<table>
<thead>
<tr>
<th>Title</th>
<th>Topics in cocyclic development of pairwise combinatorial designs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Egan, Ronan</td>
</tr>
<tr>
<td>Publication Date</td>
<td>2015-10-14</td>
</tr>
<tr>
<td>Item record</td>
<td><a href="http://hdl.handle.net/10379/5306">http://hdl.handle.net/10379/5306</a></td>
</tr>
</tbody>
</table>
PhD thesis

Topics in Cocyclic Development of Pairwise Combinatorial Designs

Ronan Egan

July 2015

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy
Supervised by Dr Dane Flannery
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>vii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>1</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>1.1. Overview</td>
<td>3</td>
</tr>
<tr>
<td>1.2. Outline</td>
<td>5</td>
</tr>
<tr>
<td>2. Preliminaries</td>
<td>7</td>
</tr>
<tr>
<td>2.1. Algebraic essentials</td>
<td>7</td>
</tr>
<tr>
<td>2.2. Pairwise combinatorial designs</td>
<td>9</td>
</tr>
<tr>
<td>2.3. Automorphism groups</td>
<td>14</td>
</tr>
<tr>
<td>2.4. Regular subgroups and group development</td>
<td>16</td>
</tr>
<tr>
<td>2.5. Cocyclic development</td>
<td>17</td>
</tr>
<tr>
<td>2.6. The translation group</td>
<td>18</td>
</tr>
<tr>
<td>2.7. Difference sets and relative difference sets</td>
<td>20</td>
</tr>
<tr>
<td>I. Cocyclic development of generalized Sylvester Hadamard matrices</td>
<td>21</td>
</tr>
<tr>
<td>3. The generalized Sylvester matrix</td>
<td>23</td>
</tr>
<tr>
<td>3.1. Introduction to the generalized Sylvester matrix</td>
<td>23</td>
</tr>
<tr>
<td>3.2. Automorphism group actions</td>
<td>24</td>
</tr>
<tr>
<td>3.3. Indexing groups of $D_{(p,m,k)}$</td>
<td>29</td>
</tr>
<tr>
<td>3.4. Existing subgroups of $AGL(k,p)$</td>
<td>33</td>
</tr>
<tr>
<td>4. Automorphisms of Kantor’s design</td>
<td>35</td>
</tr>
<tr>
<td>4.1. Actions of the translation group on $K_{2n}$</td>
<td>35</td>
</tr>
<tr>
<td>4.2. Kantor’s design as a $2-(v, k, \lambda)$-design</td>
<td>38</td>
</tr>
<tr>
<td>4.3. Regular subgroups of $P Aut(K_{2n})$</td>
<td>41</td>
</tr>
<tr>
<td>II. Shift representations on 2-cocycles</td>
<td>43</td>
</tr>
<tr>
<td>5. Shift actions</td>
<td>45</td>
</tr>
<tr>
<td>5.1. Shift actions</td>
<td>45</td>
</tr>
</tbody>
</table>
5.2. Fixed points .................................................. 46

6. Linear shift representations 53
   6.1. Shift representations .................................... 53
   6.2. Shift representations via linear groups ............... 55
   6.3. Completely reducible representations .................. 57
   6.4. Orbits in $B(G,U)$ ...................................... 63
   6.5. Computing with shift representations .................. 65
   6.6. Further computational results .......................... 66

II. Cocyclic Butson Hadamard matrices 71
7. Classification of small cocyclic $BH(n,p)$s 73
   7.1. Equivalence of generalized Hadamard and Butson Hadamard matrices .................................. 74
   7.2. Central relative difference sets ......................... 76
   7.3. Cocyclic Butson Hadamard matrices .................... 76
   7.4. Non-existence of generalized Hadamard matrices .... 77
   7.5. The full classification .................................. 82

8. Cocyclic development via dihedral and dicyclic groups 85
   8.1. Cocyclic development over dihedral groups .......... 85
   8.2. Cocyclic Hadamard matrices with dicyclic extension groups 86
   8.3. Centrally relative difference sets via pairs of binary sequences ........................................ 87

9. Conclusions and open problems 99
   9.1. Cocyclic development of the generalized Sylvester matrix 99
   9.2. Shift actions ............................................. 99
   9.3. Cocyclic Butson Hadamard matrices .................... 100
   9.4. Final comments ......................................... 101

Bibliography 102
I hereby certify that this thesis which I now submit for assessment as partial fulfillment of the requirements for the award of Doctor of Philosophy is entirely my own work and has not been taken from the work of others; save and to the extent that such work has been cited and acknowledged within the text. I have not obtained a degree in this University, or elsewhere, on the basis of this work.

Signed ____________________  Date ____________________
Abstract

This thesis is a compilation of results dealing with cocyclic development of pairwise combinatorial designs.

Motivated by a classification of the indexing and extension groups of the Paley Hadamard matrices due to de Launey and Stafford, we investigate cocyclic development of the so-called generalized Sylvester (or Drake) Hadamard matrices. We describe the automorphism groups and derive strict conditions on possible indexing groups, addressing research problems of de Launey and Flannery in doing so.

The shift action, discovered by Horadam, is a certain action of any finite group on the set of its 2-cocycles with trivial coefficients, which preserves both cohomological equivalence and orthogonality. We answer questions posed by Horadam about the shift action, in particular regarding its fixed points. One of our main innovations is the concept of linear shift representation. We give an algorithm for calculating the matrix group representation of a shift action, which enables us to compute with the action in a natural setting. We prove detailed results on reducibility, and discuss the outcomes of some computational experiments, including searches for orthogonal cocycles.

Using the algorithms developed for shift representations, and other methods, we classify up to equivalence all cocyclic BH(n, p)s where p is an odd prime (necessarily dividing n) and np ≤ 100. This was achievable with the further aid of our new non-existence results for a wide range of orders.
Acknowledgements

I acknowledge the financial support of an NUI Galway Hardiman scholarship, and the Irish Research Council. I also acknowledge the School of Mathematics, Statistics and Applied Mathematics, the College of Science, the organizers of the British Mathematics Colloquium, the organizers of the 2014 Algebraic Design Theory and Hadamard Matrices conference, and the organizers of the 2015 Combinatorics and Computer Algebra conference for assisting with travel expenses I incurred during my studies.

I am grateful for the support and guidance offered by the staff of the School of Maths over the years, in particular my Graduate Research Committee of Michael McGettrick, Ray Ryan and Jerome Sheahan. Special thanks to Jerome for his guidance during my final year of undergraduate studies, and for the many academic references he provided which played a vital role in securing funding for my PhD.

I thank Padraig Ó Catháin for his contributions as a colleague and collaborator which led to a joint publication, and to the completion of Chapter 7 of this thesis. I am grateful to Eamonn O’Brien for his correspondence and assistance with MAGMA related issues. I thank Rob Craigen for his helpful comments and discussions, in particular regarding the content of Chapter 8.

Special thanks go to my fellow postgraduate students (there are too many to name) for making the last four years as enjoyable as they were, and to Riverside Terrapin for being what it was.

