a Paley difference set, or* $\mathcal{D}$ *is equivalent to a HSR difference set.*

In the following result, note that the assumption that there exists a HSR difference set means that we may assume that both difference sets are contained in a cyclic group of prime order $p \geq 31$.

Lemma 5.15. *Let* $\mathcal{D}_1$ *and* $\mathcal{D}_2$ *be Paley and HSR difference sets in* $(\mathbb{F}_p, +)$ *respectively. Then* $\mathcal{D}_1$ *and* $\mathcal{D}_2$ *are inequivalent.*

Proof. With the notation of Definition 5.3, we have $\mathcal{D}_1 = U \cup \mu^2 U \cup \mu^4 U$ and $\mathcal{D}_2 = U \cup \mu U \cup \mu^3 U$.

We must show that there are no $a, b \in \mathbb{F}_p$ such that $\mathcal{D}_2 = a\mathcal{D}_1 - b$, or equivalently $b^{-1}\mathcal{D}_2 + 1 = ab^{-1}\mathcal{D}_1$. But observe that $ab^{-1}\mathcal{D}_1 = \pm\mathcal{D}_1$ depending on whether or not ab^{-1} is a quadratic residue. Likewise, $b^{-1}\mathcal{D}_2$ remains a union of cosets of U: $b^{-1}\mathcal{D}_2 = \mu^i U \cup \mu^{i+1}U + \mu^{i+3}U$ say.

Suppose that ab^{-1} is a quadratic residue. Then, denoting the cyclotomic number $(i,j)_6$ by (i,j), we need only show that $(i,0)+(i,2)+(i,4)+(i+1,0)+(i+1,2)+(i+1,4)+(i+3,0)+(i+3,2)+(i+3,4) \neq 0, \frac{p-1}{2}$. Now, applying the identities of Theorem 5.13, we see that

$$\frac{(p-1)}{6} \leq (i,1)+(i,3)+(i,5)+\sum_{j=0}^{5}(0,j) \leq \frac{2(p-1)}{6}.$$

If ab^{-1} is a non-residue, it suffices to replace i by $i+1$ throughout. The argument is then identical. Thus $\frac{(p-1)}{6} \leq |\mathcal{D}_2 \cap a\mathcal{D}_1 - b| \leq \frac{2(p-1)}{6}$ for any $a \in \mathbb{F}_p^*$, $b \in \mathbb{F}_p$. The result follows. □

Lemma 5.15 is a special case of Theorem 5.21, which is given as a remark both by Baumert ([4], p. 91), and by Beth, Jungnickel and Lenz ([5], Remark VI.8.4(a)). We are not aware of a proof in the literature, so we conclude this section with our own proof. We will require the following number theoretic results.

Theorem 5.16 (Zsigmondy)**.** *Let a, b and n be positive integers such that $(a, b) = 1$. Then there exists a prime p with the following properties:*

- $p \mid a^n - b^n$,
- $p \nmid a^k - b^k$ *for all* $k < n$,

with the following exceptions: $a = 2, b = 1, n = 6$; and $a + b = 2^k, n = 2$.

Corollary 5.17. *The number $2^{2n} - 1$ is not a product of twin prime powers, unless $n = 2$ or $n = 3$.*

Proof. Assume $2^{2n} - 1$ is a product of twin prime powers:

$$2^{2n} - 1 = (2^n + 1)(2^n - 1) = p_1^s p_2^r.$$

Without loss of generality, $p_1^s = 2^n - 1$. There are two cases to consider: either $2^n \equiv 1 \mod 3$, or $2^n \equiv 2 \mod 3$.

In the first case, $p_1 = 3$. Then we apply Zsigmondy's theorem to the equation $2^n - 1 = 3^s$, to obtain $n = 2$ and $s = 1$.

In the second case, $p_2 = 3$, and we have $3^r - 1 = 2^n$. Zsigmondy's theorem gives us that $r = 1$ or $r = 2$. The first of these is a vacuous solution as it gives $p_1 = 1$. The second gives $n = 3$. □

Theorem 5.18 (Mordell, [56])**.** *The only solutions of the Diophantine equation $2^n = x^2 + 7$ are $n = 3, 4, 5, 7, 15$.*

Corollary 5.19. *Suppose that $p = 2^n - 1$ is a Mersenne prime satisfying $p = x^2 + 27$ for some positive integer x. Then $p \in \{31, 127, 131071\}$.*

Proof. By Theorem 5.18, the only solutions to the equation $2^n = 4x^2 + 28$ occur when $n \in \{5, 6, 7, 9, 17\}$. But of these, the only ones such that $p = 2^n - 1$ is prime are $n \in \{5, 7, 17\}$. □

We use these number theoretic results to determine necessary and sufficient conditions for the three parameter types described in Remark 5.5.

Lemma 5.20.
- *The classical and prime power parameters coincide at Mersenne primes.*
- *The classical and TPP parameters coincide only for* $4t - 1 \in \{15, 63\}$.
- *The prime power and TPP parameters do not overlap.*

Proof.
- $2^n - 1$ is a prime power if and only if it is prime. For suppose n is odd: then $3 \mid 2^n - 1$, so $3^\alpha = 2^n - 1$. An application of Theorem 5.16 forces $n = 2$. Otherwise, $n = 2m$ is even, in which case $p^\alpha = (2^m - 1)(2^m + 1)$. Assuming that this factorisation is non-trivial leads to a contradiction. Thus, classical and prime power parameters overlap precisely at Mersenne primes.
- This follows immediately from Corollary 5.17.
- $4t - 1$ cannot be simultaneously a prime power and a product of twin prime powers.

□

We now give the main inequivalence result.