Last but not least, I thank my supervisor Dane Flannery. Without his encouragement and advice I would never have reached the point of writing these acknowledgements.
1. Introduction

This thesis is a compilation of results related by the common theme of cocyclic development of pairwise combinatorial designs (PCDs). We focus on generalized Hadamard and Butson Hadamard matrices, although much of what we do extends to other kinds of PCDs. These designs are familiar combinatorial objects; they have been studied in a range of different settings for well over a century. Renewed attention has recently been given to their algebraic aspects. Algebraic design theory, the primary field of this thesis, is the study of PCDs in terms of any underlying algebraic structure that they might have.

1.1. Overview

The origins of design theory lie in combinatorial mathematics. Many problems in combinatorics, while perhaps first studied for their aesthetic appeal, are now highly applicable to other areas of mathematics and science. Examples include Kirkman’s schoolgirl problem, Bachet’s problem of the weights, and Hadamard’s maximum determinant problem. Indeed, problems in statistics and experimental science often obtain the best solution via designs with appropriate combinatorial constraints.

Algebraic design theory, as we understand the term here, is codified in the book [21]. Within this framework we can formally define equivalence of designs, study their automorphism groups, and generate new designs through methods such as cocyclic development and various composition techniques. All these aspects of algebraic design theory are covered in the thesis.

1.1.1. Cocyclic development

There are numerous constructions of designs, some of them very old. For example, Sylvester’s construction [69] gives a Hadamard matrix of order $2^n$ for all positive integers $n$. Paley’s constructions provide the densest known class of
1. Introduction

Hadamard matrices. That is, for a sufficiently large integer interval there exists a Paley type Hadamard matrix at more orders within that interval than any resulting from other known constructions. Let \( q = p^n \) for an odd prime \( p \). The Paley type I Hadamard matrices are of order \( q + 1 \) where \( q \equiv 3 \mod 4 \), and the type II Hadamard matrices are of order \( 2(q + 1) \) where \( q \equiv 1 \mod 4 \). In fact these are all cocyclic matrices. The cocyclic development of the Paley-type matrices was exhaustively described by de Launey and Stafford (see, e.g., [23]). In Chapter 3 we embark on an analogous study of the cocyclic development of a generalization of the Sylvester matrices.

Introduced by Horadam and de Launey in 1993 [47], cocyclic development has turned out to be a fruitful construction technique for PCDs. It has the advantage of being an algebraic construction, not relying solely on combinatorial concerns. This means that we can be quite systematic in searching for and constructing cocyclic designs.

We describe cocyclic development in detail in Section 2.5. Let \( G \) and \( U \) be finite groups, with \( U \) abelian. A map \( \psi : G \times G \rightarrow U \) satisfying

\[
\psi(g, h)\psi(gh, k) = \psi(g, hk)\psi(h, k)
\]

for all \( g, h, k \in G \) is a cocycle, or more formally a 2-cocycle. The set of all such cocycles forms a group, denoted \( Z^2(G, U) \). For a cocycle \( \psi \), a matrix \( M \) equivalent under standard row and column operations to \( [\phi(gh)\psi(g, h)]_{g,h \in G} \) for some map \( \phi \) is said to be cocyclic, and \( G \) is an indexing group of \( M \).

Cocyclic development encompasses several composition results, which generate new, larger designs from existing cocyclic designs of smaller order. This usually involves taking some sort of product \( G_1G_2 \) of ingredient indexing groups \( G_1 \) and \( G_2 \).

1.1.2. Applications of designs

The wealth of their applications motivates the study of designs such as Hadamard matrices. Chapter XIII of the book [6] by Beth, Jungnickel and Lenz is devoted to applications. These range from experimental design, to optics, to algorithms. The CRC Handbook of Combinatorial Designs [14] edited by Colbourn and Dinitz is an exhaustive compendium of design theory results. Part V
gathers papers on applications. We also refer to Chapter 3 of Horadam’s book \[43\] for a detailed description of the use of Hadamard matrices in signal processing, coding, and cryptography. A large amount of information regarding complex Hadamard matrices in quantum computer science is available at \[11\], where a catalogue of known complex Hadamard matrices and Butson Hadamard matrices is curated.

### 1.2. Outline

This section briefly summarizes the content of each chapter in this thesis. Following this introduction, Chapter 2 provides the necessary preliminaries of algebraic design theory and cocyclic development, as well as other fundamental ideas that we will need.

After Chapter 2, the thesis is divided into three main parts. These are mostly independent of each other, although of course they are related under the heading of cocyclic development. Each part draws on the preliminaries in Chapter 2.

Part I, Chapter 3 is a case study of cocyclic development, focussing on what we call *generalized Sylvester Hadamard matrices*, a family of generalized Hadamard matrices that contains the Sylvester matrices as a (very) special case. In this chapter we describe the automorphism group of the generalized Sylvester matrix, and use this description to derive strict conditions for its indexing groups. We then turn our attention to a related design in Chapter 4, which we call *Kantor’s design* in honor of its appearance in \[52\], though its existence was known to Block \[7\] prior to this. Broadly speaking, the cocyclic development of Kantor’s design is subsumed by that of the Sylvester matrix of the same order; our focus is rather on group development specifically.

Part II subsumes and expands upon \[35\]. In Chapter 5 we present results about a certain action a group \(G\) has on the set of its 2-cocycles, known as *shift action*. Discovered by Horadam \[44\], the shift action has the attractive property of preserving both cohomology and orthogonality. Orthogonal cocycles yield cocyclic PCDs, and shift action enables a (slightly) more efficient search for such cocycles. We settle some research questions posed by Horadam regarding fixed points under the shift action. This also serves as a vital building block which enables us to prove some of the main results of Chapter 6.

Chapter 6 is perhaps the most significant chapter of the thesis. There we
1. **Introduction**

Introduce and develop the notion of linear shift representations. This represents the shift action of $G$ on $Z^2(G,U)$ in an associated general linear group. The matrix group, nearly always a faithful copy of $G$, acts on the underlying vector space $Z^2(G,U)$. Thus we are furnished with all the methods of linear algebra and (elementary) theory of matrix groups to compute effectively with the shift action. An algorithm for computing shift representations is described; this has been implemented in MAGMA [8]. We also answer several questions regarding reducibility of shift representations. Some computational results are given. As mentioned, the bulk of Chapter 6 has previously been published in our joint paper [35] with Dane Flannery.

Part III, Chapter 7 applies some of the machinery developed in Chapter 6. We summarize the results of [31], which is joint work with Dane Flannery and Padraig Ó Catháin. Our problem was to classify, up to equivalence, all cocyclic $n \times n$ Butson Hadamard matrices over $p$th roots unity, for an odd prime $p$ such that $np \leq 100$. Non-existence results are developed. The existing matrices in the classification were discovered using the computational tools of Chapter 6 and of [64]. All matrices found have been sorted into their respective equivalence classes, some of which were previously unknown. Detailed results of the classification are currently available at [32].