Theorem 5.21. *The four classical families of difference sets are pairwise inequivalent, with the following exceptions:*

- *The TPP and Singer families coincide for* $4t - 1 = 15$.
- *The HSR and Singer families coincide for* $4t - 1 = 31$.
- *The Paley and Singer families coincide for* $4t - 1 \in \{3, 7\}$.

Proof. It is clear that for each family of difference sets and for any choice of t, there exists at most one equivalence class of $(4t - 1, 2t - 1, t - 1)$-difference sets.

We established when the parameters of the difference sets overlap in Lemma 5.20; it is clear that such an overlap is necessary for difference sets from distinct families to be isomorphic. We deal with each case in turn.

- The affine and TPP parameters overlap if and only if $4t-1 = 15$ or $4t-1 = 63$. But the affine and TPP difference sets in groups of order 63 lie in $C_9 \times C_7$ and $C_3^2 \times C_7$ respectively, and as such are non-isomorphic.
- The prime power and TPP parameters never overlap.

- Classical and prime power parameters: these overlap at a Mersenne prime, and there exists a Paley difference set for every such prime. By Corollary 5.19, there exists a HSR difference set with affine parameters if and only if $4t - 1 \in \{31, 127, 131071\}$.

  Observe that if $\mathcal{D}_1$ and $\mathcal{D}_2$ are equivalent difference sets in G then by Theorem 5.8 $M(\mathcal{D}_1)$ and $M(\mathcal{D}_2)$ are conjugate in $\mathrm{Aut}(G)$. We consider the orders of the multiplier groups of the Singer, Paley and HSR difference sets to establish inequivalence results.

  The multiplier group of the Singer difference set in $\mathbb{F}_{2^n}^*$ consists only of the powers of 2 by Theorem 5.9, and so has order n. On the other hand, the multiplier groups of the Paley and HSR difference sets contain the quadratic and sextic residues respectively. Thus if they occur as difference sets in $(\mathbb{F}_p, +)$ with $p = 2^n - 1$, they have orders at least $\frac{2^n-2}{2}$ and $\frac{2^n-2}{6}$ respectively.

  We solve $\frac{2^n-2}{2} \leq n$, to find that the Singer and Paley families can coincide only if $n \leq 3$. So the Singer and Paley families can coincide only for $2^n \leq 8$. Similarly, the Singer and HSR families can coincide only if $2^{n-1} \leq 3n+1$, which implies that $n \leq 5$. But since the smallest non-trivial HSR difference set occurs in the cyclic group of order $2^5 - 1$, this is the only possible equivalence between HSR and Singer difference sets.

It may be verified computationally that the cases listed in the theorem are in fact equivalent. This completes the proof. □

5.3 Two families of non-cocyclic Hadamard matrices

We recall the following consequence of Lemmas 4.11 and 4.10.

Theorem 5.22. *Let H be a cocyclic Hadamard matrix developed from a difference set. Then $\mathcal{A}(H)$ is doubly transitive.*

Remark 5.23. We have shown in Sections 4.3.1 and 4.3.2 that the Paley and Sylvester matrices have 2-transitive automorphism groups. It is well known that both of these families of Hadamard matrices are cocyclic; see Sections 17.3 and 21.1 of [16], for example.

Having prepared the ground in Chapter 4 and Section 5.1, our results here are pleasingly straightforward. Essentially, our proofs proceed as follows: $\mathcal{A}(H)$ is doubly transitive by Theorem 5.22. We use the classification of Corollary 4.32 to show

that $\mathcal{A}(H)$ can only be affine doubly transitive. Then we use number theoretic arguments as in the proof of Theorem 5.21 to reduce the possibilities for the affine case to a finite list, with which we deal by ad hoc methods.

Theorem 5.24. *Let H be a TPP-Hadamard matrix of order $4t$. Then H is cocyclic if and only if $t = 4$.*

Proof. Suppose that H is cocyclic. Then Theorem 5.22 applies.

The Hadamard matrices with $\mathcal{A}(H)$ non-affine are given in Corollary 4.32. But by Lemma 4.39 and the the fact that the Paley and TPP parameters never overlap, no matrix on the list of Corollary 4.32 is developed from a TPP difference set.

So $\mathcal{A}(H)$ is affine. Then by Corollary 5.17, $4t = 16$, or $4t = 64$. If $4t = 16$, then H is equivalent to a Sylvester matrix by Theorem 5.21. We computed the automorphism group of the TPP-Hadamard matrix of order 64 in Magma, and found that it is not cocyclic. □

Theorem 5.24 provides a complete solution to Horadam's Research Problem 39. We now consider the HSR difference sets.

Theorem 5.25. *Suppose that H is a HSR-matrix of order $p+1$. Then H is cocyclic if $p = 31$, and possibly if $p = 131071$, but not otherwise.*

Proof. Suppose that H is cocyclic. Then Theorem 5.22 applies.

In the non-affine case, by Corollary 4.32 and Lemma 4.39 again, and the fact that $12 \neq x^2 + 27$ for any integer x, H must be equivalent to a Paley matrix. By Theorem 4.41, the automorphism group of the underlying symmetric 2-design of the Paley matrix of order $p+1$ has a unique conjugacy class of regular subgroups. Then Lemma 5.15 supplies a contradiction.

In the affine case, by Corollary 5.19, the order of H is 32, 128 or 131072. By Theorem 5.21, the HSR-matrix of order 32 is equivalent to the Sylvester matrix of that order, and so is cocyclic. By direct computation in Magma, the HSR-matrix of order 128 does not have a transitive automorphism group, and so is not cocyclic. □

We conclude with an application of the classification of doubly transitive permutation groups to settle the remaining order 2^{17} in Theorem 5.25.

Lemma 5.26. *The HSR-matrix H of order 131072 is not cocyclic.*

Proof. First, we prove that $\mathcal{A}(H)$ is non-solvable. The sextic residues in $\mathbb{F}_{2^{17}-1}$ are multipliers of the difference set corresponding to H. By Theorem 5.8, and Lemmas 2.59 and 4.3, $\mathcal{A}(H)$ contains a subgroup of order $\frac{2^{17}-2}{6}$.

By Theorem 2.20, a solvable doubly transitive group of degree 2^{17} is a subgroup of $A\Gamma L_1(2^{17})$. But this has order $17(2^{17})(2^{17}-1)$, which is not divisible by $\frac{2^{17}-2}{6}$.

So the automorphism group of H is non-solvable. By Theorem 2.21, there are only three infinite families of doubly transitive affine groups, and two of these are easily dispatched: both $G_2(q)$ and $Sp_{2n}(q)$ act on even dimensional vector spaces. Thus if $\mathcal{A}(H)$ is doubly transitive then $\mathcal{A}(H)_1$ contains $SL_{17}(2)$ as a normal subgroup. Recall that $SL_n(2) \cong PGL_n(2)$ is itself doubly transitive. Hence as a transitive extension of $\mathcal{A}(H)_1$, $\mathcal{A}(H)$ is triply transitive. But by Theorem 4.27, a Hadamard matrix with a triply transitive automorphism group of degree > 12 is equivalent to a Sylvester Hadamard matrix. All Singer subgroups of $PSL_2(17)$ are conjugate; but this yields a contradiction of Theorem 5.21. □

6 Skew Hadamard difference sets

We have described methods by which one may test if a given Hadamard matrix H is cocyclic, and whether H is developed from a difference set. These methods were used in Chapter 4 to derive a complete list of Hadamard matrices with $\mathcal{A}(H)$ non-affine doubly transitive. With one exception these matrices are Paley matrices. The exception is of order 36 and is neither cocyclic nor developed from a difference set. In this chapter we show that a difference set corresponding to a Paley matrix is necessarily equivalent to a skew Hadamard difference set. We then show that a Hadamard matrix developed from a skew Hadamard difference set is cocyclic if and only if it is equivalent to a Paley matrix. This results in a description of a new 3-parameter family of skew Hadamard difference sets. We conclude the thesis with a number of open questions arising from our work.

6.1 Skew Hadamard difference sets

Definition 6.1. Let $\mathcal{D}$ be a (v, k, λ)-difference set in G. Then $\mathcal{D}^{-1} = \{d^{-1} \mid d \in \mathcal{D}\}$ is also a (v, k, λ)-difference set in G. We say that $\mathcal{D}$ is *skew* if $\left|\mathcal{D} \cap \mathcal{D}^{-1}\right| = 0$ and $G = \mathcal{D} \cup \mathcal{D}^{-1} \cup \{1\}$.

The following lemma is a trivial consequence of Definition 6.1.

Lemma 6.2. *Let $\mathcal{D}$ be a skew difference set in G. Then $\mathcal{D}$ is a Paley-Hadamard difference set.*

Proof. Partition G as $\mathcal{D} \cup \mathcal{D}^{-1} \cup \{1\}$, and set $k = |\mathcal{D}|$. It is clear that $|G| = 2k + 1$. Counting in two different ways the number of times each non-identity element of G is represented in the form $d_i d_j^{-1}$, we have

$$\lambda(2k) = k(k-1).$$

So $\lambda = \frac{k-1}{2}$. Observing that λ is a positive integer and making the substitution $t - 1 = \frac{k-1}{2}$, we have that $\mathcal{D}$ is a $(4t-1, 2t-1, t-1)$-difference set, as required. □

In light of Lemma 6.2, the terms 'skew' and 'skew Hadamard' are interchangeable when referring to difference sets. Both are widespread in the literature. Skewness is a strong condition to impose on a difference set and it implies several non-existence results.

Theorem 6.3 ([4], Theorem 4.15)**.** *The only skew difference sets in cyclic groups are the Paley difference sets in groups of prime order.*

For many years the Paley difference sets were the only known examples of skew difference sets, and it was conjectured that they were the only examples. Recently Ding and Yuan [20] used Dickson polynomials to construct new skew difference sets in the additive groups of $\mathbb{F}_{3^5}$ and $\mathbb{F}_{3^7}$. They showed that these difference sets are inequivalent to the Paley ones. They conjectured that their construction produces inequivalent difference sets for all elementary abelian groups of order 3^{2n+1}. This paper revitalised the study of skew Hadamard difference sets: recent results of Feng [22] give a construction for such difference sets in non-abelian groups of order p^3. Muzychuk [57] goes even further: he shows that there are exponentially many equivalence classes of skew Hadamard difference sets in elementary abelian groups of order q^3. In the next section we construct the first triply infinite family of skew difference sets inequivalent to the Paley family. These appear to be the first known skew difference sets in non-abelian p-groups of unbounded exponent.

6.2 A new construction of skew Hadamard difference sets

We recall for the last time that a (v, k, λ)-difference set corresponds to a regular subgroup of the automorphism group of a symmetric 2-(v, k, λ) design. One direction of the following lemma is stated in Remark VI.8.24 of [5].

Lemma 6.4. *Let G be a group containing a difference set $\mathcal{D}$, and let M be an incidence matrix of the underlying 2-design. Set $M^* = 2M - J = \mathrm{Dev}(\mathcal{D})$. That is,*

$$M^* = [\chi(g_i g_j^{-1})]_{g_i, g_j \in G}$$

where the ordering of the elements of G used to index rows and columns is the same, and where $\chi(g) = 1$ if $g \in \mathcal{D}$ and -1 otherwise. Then $M^* + I$ is skew-symmetric if and only if $\mathcal{D}$ is skew Hadamard.