In Chapter 8 we review known results on cocyclic development of (ordinary) Hadamard matrices over dicyclic and dihedral groups. There exists a cocyclic Hadamard matrix of order $4t$ if and only if there is a central relative $(4t, 2, 4t, 2t)$-difference set in a certain corresponding group known as Hadamard group. A key example of the latter is the dicyclic group $Q_{8t}$ of order $8t$. We introduce a correspondence between the central relative difference sets and pairs of $\{\pm 1\}$-sequences with certain autocorrelation properties. This chapter builds on the work of Flannery [33], Schmidt [67], and Ito [50, 51]. It lends further strong support to de Launey and Horadam’s ‘cocyclic Hadamard conjecture’.

Finally, in Chapter 9 we make some concluding comments, and discuss avenues for future research. We pose several viable research problems suggested by the results of this thesis.
2. Preliminaries

This chapter presents a small amount of background material required for our purposes. The chapter also serves to fix some notation that we use throughout the thesis. Any other necessary background will be covered or referenced just before it is used.

2.1. Algebraic essentials

We assume familiarity with basic group, ring, and module theory, as may be found in a graduate algebra text such as [48].

2.1.1. Group products

For subgroups $H, K$ of a group $G$, $[H, K] = \langle [h, k] : h \in H, k \in K \rangle$ where $[h, k] = h^{-1}h^k = h^{-1}k^{-1}hk$. (If $H = K = G$ then we also denote the commutator subgroup $[G, G]$ of $G$ by $G'$.) When $|H \cap K| = 1$ we often write $H \cap K = 1$.

Suppose that the group $G$ is a product of its subgroups $H$ and $K$; i.e., $G = HK = \{ab | a \in H, b \in K\}$. If $H \cap K = 1$ and $H \leq G$ then $G = H \times K$ is a semidirect product or split extension (of $H$ by $K$); $G$ splits over $H$, and $K$ is a complement of $H$ in $G$. If also $[H, K] = 1$ then $G = H \times K$ is the direct product. We may call this the direct sum if both $H$ and $K$ are abelian.

For a permutation group $G$ of degree $n$ (i.e., subgroup of the full symmetric group $\text{Sym}(n)$ on $\{1, \ldots, n\}$) and group $H$, the wreath product $H \wr G$ is the semidirect product $H^n \rtimes G$ where

$$g(h_1, h_2, \ldots, h_n)g^{-1} = (h_{g^{-1}1}, h_{g^{-1}2}, \ldots, h_{g^{-1}n}), \ g \in G, h_i \in H.$$ 

2.1.2. Linear groups

Let $R$ be an associative ring with 1 (our rings are always associative and unital). The general linear group $\text{GL}(n, R)$ of degree $n$ over $R$ is the group of all invertible
2. Preliminaries

\( n \times n \) matrices with entries in \( R \). If \( R = \mathbb{F} \) is a field then \( \text{GL}(n, \mathbb{F}) \) consists of all \( n \times n \) matrices with entries in \( \mathbb{F} \) and non-zero determinant; if \( \mathbb{F} \) is the finite field \( \text{GF}(q) \) of size \( q \) then we use the notation \( \text{GL}(n, q) \). Say \( q = p^r \), \( p \) prime. The set of all \( n \times n \) upper unitriangular matrices over \( \text{GF}(q) \) (i.e., the matrices with 1s on the main diagonal and zeros everywhere below) is a Sylow \( p \)-subgroup of \( \text{GL}(n, q) \), of order \( q^{n(n-1)/2} \).

We denote by \( \text{Sp}(2n, q) \) the symplectic group of degree \( 2n \) over \( \text{GF}(q) \). Up to conjugacy, this is the set of all \( x \in \text{GL}(2n, q) \) such that \( xF x^\top = F \) (equivalently, \( x^\top F x = F \)) where \( F = \begin{bmatrix} 0_n & I_n \\ -I_n & 0_n \end{bmatrix} \), \( I_n \) the \( n \times n \) identity matrix and \( 0_n \) the \( n \times n \) matrix of all zeros. Note that \( \text{Sp}(2n, q) \leq \text{SL}(2n, q) \), the subgroup of \( \text{GL}(2n, q) \) comprised of matrices with determinant 1.

2.1.3. Actions

We allow groups \( G \) to act on the left or right of a (non-empty) set \( X \). An action of \( G \) on \( X \) is faithful if for each non-identity element \( g \) of \( G \) there exists some \( x \in X \) such that \( gx \neq x \). The action is transitive if \( X \) is the unique \( G \)-orbit.

The action is \( k \)-transitive if \( X \) has at least \( k \) elements and for any two \( k \)-tuples \( (x_1, x_2, \ldots, x_k) \) and \( (y_1, y_2, \ldots, y_k) \) of pairwise distinct elements of \( X \), there is \( g \in G \) such that \( gx_i = y_i \) for \( 1 \leq i \leq k \).

A group action is semi-regular if each point stabilizer \( G_x := \{ g \in G \mid gx = x \} \) is trivial. The action is regular if it is both semi-regular and transitive.

A permutation group \( G \leq \text{Sym}(X) \) is called primitive if \( G \) acts transitively on \( X \) and preserves no non-trivial partition of \( X \).

2.1.4. Linear representations

Let \( G \) be a finite group and \( \mathbb{K} \) be a field. A (linear) representation of \( G \) over \( \mathbb{K} \) is a homomorphism \( \Gamma \) of \( G \) into the general linear group \( \text{GL}(V) \) of all invertible \( \mathbb{K} \)-linear transformations of a finite dimensional \( \mathbb{K} \)-vector space \( V \). After choosing a basis for \( V \), we may identify \( \text{GL}(V) \) with \( \text{GL}(n, \mathbb{K}) \), and call \( \Gamma \) a matrix representation of \( G \). The dimension \( n \) of \( V \) is the degree of \( \Gamma \). We say that \( \Gamma \) is faithful if it is injective. We usually assume that the linear group \( \Gamma(G) \) acts on the right of \( V \); in matrix terms this means that we are treating the elements of \( V \) as row vectors.
Given a representation $\Gamma : G \to \text{GL}(V)$, the $\mathbb{K}$-vector space $V$ is a $\Gamma(G)$-module. A subspace $W$ of $V$ is a $\Gamma(G)$-submodule if $w\Gamma(g) \in W$ for all $w \in W$ and $g \in G$. If $V$ has no proper non-zero $\Gamma(G)$-submodules then $V$ is said to be irreducible; otherwise it is reducible. A module $V$ is completely reducible if it is a direct sum of irreducible submodules. Note that an irreducible module is completely reducible.

2.2. Pairwise combinatorial designs

The notion of PCD is introduced in [21], the vital reference for this subsection, where full justifications of statements may be found.

Let $A$ be a non-empty finite set not containing 0. (To begin with, 0 is just a special symbol apart from the elements of $A$; later, 0 becomes the additive identity of a ring containing $A$.) Let $\Lambda$ be a set of $2 \times v (0, A)$-arrays closed under all permutations of rows and columns. We also insist that no array in $\Lambda$ has a repeated row. Then $\Lambda$ is an orthogonality set. A pairwise combinatorial design $\text{PCD}(\Lambda)$ is a $v \times v$ array $D$ such that each pair of distinct rows of $D$ is in $\Lambda$ (each pair of rows are $\Lambda$-orthogonal).