Proof. Suppose that $(M^* + I)^\top = -M^* - I$. The elements of $\mathcal{D}$ are precisely the g_i for which $\chi(g_i) = 1$. But by skew-symmetry of $M^* + I$ we obtain that

$\chi(1g_i^{-1}) = -\chi(g_i 1^{-1})$, so that $g_i \in \mathcal{D}$ if and only if $g_i^{-1} \notin \mathcal{D}$. Hence $\mathcal{D}$ is skew as required.

In the other direction, observe that

$$(M^*)^\top = \left[\chi(g_i g_j^{-1})\right]^\top_{g_i,g_j\in G} = \left[\chi(g_j g_i^{-1})\right]_{g_i,g_j\in G} = \left[\chi((g_i g_j^{-1})^{-1})\right]_{g_i,g_j\in G}.$$

So if $\mathcal{D}$ is skew Hadamard then $(M^* + I)^\top = -M^* - I$. □

Corollary 6.5. *Suppose that $\mathcal{D}$ is a skew difference set with underlying symmetric design $\mathcal{S}$. Then any other difference set arising from a regular subgroup of* $\mathrm{Aut}(\mathcal{S})$ *is equivalent to a skew difference set.*

Proof. Since $\mathcal{D}$ is skew, $M^* + I$ is a skew-symmetric matrix by Lemma 6.4. And again by Lemma 6.4, any other difference set over $\mathcal{S}$ will be equivalent to a skew difference set. □

Now, in light of Corollary 6.5, we revisit the difference sets associated with the Paley matrices which were constructed in Theorem 4.41. Let H be a Paley matrix of order $q + 1 = p^{tp^e} + 1$, and recall that we described a Sylow p-subgroup of $\mathcal{A}(H)$ as a semidirect product $T_0 \rtimes \langle \sigma^t \rangle$, where T_0 is an isomorphic copy of the additive group of $\mathbb{F}_q$, and σ^t is a suitable power of the Frobenius automorphism.

Since the group T_1 (as defined in the proof of Theorem 4.50) acts regularly on the Paley design, Theorem 2.47 guarantees the existence of a Paley-Hadamard difference set in T_1. In fact, we can describe this difference set in terms of the Paley difference set in T_0.

Theorem 6.6. *The group T_1 contains a difference set $\mathcal{D}_1 = \left\{\sigma^{tw(a)}a \mid a \in \mathcal{D}\right\}$. Furthermore $\langle \sigma^t \rangle \leq M(\mathcal{D}_1)$, and $\mathcal{D}_1$ is skew.*

Proof. We describe $\mathcal{D}_1$ explicitly. Recall that $T_1 = \{\sigma^{tw(a)}a \mid a \in T_0\}$. Let $\mathcal{D}_0$ be the quadratic residues in T_0, and define $\mathcal{D}_1 = \{\sigma^{tw(a)}a \mid a \in \mathcal{D}_0\}$.

We show that $\mathcal{D}_1^{\sigma^t} = \mathcal{D}_1$: observe that

$$\left\{(\sigma^{tw(a)}a)^{\sigma^t} \mid a \in \mathcal{D}_0\right\} = \left\{\sigma^{tw(a)}a^{\sigma^t} \mid a \in \mathcal{D}_0\right\}.$$

Thus it suffices to observe that the quadratic residues are preserved by σ (and hence by σ^t). Let β be a primitive element of $\mathbb{F}_q$. Then $x = \beta^k$ is a quadratic residue if and only $k \equiv 0 \mod 2$. Clearly $x^\sigma = x^p = \beta^{kp}$ is a quadratic residue if and only if x is. Hence $\mathcal{D}_1$ is fixed by σ^t.

Define $X_i = \{a \mid a \in \mathcal{D}_0, w(a) = i\}$, and write $\mathcal{D}_t = \cup_{i=0}^{p-1} \sigma^{ti} X_i$. Then since σ is weight preserving, each X_i is a union of orbits of σ^t. This implies that

$$X_i X_j^{-1} = X_i^{\sigma^{tk}} (X_j^{-1})^{\sigma^{tk}} = (X_i X_j^{-1})^{\sigma^{tk}}$$

for any k. Then the multiset of quotients

$$\{\sigma^{t(i-j)}(ab^{-1})^{\sigma^{-tj}} \mid \sigma^{ti}a, \sigma^{tj}b \in \mathcal{D}_1\}$$

represents each element of T_t equally often, because $\mathcal{D}_0$ is a difference set and each of the multisets $X_i X_j^{-1}$ is invariant under σ^t. Thus $\mathcal{D}_t$ is a difference set in T_t. Since the Paley matrices are skew, $\mathcal{D}_t$ is skew by Corollary 6.5. □

Remark 6.7. Any group T_k, as a conjugate of T_1, also contains a Paley-Hadamard difference set.

Note that, for a Paley matrix H, $\mathcal{A}(H)$ has a unique conjugacy class of regular subgroups of each isomorphism type. So Theorem 6.6 gives an explicit description of all difference sets which give rise to a Paley matrix, up to equivalence.

Thus Theorem 6.6 furnishes a family of skew non-abelian difference sets in groups of order p^{np^e} for any prime $p \equiv 3 \mod 4$, n odd and coprime to p, and $e \geq 1$. These difference sets have not previously appeared in the literature.

Note that by Corollary 4.42, there are no other difference sets which give rise to a Hadamard matrix with non-affine doubly transitive automorphism group. Thus we have the following theorem.

Theorem 6.8. *Let $\mathcal{D}$ be a difference set which gives rise to a Hadamard matrix H with $\mathcal{A}(H)$ non-affine doubly transitive. Then $\mathcal{D}$ is equivalent to a skew difference set.*

To conclude this section, we observe that there are no other skew Hadamard difference sets for which the corresponding Hadamard matrix has a doubly transitive automorphism group.

Theorem 6.9. *Let H be a Hadamard matrix of order greater than 8 with affine doubly transitive automorphism group. Then H is not developed from a skew Hadamard difference set.*

Proof. First, suppose that H is developed from a skew Hadamard difference set. Then by Lemma 6.4, the incidence matrix for the underlying 2-design is skew; hence any difference set corresponding to H will be equivalent to a skew difference set.

H has order 2^n for some n, and by a result of Moorhouse [55] is equivalent to the Sylvester matrix of that order. As we know from Subsection 4.3.2, if $\mathcal{S}$ is the underlying design then $\mathrm{Aut}(\mathcal{S})$ contains a cyclic regular subgroup (a Singer cycle). If H is developed from a cyclic skew difference set then H is equivalent to a Paley matrix, by Theorem 6.3. But the Sylvester and Paley matrices coincide only at orders 4 and 8 by Theorem 5.21. □

Corollary 6.10. *Let $\mathcal{D}$ be a skew difference set, and H the Hadamard matrix developed from $\mathcal{D}$. Then $\mathcal{A}(H)$ is doubly transitive if and only if H is equivalent to a Paley matrix.*

6.2.1 Example

We work through an example in the field with 27 elements. The polynomial $x^3 + 2x + 1$ is easily seen to be irreducible over $\mathbb{F}_3$. Hence $\mathbb{F}_3[x]/\left(x^3 + 2x + 1\right)$ is a representation of $\mathbb{F}_{3^3}$. We will need to use both multiplicative and additive forms for the field elements. For the convenience of the reader, we give a conversion table. We also require a normal basis for the field as a vector space over $\mathbb{F}_3$. By inspection, a suitable choice is $a_1 = x^4, a_2 = x^{12}, a_3 = x^{10}$. Finally, we give a representation of each field element in the (multiplicatively written) elementary abelian group $G = \langle a_1, a_2, a_3\rangle$.

Now, we recall that the quadratic residues of $\mathbb{F}_{3^3}$ form the Paley difference set in G. This is the set

$$P = \left\{a_1, a_1a_2^2, a_1a_2^2a_3^2, a_1^2a_2^2, a_1^2a_3, a_1^2a_3^2, a_1^2a_2a_3^2, a_1^2a_2^2a_3, a_1^2a_2^2a_3^2, a_2, a_2a_3^2, a_2^2a_3^2, a_3\right\}.$$

It may be verified by hand that P is indeed a skew difference set.

Denote the Frobenius automorphism by σ, and form the group $\Gamma = \langle a_1, a_2, a_3, \sigma\rangle$, which has order 81, and is a Sylow 3-subgroup of $A\Gamma L_1(3^3)$.

Define $T_1 = \langle a_1\sigma, a_2\sigma, a_3\sigma\rangle$. Then there is a bijection (not a homomorphism) $\phi : G \to T_1$ given by $\phi : a_1^{t_1}a_2^{t_2}a_3^{t_3} \mapsto a_1^{t_1}a_2^{t_2}a_3^{t_3}\sigma^{t_1+t_2+t_3}$.

Multiplicative	Additive	Image in G
1	1	$a_1^2a_2^2a_3^2$
x	x	$a_1a_3^2$
x^2	x^2	$a_1^2a_3^2$
x^3	$x+2$	$a_1^2a_2$
x^4	x^2+2x	a_1
x^5	$2x^2+x+2$	a_2a_3
x^6	x^2+x+1	$a_1^2a_2^2$
x^7	x^2+2x+2	$a_1^2a_2a_3$
x^8	$2x^2+2$	$a_1^2a_2a_3^2$
x^9	$x+1$	$a_2^2a_3$
x^{10}	x^2+x	a_3
x^{11}	x^2+x+2	$a_1a_2a_3^2$
x^{12}	x^2+2	a_2
x^{13}	2	$a_1a_2a_3$
x^{14}	$2x$	$a_1^2a_3$
x^{15}	$2x^2$	a_1a_3
x^{16}	$2x+1$	$a_1a_2^2$
x^{17}	$2x^2+x$	a_1^2
x^{18}	x^2+2x+1	$a_2^2a_3^2$
x^{19}	$2x^2+2x+2$	a_1a_2
x^{20}	$2x^2+x+1$	$a_1a_2^2a_3^2$
x^{21}	x^2+1	$a_1a_2^2a_3$
x^{22}	$2x+2$	$a_2a_3^2$
x^{23}	$2x^2+2x$	a_3^2
x^{24}	$2x^2+2x+1$	$a_1^2a_2^2a_3$
x^{25}	$2x^2+1$	a_2^2
(x^{26})	1	$a_1^2a_2^2a_3^2$

Table 6.1: Multiplicative and additive representations of $\mathbb{F}_{3^3}$

We claim that $\mathcal{D}_1 = \phi(P)$, whose elements are listed below, is a skew difference set.

$$\begin{aligned}\mathcal{D}_1 \;=\; & \{\, a_1a_2^2, a_1^2a_3, a_2a_3^2, a_1^2a_2^2a_3^2, \\ & a_1\sigma, a_2\sigma, a_3\sigma, a_1^2a_2^2\sigma, a_1^2a_3^2\sigma, a_2^2a_3^2\sigma, \\ & a_1a_2^2a_3^2\sigma^2, a_1^2a_2a_3^2\sigma^2, a_1^2a_2^2a_3\sigma^2 \,\}\end{aligned}$$

To verify that $\mathcal{D}_1$ is skew we observe that the inverse of an element of class t has class $3-t$. No pair of elements of weight zero is of the form $\{g, g^{-1}\}$ since P is skew. So it suffices to check that no element of class 2 in $\mathcal{D}_1$ has an inverse in $\mathcal{D}_1$. But observe that every element of class 2 contains each a_i with non-trivial exponent, while there are no elements of class 1 with this property. Skewness follows.