An ambient ring $\mathcal{R}$ for an orthogonality set $\Lambda$ is, at least in the first instance, merely an (associative, unital) ring containing $A$. We can always arrange for $\mathcal{R}$ to be an involutory ring that contains a ‘row group’ $R \cong \Pi^\text{row}_\Lambda$ and ‘column group’ $C \cong \Pi^\text{col}_\Lambda$ in its group of units. (There are other, quite technical, requirements; see [21, Chapter 5]. The group $\Pi^\text{row}_\Lambda$ consists of all local row equivalence operations—permutations of $\{0\} \cup A$ fixing 0 which, if applied entrywise to a row, leave $\Lambda$ invariant. The group $\Pi^\text{col}_\Lambda$ of local column equivalence operations is defined analogously.) This kind of ambient ring is required to model $\Lambda$-equivalence, as we sketch out in Section 2.2.4 below.

2.2.1. Matrices

When we use the term matrix for an array, we are often treating its entries as elements of some ring.

Let $\text{Mat}(n, \mathcal{R})$ denote the set of all $n \times n$ matrices with entries in a ring $\mathcal{R}$. This is itself a ring under matrix multiplication and addition, with identity $I_n$.

A monomial matrix has exactly one non-zero entry in every row and column. A permutation matrix is a monomial matrix with each non-zero entry equal to
2. Preliminaries

1 (in some ring). Denote by Perm($n, \mathcal{R}$) or just Perm($n$) the group of all $n \times n$ permutation matrices over $\mathcal{R}$; Mon($n, \mathcal{R}$) is the group of all $n \times n$ monomial matrices over $\mathcal{R}$. We may identify Perm($n$) with Sym($n$) via the isomorphism $\alpha \mapsto P_{\alpha} := [\delta_{\alpha(j)}]_{1 \leq i,j \leq n}$ (using Kronecker delta notation, i.e., $\delta_{r,s}$ is 1 if $r = s$ and 0 otherwise). If $M \in \text{Mat}(n, \mathcal{R})$ then pre-multiplication of $M$ by $P_{\alpha}$ moves row $i$ to row $\alpha(i)$; post-multiplication of $M$ by $P_{\alpha}^T$ moves column $j$ to column $\alpha(j)$.

A *regular* matrix is one with constant row and column sum. A *normalized* matrix has first row and first column consisting entirely of 1s. An $n \times n$ *circulant* matrix $C = [c_{ij}]$ has each row equal to the row above it but shifted rightwards one position, i.e., $c_{i+1,j+1} = c_{ij}$. A circulant matrix is fully specified by any one of its rows or columns. If subsequent rows of $C$ are shifted leftwards one position instead, i.e., $c_{i+1,j-1} = c_{ij}$, then $C$ is *back circulant*.

Let $A$ and $B$ be matrices, not necessarily square or of the same dimension. We denote by $A \otimes B$ the *Kronecker product* of $A$ and $B$. That is, $A \otimes B$ is the block matrix with $(i,j)$th block $a_{ij} B$. Note that we can permute rows and columns of $B \otimes A$ to get $A \otimes B$ as long as the entries of $A$ commute with the entries of $B$.

2.2.2. Design basics

Let $P$ be a set of $v$ points. Let $\mathcal{B}$ be a set of $k$-subsets of $P$, called *blocks*, where every $t$ distinct points lie in precisely $\lambda$ blocks. The pair $(P, \mathcal{B})$ is a $t$-$(v, k, \lambda)$-design. If every point is in precisely $r$ blocks and $|\mathcal{B}| = b$, then $vr = bk$. The design $(P, \mathcal{B})$ is symmetric if $|\mathcal{B}| = |P|$. Thus $k = r$ for a symmetric design.

An *incidence structure* is a triple $D = (P, \mathcal{B}, I)$ where $I$ is a binary relation between $P$ and $\mathcal{B}$. That is, $(p, B) \in I$ if and only if $p \in B$ for any $p \in P$ and $B \in \mathcal{B}$. An *incidence matrix* of the design $(P, \mathcal{B})$ is $M = [\phi(p, B)]_{p \in P, B \in \mathcal{B}}$ where $\phi(p, B) = 1$ if $(p, B) \in I$ and $\phi(p, B) = 0$ otherwise. The dual structure $D^*$ of $D$ is defined by $D^* = (\mathcal{B}, P, I^*)$ where $(B, p) \in I^*$ if and only if $(p, B) \in I$.

2.2.3. The expanded design and the associated design

Let $M$ be a PCD($\Lambda$) with ambient involutory ring $\mathcal{R}$ for $\Lambda$, containing row group $R \cong \Pi^\text{row}_\Lambda$ and column group $C \cong \Pi^\text{col}_\Lambda$. The *expanded design* $E_M$ of $M$ is

$$E_M = [rMc]_{r \in R, c \in C}.$$
The associated design $A_M$ of $M$ is obtained from the expanded design by replacing each of its non-identity entries with 0.

2.2.1 Example. Let $\zeta$ be a primitive third root of unity. If

$$M = \begin{bmatrix}
1 & 1 & 1 \\
1 & \zeta & \zeta^2 \\
1 & \zeta^2 & \zeta
\end{bmatrix}$$

then $E_M$ and $A_M$ are

$$\begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}$$

respectively.

2.2.4. Equivalence

Two matrices $M$, $N$ are permutation equivalent, written $M \sim N$, if there are permutation matrices $P$ and $Q$ such that $PMQ = N$. That is, $N$ can be obtained from $M$ by permuting the rows and columns of $M$—and vice versa.

Let $R$ be an ambient involutory ring for an orthogonality set $\Lambda$ of $2 \times v$ arrays with alphabet $A$. Two $v \times v$ ($0, A$)-arrays $X$ and $Y$ are $\Lambda$-equivalent if $Y$ can be obtained from $X$ by any sequence of the following operations:

- interchanging two rows or two columns of $X$,
- replacing a row $[x_{ij}]_{1 \leq j \leq v}$ by $[\rho(x_{ij})]_{1 \leq j \leq v}$ for some permutation $\rho \in \Pi_{\Lambda}^{\text{row}}$,
- replacing a column $[x_{ij}]_{1 \leq i \leq v}$ by $[\kappa(x_{ij})]_{1 \leq i \leq v}$ for some permutation $\kappa \in \Pi_{\Lambda}^{\text{col}}$.

If $R$, $C$ as usual are row and column groups in $\mathcal{R}$, then the above amounts to there being $P \in \text{Mon}(n, R)$ and $Q \in \text{Mon}(n, C)$ such that $Y = PXQ$. We write $X \approx_{\Lambda} Y$ if $X$ and $Y$ are $\Lambda$-equivalent.
2. Preliminaries

2.2.5. Hadamard matrices

A Hadamard matrix of order $n$ is an $n \times n$ matrix $H$ with entries in $\{\pm 1\}$ such that

$$HH^\top = nI_n.$$ 

A Hadamard matrix of order $n$ can exist only for $n = 1$, $2$ or $n$ a multiple of $4$; but it is still unknown whether the converse holds.

A regular Hadamard matrix must have square order. A circulant Hadamard matrix is regular, and the only known circulant Hadamard matrix has order $4$; see Example 2.3.1. Indeed, Ryser [66, p.134] conjectured that there is no circulant Hadamard matrix of order $n$ for $n \neq 4$.

We say that Hadamard matrices $H_A$, $H_B$ of order $n$ are Hadamard equivalent if there are $\{\pm 1\}$-monomial matrices $P$, $Q$ such that $PH_AQ = H_B$ (this is precisely $\Lambda$-equivalence for Hadamard matrices as PCD($\Lambda$)s).

We define the Sylvester Hadamard matrix $H_m$ of order $2^m$ as follows: let $H_0 = [1]$, and for $m \geq 1$ let

$$H_m = \bigotimes^m \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$ 

Sometimes we also denote by $H_m$ any matrix in the permutation equivalence class of $H_m$. Let $V_m$ be the $m$-dimensional vector space over GF(2). Then $H_m = [(-1)^{x \cdot y}]_{x,y \in V_m}$ where the ordering of the elements of $V_m$ is lexicographic (say). Note that we can essentially choose any ordering of rows and columns of $H_m$, thinking of the design as being defined up to permutation equivalence. This is a recurring philosophy that we adopt when indexing PCDs.

Let $D = (P, B)$ be a symmetric design with $|P| = v$, such that every point is in precisely $k$ blocks, and every block is a $k$-subset of $P$. Let $H' = 2M - J_v$ where $M$ is an incidence matrix for $D$ and $J_v$ denotes the $v \times v$ all $1$s matrix. Then let $H$ be the matrix obtained by appending a row and column of $1$s to $H'$. If $H$ is Hadamard then $D$ is called a Hadamard design. The parameters of a Hadamard design are $v = 4n - 1$, $k = 2n - 1$, and $\lambda = n - 1$ for some positive integer $n$. Likewise, every Hadamard matrix gives rise to a Hadamard design, by reversing this process. The matrix $H'$ is the core of the Hadamard matrix.
2.2.6. Generalized Hadamard matrices

Let $G$ be a finite non-trivial group, and denote by $\mathbb{Z}G$ the group ring of $G$ over the integers $\mathbb{Z}$. If $S \subseteq G$ then $S$ is also shorthand for the element $\sum_{x \in S} x$ of $\mathbb{Z}G$. Now let $n$ be a positive integer divisible by $|G|$. A generalized Hadamard matrix $\text{GH}(n, G)$ of order $n$ over $G$ is an $n \times n$ matrix $H$ with entries in $G$ such that

$$HH^* = nI_n + \frac{n}{|G|} G(J_n - I_n)$$

over the ambient ring $\mathbb{Z}G$, where $H^*$ is the transpose of the matrix obtained by inverting all entries of $H$. (Note that inversion on $G$ extended $\mathbb{Z}$-linearly is the ambient ring involution for this PCD($\Lambda$).)

2.2.2 Example. Let $p$ be a prime and denote the $k$-dimensional vector space over $\text{GF}(p^m)$ by $V_k$. Then

$$D_{(p,m,k)} = [xy^T]_{x,y \in V_k}$$

is a $\text{GH}(p^mk, C^m_p)$, written additively.

In Chapter 3, we explore the family of generalized Hadamard matrices of Example 2.2.2 in depth.

2.2.7. Butson Hadamard matrices

Let $\zeta_k$ be a primitive $k$th root of unity. A Butson Hadamard matrix $\text{BH}(n, k)$ of order $n$ and phase $k$ is an $n \times n$ matrix $H$ with entries in $\langle \zeta_k \rangle$ such that $HH^* = nI_n$ over $\mathbb{C}$. Here $*$ denotes the Hermitian, i.e., complex conjugate, transpose (complex conjugation being the ring involution here). Butson matrices are also referred to as complex generalized Hadamard matrices. When $k = 4$, i.e., when the entries are in $\{\pm 1, \pm i\}$, $H$ is a complex Hadamard matrix.

2.2.3 Example. The matrix $M$ of Example 2.2.1 is a $\text{BH}(3, 3)$.

The transpose of a $\text{BH}(n, k)$ is also a $\text{BH}(n, k)$. The transpose of a $\text{GH}(n, K)$ is not necessarily a $\text{GH}(n, K)$, except when $K$ is abelian. However, if $H$ is a Butson or generalized Hadamard matrix then $H^*$ is too.
2. Preliminaries

For proofs of the next two results, see Theorem 2.8.4 and Lemma 2.8.5 in [21].

2.2.4 Theorem. If there exists a BH\((n,k)\), and \(p_1, \ldots, p_r\) are the primes dividing \(k\), then \(n = a_1 p_1 + \cdots + a_r p_r\) for some \(a_1, \ldots, a_r \in \mathbb{N}\).

Let \(p\) be a prime for the remainder of this section. By Theorem 2.2.4, a BH\((n,p)\) can exist only if \(p|n\).

2.2.5 Lemma. \(\sum_{i=0}^{n} a_i \zeta^i_p = 0\) for \(n < p\) and \(a_0, \ldots, a_n \in \mathbb{N}\) not all zero if and only if \(n = p - 1\) and \(a_0 = \cdots = a_n\).

Let \(C = \langle x \rangle \cong C_k\) and define \(\eta_k : \mathbb{Z}C \to \mathbb{Z}[\zeta_k]\) by \(\eta_k(\sum_{i=0}^{k-1} c_i x^i) = \sum_{i=0}^{k-1} c_i \zeta^i_k\). Clearly \(\eta_k\) extends to a ring epimorphism \(\text{Mat}(n, \mathbb{Z}C) \to \text{Mat}(n, \mathbb{Z}[\zeta_k])\).

2.2.6 Lemma. (i) If \(M\) is a GH\((n,C_k)\) then \(\eta_k(M)\) is a BH\((n,k)\).

(ii) If \(M\) is a BH\((n,p)\) then \(\eta_p^{-1}(M)\) is a GH\((n,C_p)\).

Proof. Part (i) is easy, and part (ii) uses Lemma 2.2.5 \(\blacklozenge\)

Thus, for all intents and purposes a BH\((n,p)\) is exactly the same design as a GH\((n,C_p)\). In his paper [12], Butson shows how to construct BH\((2^a p^b, p)\) for \(0 \leq a \leq b\). We study cocyclic Butson Hadamard matrices in detail in Chapter 7.

2.3. Automorphism groups

Let \(M \in \text{Mat}(n, \mathcal{R})\). The permutation automorphism group of \(M\) is

\[\text{PAut}(M) = \{(P, Q) \mid P, Q \in \text{Perm}(n) \text{ and } PMQ^\top = M\}\].

That is, \(\text{PAut}(M)\) is the stabilizer of \(M\) under the action of \(\text{Perm}(n) \times \text{Perm}(n)\) on \(\text{Mat}(n, \mathcal{R})\) defined by \((P, Q)X = PXQ^\top\). The corresponding orbit of \(M\) is its permutation equivalence class.