It remains only to check that $\mathcal{D}_1$ is indeed a difference set. We leave this (rather tedious) exercise to the reader. It may be accomplished by consideration of the five orbits of σ on $\mathcal{D}_1$, as in Theorem 6.6.

6.3 Proposals for future work

In this final section, we gather some suggestions for future research.

6.3.1 Cocyclic development

Suppose that M is a cocyclic matrix with cocycle $\psi : G \times G \to U$. All accounts of cocyclic development of which we are aware proceed by the construction of an expanded matrix, on which the central extension of U by G given by ψ acts regularly. An equivalence between such regular actions (in which the action of U is specified) and cocycles of M is then established.

In our proof of Lemma 2.81 we showed that a cocyclic matrix M has a totally regular subgroup $G \leq \mathcal{G}(M)$ without the introduction of the expanded matrix of M. We have not yet managed to obtain a proof of Lemma 2.85 without the introduction of $\mathcal{E}_M$. Such a proof should certainly be possible.

Problem 6.11. *Give an account of cocyclic development entirely in terms of $\mathcal{G}(M)$ for a matrix M with entries in a commutative ring, R. Remove the restrictions that M contain no zero entries, and that M be invertible.*

We note that the general theory of [16] avoids the restrictions on M stated in Problem 6.11. Currently, testing a matrix of order n over an alphabet of size k

for cocyclic development involves computations in a permutation group of degree nk. A solution of this problem would allow for the development of more effective computational techniques for cocyclic matrices: such a test could be achieved via computations in a permutation group of degree n. Projecting $\mathcal{G}(M)$ onto $\mathcal{A}(M)$, one could search for regular subgroups, lift these to subgroups of $\mathrm{Aut}(M)$ and test for total regularity. The additional test required involves only linear algebra, and so could be achieved in reasonable time.

Furthermore, as we observed in Chapter 2, there are many special classes of matrices M for which computation in $\mathcal{A}(M)$ is sufficient to determine whether or not M is cocyclic. Thus we pose a second problem.

Problem 6.12. *Find new classes of matrices for which it suffices to test for cocyclic development in $\mathcal{A}(M)$. (For example, such that every regular subgroup of $\mathcal{A}(M)$ gives rise to a cocycle of M.)*

6.3.2 Hadamard matrices of small order

We begin with an obvious problem, leading directly from the results of Chapter 3. It is probably reasonable to aim to classify all cocyclic Hadamard matrices of order at most 100 in the near future. Special cases of the classification may be carried out using currently available computation resources.

Problem 6.13. *Classify the cocyclic Hadamard matrices of order at most* 100.

Attacks on this problem could be motivated by a solution to Problem 6.11, as well as the computational techniques developed by Alvarez et al. [1] for cocyclic matrices. The approach of classifying Hadamard matrices via Hadamard 3-designs has not yet been explored, to our knowledge. We note that interesting theoretical and computational techniques for classifying block designs with prescribed automorphism groups are under development by the Croatian school of design theory [13, 30].

We turn now to questions motivated by the data presented in Section 3.4.1. First, we ask whether an extension of the circulant Hadamard conjecture is possible. Our motivation is that there are 14 groups of order 36, of which 12 are indexing groups for cocyclic Hadamard matrices. The two that are not both have exponent 36. (One is cyclic, the other a split extension $C_9 \rtimes C_4$, with centre of order 2.)

Problem 6.14 (cf. Jedwab [42])**.** *Does there exist a group G, which is the indexing group for a cocyclic Hadamard matrix, and for which $exp(G) = |G|$? If G is cyclic, it is known that $|G| \geq 10^{22}$, whereas the non-cyclic case does not appear to have been studied.*

We state formally the problem suggested at the end of Chapter 3: that of constructing new families of Hadamard matrices.

Problem 6.15. *Examine the Hadamard matrices produced in Chapter 3 and Problem 6.13 (and their automorphism groups) for new construction methods.*

Finally, we have produced many examples of cocyclic Hadamard matrices H with $\mathcal{A}(H)$ imprimitive. We have also studied the case that $\mathcal{A}(H)$ is doubly transitive in some detail. We are not aware of a single Hadamard matrix for which $\mathcal{A}(H)$ is simply primitive however.

Problem 6.16. *Does there exist a cocyclic Hadamard matrix H such that $\mathcal{A}(H)$ is a simply primitive permutation group?*

One attack on this problem may be via the theory of B-groups (see p. 96 of [21]).

Definition 6.17. A group G is a *B-group* if a primitive permutation group containing a regular subgroup isomorphic to G is necessarily doubly transitive.

Typical examples of B-groups are cyclic groups of prime order. As we have seen, Hadamard matrices H with doubly transitive automorphism groups appear to be rare. Thus if many of the regular subgroups of $\mathcal{A}(H)$ are B-groups, we would expect to see few Hadamard matrices with $\mathcal{A}(H)$ primitive.

6.3.3 Automorphism groups of Hadamard matrices

In the course of our treatment of twin prime power Hadamard matrices we constructed large subgroups of their automorphism groups. Finding the full automorphism group of a family of combinatorial structures is in general a difficult problem, but we pose it here.