Now let \(M\) be a PCD\((\Lambda)\), where \(\Lambda\) is an orthogonality set of \(2 \times n\) arrays. Further, let \(\mathcal{R}\) be an ambient ring for \(\Lambda\) with involution \(*\), row group \(R \cong \Pi^\text{row}_\Lambda\) and column group \(C \cong \Pi^\text{col}_\Lambda\) as before. The (full) automorphism group of \(M\) is

\[\text{Aut}(M) = \{(P, Q) \mid P \in \text{Mon}(n, R), Q \in \text{Mon}(n, C), \text{ and } PMQ^* = M\}\].
Here $Q^*$ is obtained by transposing $Q$ and applying $*$ entrywise. The direct product $\text{Mon}(n, R) \times \text{Mon}(n, C)$ acts on the set of all PCD($\Lambda$)s via $(P, Q)M = PMQ^*$. The stabilizer of $M$ under this action is $\text{Aut}(M)$; the orbits are the $\Lambda$-equivalence classes of PCD($\Lambda$)s. Clearly $\text{PAut}(M) \leq \text{Aut}(M)$.

Let $\rho_1$ be the projection homomorphism of $\text{Aut}(M)$ onto first components, and $\rho_2$ be the projection homomorphism onto second components. That is, $\rho_1 : (P, Q) \mapsto P$ and $\rho_2 : (P, Q) \mapsto Q$. Sometimes the $\rho_i$ are isomorphisms of $S \leq \text{Aut}(M)$ onto groups of monomial or permutation matrices. For example, this will occur if $M$ is invertible (over $\mathbb{R}$).

2.3.1. Automorphism groups of expanded designs

Let $D, E$ be PCD($\Lambda$)s, where $\Lambda$ is an orthogonality set of order $n$. We have $\text{PAut}(D) \leq \text{Aut}(D)$. Also, if $D \sim E$ then $\text{PAut}(D) \cong \text{PAut}(E)$; indeed, these two groups are conjugate in $\text{Perm}(n)^2$. Similarly $\text{Aut}(D) \cong \text{Aut}(E)$ if $D \cong_\Lambda E$. However if $D \cong_\Lambda E$ then it is not necessarily true that $\text{PAut}(D) \cong \text{PAut}(E)$. This subtlety has led to some confusion in the literature.

2.3.1 Example. Kantor’s ‘symplectic design’ $K_{2m}$ (see [52]) is the following (regular) Hadamard matrix.

$$K_{2m} = \otimes^m \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}.$$ $K_2$ and the Sylvester matrix $H_2$ are certainly Hadamard equivalent, as there is only one equivalence class of Hadamard matrices of order 4. However $\text{PAut}(H_2) \not\cong \text{PAut}(K_2)$; for a justification, see Example 2.4.2 below.

In the following $H$ is a GH($n, G$). Then $H$ has ambient ring $\mathbb{Z}G$, $R = C = G$, and the ring involution is inversion in $G$ extended to $\mathbb{Z}G$. Furthermore $H$ has expanded design $\mathcal{E}_H = [aHb]_{a,b \in G}$. The following is a special case of [21, Theorem 9.6.12].

2.3.2 Theorem. $\text{Aut}(H) \cong \text{PAut}(\mathcal{E}_H)$.

The isomorphism of Theorem 2.3.2 is described in detail in [21, Section 9.6]. For any $X \in \text{Mon}(n, G)$ there are unique disjoint $(0, 1)$-matrices $X_g$ such that
2. Preliminaries

\[ X = \sum_{g \in G} gX. \]

Let

\[ S_g = [\delta^a_{gb}]_{a,b \in G} \quad \text{and} \quad T_g = [\delta^a_{gb}]_{a,b \in G}. \]  

(2.3.1)

Let \( \theta^{(1)}(X) = \sum_{g \in G} T_g \otimes X_g \) and \( \theta^{(2)}(X) = \sum_{g \in G} S_g \otimes X_g. \) Then \( \Theta : \text{Aut}(H) \rightarrow \text{PAut}(E_H) \) defined by \( \Theta : (X,Y) \mapsto (\theta^{(1)}(X), \theta^{(2)}(Y)) \) is an isomorphism as in Theorem 2.3.2.

2.3.3 Example. Let \( H \) be a Hadamard matrix, and let \( (X,Y) \in \text{Aut}(H) \). Then

\[ \Theta((X,Y)) = \left( \begin{bmatrix} X_1 & X_{-1} \\ X_{-1} & X_1 \end{bmatrix}, \begin{bmatrix} Y_1 & Y_{-1} \\ Y_{-1} & Y_1 \end{bmatrix} \right). \]

Recall the associated design from section 2.2.3.

2.3.4 Lemma. If \( H \) is a GH\((n,G)\) then \( \text{PAut}(E_H) \leq \text{PAut}(A_H) = \text{Aut}(A_H) \).

Proof. Since \( \text{PAut}(E_H) \) does not move the identity entries of \( E_H \), it also leaves \( A_H \) invariant.

2.3.5 Remark. Equality in Lemma 2.3.4 holds when \( H \) is a Hadamard matrix.

2.4. Regular subgroups and group development

Let \( M \in \text{Mat}(n, \mathbb{R}) \). We call a subgroup \( S \) of \( \text{PAut}(M) \) regular if the induced actions of \( \rho_1(S) \) and \( \rho_2(S) \) on the sets of row indices and column indices of \( M \) are both regular. We say that \( M \) is group-developed over a group \( G \) if \( M \) is permutation equivalent to \( [\phi(gh)]_{g,h \in G} \) for some function \( \phi : G \mapsto \mathbb{R} \) and indexing of \( M \) by \( G \) by \( G \).

2.4.1 Theorem. \( M \) is group-developed over a group \( G \) of order \( n \) if and only if there exists a regular subgroup of \( \text{PAut}(M) \) isomorphic to \( G \).

Proof. This is well-known; see, e.g., [21, Theorem 10.3.8].

In particular, a group-developed matrix must be regular, and a normalized matrix of size greater than 1 is not group-developed (although it may certainly be \( \Lambda \)-equivalent to a group-developed design).

2.4.2 Example. Recall Example 2.3.1 because \( K_2 \) is circulant, it is group-developed over the cyclic group \( C_4 \). However \( H_2 \) is normalized and thus is not group-developed. In this instance \( \text{PAut}(K_2) \cong \text{Sym}(4) \) whereas \( \text{PAut}(H_2) \cong \text{Sym}(3) \).
2.5. Cocyclic development

Let $G$ be a group and $U$ be an abelian group. A function $\psi: G \times G \to U$ such that

$$\psi(g, h)\psi(gh, k) = \psi(g, hk)\psi(h, k) \quad \forall g, h, k \in G$$  \hspace{1cm} (2.5.1)

is a (2)-cocycle. The cocycle $\psi$ is normalized if $\psi(g, 1) = \psi(1, g) = 1$ for all $g \in G$.