For a twin prime power difference set $\mathcal{D}$, $\mathrm{Dev}\,(\mathcal{D})$ has automorphisms of the following types:

- $t_{a,b} : (x, y) \mapsto (x + a, y + b)$ for $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q+2}$,
- $m_{c,d} : (x, y) \mapsto (cx, dy)$ for $c \in \mathbb{F}_q^*$, $d \in \mathbb{F}_{q+2}$ and $\chi(c)\chi(d) = 1$
- $\sigma_p : (x, y) \mapsto (x^p, y)$, $\sigma_r : (x, y) \to (x, y^r)$.

Problem 6.18 (Conjecture 1, [60])**.** *Let χ denote the standard quadratic residue function on a finite field. Show that*

$$G = \left\langle (-I, -I), t_{a,b}, m_{c,d}, \sigma_p, \sigma_r : a \in \mathbb{F}_q, b \in \mathbb{F}_{q+2}, c \in \mathbb{F}_q^*, d \in \mathbb{F}_{q+2}^*, \chi(c)\chi(d) = 1 \right\rangle$$

is the full automorphism group of the TPP-Hadamard matrix arising from q and $q+2$, of order $mn(q+2)(q+1)(q)(q-1)$. Determine its isomorphism type.

We observe that G has only two non-trivial systems of imprimitivity, and is maximal with this property: any overgroup of this group either preserves a single system of imprimitivity or is primitive. It should be possible to use this information to derive a contradiction, thus proving that we have indeed described the full automorphism group.

Similarly, we can ask for the full automorphism group of a HSR-Hadamard matrix.

Problem 6.19. *Determine the full automorphism group of a HSR-Hadamard matrix.*

6.3.4 Skew Hadamard difference sets

A research problem of Jungnickel [44] is to classify all skew Hadamard difference sets. Note that every skew Hadamard difference set has a corresponding Hadamard 3-design.

Theorem 6.20 (Kimberley, Theorem 7, [50])**.** *Let Δ be the Hadamard 3-design of the Hadamard matrix H. Then $\mathcal{A}(H)$ is doubly transitive on the rows of H if and only if the induced action of $\mathcal{A}(H)$ on the blocks of Δ is transitive.*

Suppose that H is developed from a skew Hadamard difference set. We observe that $\mathcal{A}(H)$ has at most four orbits on the blocks of the associated Hadamard 3-design. Our classification of skew Hadamard difference sets for which the automorphism group of the corresponding Hadamard matrix is transitive gives a classification for the case that $\mathcal{A}(H)$ is transitive on the blocks of the associated Hadamard 3-design.

Problem 6.21. *Investigate the skew Hadamard difference sets for which $\mathcal{A}(H)$ has precisely 2 or 3 or 4 orbits on the blocks of the associated 3-design.*

Index

Bibliography

[1] V. Álvarez, J. A. Armario, M. D. Frau, and P. Real. A system of equations for describing cocyclic Hadamard matrices. *J. Combin. Des.*, 16(4):276–290, 2008.

[2] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[3] E. F. Assmus, Jr. and C. J. Salwach. The (16, 6, 2) designs. *Internat. J. Math. Math. Sci.*, 2(2):261–281, 1979.

[4] L. D. Baumert. *Cyclic difference sets*. Lecture Notes in Mathematics, Vol. 182. Springer-Verlag, Berlin, 1971.

[5] T. Beth, D. Jungnickel, and H. Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[6] N. L. Biggs. T. P. Kirkman, mathematician. *Bull. London Math. Soc.*, 13(2):97–120, 1981.

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

[8] I. Bouyukliev, V. Fack, and J. Winne. 2-(31,15,7), 2-(35,17,8) and 2-(36,15,6) designs with automorphisms of odd prime order, and their related Hadamard matrices and codes. *Des. Codes Cryptogr.*, 51(2):105–122, 2009.

[9] R. H. Bruck. Difference sets in a finite group. *Trans. Amer. Math. Soc.*, 78:464–481, 1955.

[10] W. Burnside. *Theory of groups of finite order*. Dover Publications Inc., New York, 1955. 2d ed.

[11] P. J. Cameron. Permutation groups. In *Handbook of combinatorics, Vol. 1, 2*, pages 611–645. Elsevier, Amsterdam, 1995.

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[13] D. Crnković and S. Rukavina. On Hadamard $(35, 17, 8)$ designs and their automorphism groups. *J. Appl. Algebra Discrete Struct.*, 1(3):165–180, 2003.

[14] C. W. Curtis. *Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer*, volume 15 of *History of Mathematics*. American Mathematical Society, Providence, RI, 1999.

[15] C. W. Curtis, W. M. Kantor, and G. M. Seitz. The 2-transitive permutation representations of the finite Chevalley groups. *Trans. Amer. Math. Soc.*, 218:1–59, 1976.

[16] W. de Launey and D. Flannery. *Algebraic Design Theory*. Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence, RI, 2011.

[17] W. de Launey, D. L. Flannery, and K. J. Horadam. Cocyclic Hadamard matrices and difference sets. *Discrete Appl. Math.*, 102(1-2):47–61, 2000. Coding, cryptography and computer security (Lethbridge, AB, 1998).

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

[19] J. F. Dillon. Some REALLY beautiful Hadamard matrices. *Cryptogr. Commun.*, 2(2):271–292, 2010.

[20] C. Ding and J. Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.

[21] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[22] T. Feng. Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism. *J. Combin. Theory Ser. A*, 118(1):27–36, 2011.

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

[24] S. W. Golomb and H.-Y. Song. A conjecture on the existence of cyclic Hadamard difference sets. *J. Statist. Plann. Inference*, 62(1):39–41, 1997.