For sets $X$, $Y$, $\text{Fun}(X, Y)$ denotes the set of all maps $X \to Y$; if $X$, $Y$ are groups and $Y$ is abelian then $\text{Fun}(X, Y)$ is an abelian group under pointwise product. The set $Z^2(G, U)$ of all cocycles $\psi: G \times G \to U$ becomes a group under this product. The cocycle $\partial \phi$ defined by $\partial \phi(g, h) = \phi(g)^{-1}\phi(h)^{-1}\phi(gh)$ for some $\phi \in \text{Fun}(G, U)$ is called a coboundary. The set $B^2(G, U)$ of all coboundaries forms a subgroup of $Z^2(G, U)$. We have $B^2(G, U) \cong \text{Fun}(G, U)/\text{Hom}(G, U)$. Define $H^2(G, U) = Z^2(G, U)/B^2(G, U)$, the second cohomology group of $G$ (with trivial coefficients in $U$). The elements of $H^2(G, U)$ are cohomology classes $[\psi]$; two cocycles in the same class are cohomologous. Note that any cocycle is cohomologous to a normalized one (in many situations this means that we can assume that our cocycles are all normalized).

Let $E$ and $G$ be groups and let $U$ be an abelian subgroup of $E$. Then $E$ is a central extension of $U$ by $G$ if $U \leq Z(E)$ and $E/U \cong G$. More weakly, $E$ is a central extension of $U$ by $G$ if $E$ has a subgroup $U' \cong U$ in its center and $E/U' \cong G$.

Let $\psi: G \times G \to U$ be a cocycle. We define the canonical central extension $E_\psi$ of $U$ by $G$ as the group with elements $(x, a)$, $x \in G$, $a \in U$, and multiplication given by $(x, a)(y, b) = (xy, \psi(x, y)ab)$. If $\psi \in B^2(G, U)$ then $E_\psi \cong G \times U$. More generally, if $\psi'$ is cohomologous to $\psi$ then $E_{\psi'}$ is equivalent to $E_\psi$: there is an isomorphism $f: E_\psi \to E_{\psi'}$ such that $f((1, u)) = (1, u)$ and $f((x, u))$ has first component $x$ for all $u \in U$ and $x \in G$. Conversely, any central extension of $U$ by $G$ gives rise to a cocycle $G \times G \to U$. This yields an induced one-to-one correspondence between $H^2(G, U)$ and equivalence classes of central extensions of $U$ by $G$.

The Universal Coefficients Theorem, as follows, provides the foundation of an algorithm to compute representatives of the elements of $H^2(G, U)$ [21], p. 250. Let $H_2(G)$ denote the second homology group (Schur multiplier) of $G$. If $A$ is
2. Preliminaries

abelian then \( \text{Ext}(A, U) \leq H^2(A, U) \) consists of all \([\psi]\) such that \(E_\psi\) is abelian.

2.5.1 Theorem. For finite \( G \) and \( U \),

\[
H^2(G, U) \cong \text{Ext}(G/[G, G], U) \oplus \text{Hom}(H_2(G), U)
\]

Let \( M \) be a PCD(\( \Lambda \)), where \( \Lambda \) is an orthogonality set with alphabet \( \mathcal{A} \) that is a finite abelian group \( U \). We say \( M \) is cocyclic, with cocycle \( \psi : G \times G \to U \), if

\[
M \cong_\Lambda [\psi(g, h)\phi(gh)]_{g, h \in G}
\]

for some function \( \phi \). (Thus group development of PCD(\( \Lambda \))s is a special case of cocyclic development.) We call \( G \) an indexing group of the cocyclic design \( M \), and \( E_\psi \) (or any isomorphic copy) an extension group of \( M \). For the rest of the thesis we drop the superscript ‘2’ on \( Z^2(G, U) \), \( B^2(G, U) \), and \( H^2(G, U) \).

We can define cocyclic development of other kinds of arrays (and call them ‘cocyclic’ too), but PCD(\( \Lambda \))s as always are our main concern. Indeed, it suffices to restrict attention to generalized Hadamard matrices for this thesis. Let \( H \) be a GH(\( n, U \)), and define

\[
\Theta_U = \{(T_u \otimes I_n, S_u \otimes I_n) \mid u \in U\} \leq \text{Perm}(n|U|)^2
\]

where \( S_u, T_u \) are as in \[2.3.1\]. A regular subgroup of \( \text{PAut}(E_H) \) whose center contains \( \Theta_U \) is centrally regular. For any cocycle \( \psi : G \times G \to U \), an injective homomorphism \( \alpha : E_\psi \to \text{PAut}(E_H) \) is a centrally regular embedding if \( \alpha(E_\psi) \) is regular, and \( \alpha((1, u)) = (T_u \otimes I_n, S_u \otimes I_n) \) for all \( u \in U \).

2.5.2 Theorem. A generalized Hadamard matrix \( H \) is cocyclic with cocycle \( \psi \) if and only if there exists a centrally regular embedding of \( E_\psi \) into \( \text{PAut}(E_H) \).

Proof. See [21, Theorem 14.6.4]. ♦

2.6. The translation group

Let \( \mathbb{F} = \text{GF}(p^m) \) for a prime \( p \). We denote the \( k \)-dimensional \( \mathbb{F} \)-vector space by \( V_k \). For \( v \in V_k \) define \( \pi_v : V_k \to V_k \) by \( \pi_v : x \mapsto x + v \). The subgroup \( \{ \pi_v \mid v \in V_k\} \) of \( \text{Sym}(V_k) \) is denoted \( \Sigma_k \), and called the translation group (of \( V_k \)).
2.6.1 Lemma. \( \Sigma_k \) is an additive abelian group; moreover it is isomorphic to the elementary abelian group \( C_{p^m}^{mk} \).

Proof. It is easy to see that \( \pi_v(V_k) \) permutes the vectors in \( V_k \). Also \( \pi_u \pi_v(x) = x + u + v = \pi_{u+v}(x) \) for all \( u, v \in V_k \). Thus \( \Sigma_k \leq \text{Sym}(k) \). The map \( f : V_k \rightarrow \Sigma_k \) defined by \( f(v) = \pi_v \) is an isomorphism, and \( V_k = F \oplus \cdots \oplus F \) is elementary abelian \( p \)-group of rank \( mk \).

The affine general linear group \( AGL(k, F) \) figures prominently in Chapter 3. This is the permutation group \( \text{GL}(k, F) \rtimes \Sigma_k \) on \( V_k \), where \( \text{GL}(k, F) \) acts on \( V_k \) by ordinary matrix multiplication.

For a \( p^{mk} \times p^{mk} \) array \( X \), we say that \( \Sigma_k \) embeds naturally into \( \text{PAut}(X) \) if \( (P_{\pi_v}, P_{\pi_{-v}}) \in \text{PAut}(X) \) for all \( v \in V_k \), where \( P_\phi = [\delta^{x}_{\phi(y)}]_{x,y \in V_k} \in \text{Perm}(p^{mk}) \) in our usual notation.

2.6.2 Lemma. \( \Sigma_k \) embeds naturally in \( \text{PAut}(X) \) if and only if \( X \) is group-developed over \( C_{p^m}^{mk} \).