[25] D. Gorenstein, R. Lyons, and R. Solomon. *The classification of the finite simple groups*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1994.

[26] J. Hadamard. Résolution d'une question relative aux déterminants. *Bull. Sci. Math.*, 17:240–246, 1893.

[27] M. Hall, Jr. Note on the Mathieu group M_{12}. *Arch. Math. (Basel)*, 13:334–340, 1962.

[28] M. Hall, Jr. Group properties of Hadamard matrices. *J. Austral. Math. Soc. Ser. A*, 21(2):247–256, 1976.

[29] M. Hall, Jr. *Combinatorial theory*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons Inc., New York, second edition, 1986.

[30] D. Held, M.-O. Pavčević, and M. Schmidt. A series of finite groups and related symmetric designs. *Glas. Mat. Ser. III*, 42(62)(2):257–272, 2007.

[31] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata*, 2:425–460, 1974.

[32] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II. *J. Algebra*, 93(1):151–164, 1985.

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

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

[35] D. R. Hughes and F. C. Piper. *Design theory*. Cambridge University Press, Cambridge, 1985.

[36] B. Huppert and N. Blackburn. *Finite groups. III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982.

[37] N. Ito. Hadamard matrices with "doubly transitive" automorphism groups. *Arch. Math. (Basel)*, 35(1-2):100–111, 1980.

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

[39] N. Ito and H. Kimura. Studies on Hadamard matrices with "2-transitive" automorphism groups. *J. Math. Soc. Japan*, 36(1):63–73, 1984.

[40] N. Ito and J. S. Leon. An Hadamard matrix of order 36. *J. Combin. Theory Ser. A*, 34(2):244–247, 1983.

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

[42] J. Jedwab. What can be used instead of a Barker sequence? In *Finite fields and applications*, volume 461 of *Contemp. Math.*, pages 153–178. Amer. Math. Soc., Providence, RI, 2008.

[43] D. Jungnickel. On difference matrices, resolvable transversal designs and generalized Hadamard matrices. *Math. Z.*, 167(1):49–60, 1979.

[44] D. Jungnickel. Difference sets. In *Contemporary design theory*, Wiley-Intersci. Ser. Discrete Math. Optim., pages 241–324. Wiley, New York, 1992.

[45] W. M. Kantor. 2-transitive symmetric designs. *Trans. Amer. Math. Soc.*, 146:1–28, 1969.

[46] W. M. Kantor. Automorphism groups of Hadamard matrices. *J. Comb. Theory*, 6:279–281, 1969.

[47] W. M. Kantor. Symplectic groups, symmetric designs, and line ovals. *J. Algebra*, 33:43–58, 1975.

[48] W. M. Kantor. Classification of 2-transitive symmetric designs. *Graphs Combin.*, 1(2):165–166, 1985.

[49] H. Kharaghani and B. Tayfeh-Rezaie. On the classification of Hadamard matrices of order 32. *J. Combin. Des.*, 18(5):328–336, 2010.

[50] M. E. Kimberley. On collineations of Hadamard designs. *J. London Math. Soc. (2)*, 6:713–724, 1973.

[51] T. P. Kirkman. On a problem in combinations. *Cambridge and Dublin Math. J.*, 2:191–204, 1847.

[52] T. P. Kirkman. Note on an unanswered prize question. *Cambridge and Dublin Math. J.*, 5:255–262, 1850.

[53] T. P. Kirkman. On the perfect r-partitions of $r^2 + r + 1$. *Trans of the Hist. Soc. of Lancashire and Cheshire*, 9:127–142, 1857.

[54] M. W. Liebeck, C. E. Praeger, and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra*, 111(2):365–383, 1987.

[55] G. E. Moorhouse. *The 2-transitive complex Hadamard matrices. Preprint.* http://www.uwyo.edu/moorhouse/pub/complex.pdf.

[56] L. J. Mordell. The diophantine equations $2^n = x^2 + 7$. *Ark. Mat.*, 4:455–460, 1962.

[57] M. Muzychuk. On skew Hadamard difference sets. *Arxiv.net*, 1012.2089v1, 2010.

[58] P. Ó Catháin. *Automorphisms of pairwise combinatorial designs.* Ph.D. thesis, National University of Ireland, Galway, 2011.

[59] P. Ó Catháin and M. Röder. The cocyclic Hadamard matrices of order less than 40. *Des. Codes Cryptogr.*, 58(1):73–88, 2011.

[60] P. Ó Catháin and R. M. Stafford. On twin prime power Hadamard matrices. *Cryptogr. Commun.*, 2(2):261–269, 2010.

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

[62] R. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.

[63] D. Passman. *Permutation groups.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[64] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1995.

[65] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

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

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

[68] M. Röder. *RDS, Version 1.0*. http://www.gap-system.org/Packages/rds.html, 2008.

[69] H. J. Ryser. *Combinatorial mathematics*. The Carus Mathematical Monographs, No. 14. Published by The Mathematical Association of America, 1963.

[70] K. W. Smith. Non-abelian Hadamard difference sets. *J. Combin. Theory Ser. A*, 70(1):144–156, 1995.

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

[72] T. Storer. *Cyclotomy and difference sets*. Lectures in Advanced Mathematics, No. 2. Markham Publishing Co., Chicago, Ill., 1967.

[73] J. Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to newton's rule, ornamental tile-work, and the theory of numbers. *Phil. Mag.*, 34(1):461–475, 1867.

[74] H. Wielandt. *Finite permutation groups*. Translated from the German by R. Bercov. Academic Press, New York, 1964.

[75] J. Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 11:65–81, 1944.

[76] R. A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2009.