Proof. Suppose that \( X \) is \( C_{p^m}^{mk} \)-developed: \( X = [h(x + y)]_{x,y \in V_k} \) for some set map \( h \) and indexing of \( X \) by \( V_k \). Let \( P = P_{\pi_v} = [\delta^{x}_{\pi_v(y)}]_{x,y \in V_k} \). Then

\[
PXP = [\delta^{x}_{\pi_v(u)}]_{x,u}[h(u + w)]_{u,w}[\delta^{w}_{\pi_v(y)}]_{w,y} = \sum_{u,w} \delta^{x}_{\pi_v(u)} h(u + w) \delta^{w}_{\pi_v(y)}
\]

\[
= [h((x - v) + (y + v))]_{x,y}
\]

\[
= X.
\]

Thus \( \alpha : \Sigma_k \rightarrow \text{PAut}(X) \) defined by \( \pi_v \mapsto (P_{\pi_v}, P_{\pi_v}^T) \) is a natural embedding (note that \( P_{\pi_u}P_{\pi_v} = P_{\pi_{u+v}} = P_{\pi_v}P_{\pi_u} \)).

Next suppose that \( \alpha \) is a natural embedding of \( \Sigma_k \) into \( \text{PAut}(X) \). Denote the entry in row \( x \), column \( y \) of \( X \) by \( f(x, y) \). Then \( \alpha(\pi_v) \) acts on \( X \) to produce \([f(x - v, y + v)]_{x,y}; \) so \( f(x, y) = f(x - v, y + v) \) for all \( v \). In particular, \( f(x, y) = f(0, x + y) \). Hence, if we define the map \( h \) from \( V_k \) to the set of entries of \( X \) by \( h(a) = f(0, a) \), then \( X = [h(x + y)]_{x,y} \).

Lemma 2.6.2 is really just an illustration of the general fact that an array is group-developed over a group \( G \) if and only if \( G \) acts regularly on the array.
2. Preliminaries

2.7. Difference sets and relative difference sets

Let $G$ be a group of order $v$. A $k$-subset $D$ of $G$ is said to be a $(v, k, \lambda)$-difference set in $G$ if each non-identity element of $G$ occurs exactly $\lambda$ times as a ‘difference’ $de^{-1}$ for distinct elements $d$ and $e$ of $D$.

Let $E$ be a group of order $vm$ with a normal subgroup $N$ of order $m$. Suppose that $R$ is a $k$-subset of $E$, such that the multiset of quotients $r_1r_i^{-1}$, $r_i \in R$, $r_1 \neq r_2$, contains each element of $E \setminus N$ exactly $\lambda$ times, and contains no element of $N$. Then $R$ is called a $(v, m, k, \lambda)$-relative difference set in $E$ with forbidden subgroup $N$. Note that a $(v, k, \lambda)$-difference set in $E$ is the same thing as a $(v, 1, k, \lambda)$-relative difference set in $E$. If $N$ is a central subgroup of $E$ then we call $R$ a central relative difference set.

For certain parameters, the existence of difference sets and central relative difference sets is equivalent to the existence of group-developed and cocyclic PCD($\Lambda$)s; see [22] and [21, Chapters 10, 15]. Here is a sample result along these lines.

2.7.1 Theorem.  
(i) Let $G$ be a group of order $4t^2$. Then there is a group-developed Hadamard matrix over $G$ if and only if there is a $(4t^2, 2t^2 - t, t^2 - t)$-difference set in $G$.

(ii) There is a cocyclic Hadamard matrix over a group $G$ of order $4t$ if and only if there is a $(4t, 2, 4t, 2t)$-central relative difference set in an extension $E$ of $(−1)$ by $G$.

Of course, part (i) of the theorem is a specialization of part (ii), where the forbidden subgroup is trivial. The group $E$ in part (ii) is an extension group of the cocyclic Hadamard matrix, also called a Hadamard group [19].

Results akin to Theorem 2.7.1 hold for other PCD($\Lambda$)s. The passage between difference set and cocyclic design, as in Theorem 2.7.1 is constructive. Thus, classifying cocyclic PCD($\Lambda$)s amounts to listing relative difference sets.
Part I.

Cocyclic development of generalized Sylvester Hadamard matrices
3. The generalized Sylvester matrix

This chapter is in the spirit of previous work by de Launey and Stafford [23, 24, 25]. They determined the automorphism groups of the Paley conference matrix and Hadamard matrices, and classified the centrally regular subgroups in all cases. We attempt to achieve a similar classification for the generalized Sylvester matrices.

Our major new contributions are in Sections 3.2 and 3.3. There we describe the automorphism groups of the generalized Sylvester matrix, and prove existence of some infinite families of indexing groups. A bound on the exponent of indexing groups is given. We then prove the main theorem of the chapter, identifying the indexing groups as regular subgroups of an affine general linear group (this addresses [21, Research Problem 9] as a special case). We conclude with some remarks relating to the converse of the main theorem.

Throughout this chapter, $p$ is a prime, and $m, k$ are positive integers.

3.1. Introduction to the generalized Sylvester matrix

Let $V_k$ be the $k$-dimensional (row) vector space over $\mathbb{F} = \text{GF}(p^m)$. The $p^{mk} \times p^{mk}$ matrix

$$D_{(p,m,k)} = [xy^\top]_{x,y \in V_k} = \otimes^k [xy]_{x,y \in V_1}$$

is a $\text{GH}(p^{mk}, C_p^m)$ with entries in the additive group $V_1$ of $\mathbb{F}$, the Kronecker multiplication being carried out over $\mathbb{Z}[V_1]$. We call $D_{(p,m,k)}$ a generalized Sylvester matrix or Drake matrix (see [29, Propositions 1.5, 1.6]).

For the real Sylvester Hadamard matrices we take $p = 2$ and $m = 1$, and then $D_{(2,1,k)} = \frac{1}{2}(J - H_k)$ where $J$ is the $2^k \times 2^k$ all 1s matrix. Multiplicatively,

$$H_k = [(-1)^{xy^\top}]_{x,y \in V_k}.$$ 

The automorphism group of the Drake matrix is known; see [21, pp. 101–103].
3. The generalized Sylvester matrix

Unless \( k = m = 1 \) and \( p = 2 \),

\[
    \text{Aut}(D_{(p,m,k)}) \cong (Z \times C_p^m) \rtimes \text{AGL}(k, \mathbb{F}) \tag{3.1.1}
\]

where the center \( Z \cong C_p^m \) consists of scalar matrices (diagonal matrices with the same element in each diagonal entry). The affine group \( \text{AGL}(k, \mathbb{F}) \) acts in the expected way on column indices. That is, each pair \( A \in \text{GL}(k, \mathbb{F}), a \in V_k \) sends \( x \in V_k \) to \( xA + a \). Also \( \text{AGL}(k, \mathbb{F}) \) fixes the row of \( D_{(p,m,k)} \) labeled by the zero vector. Let \( \Sigma_k \) be the translation subgroup \( \{ \pi_v \mid v \in V_k \} \) of \( \text{AGL}(k, \mathbb{F}) \), where \( \pi_v \in \text{Sym}(V_k) \) for \( v \in V_k \) is defined by \( \pi_v : x \mapsto x + v \). Then the middle factor \( C_p^m \) in (3.1.1) acts as \( \Sigma_k \) on row indices. (Given an automorphism \((P,Q)\) of \( D_{(p,m,k)} \), saying what \( P \) does to rows determines what \( Q \) does to columns, and vice versa, because \( D_{(p,m,k)} \) is invertible.)

3.1.1. Cocyclic development of \( D_{(p,m,k)} \)

We wish to determine the indexing groups of \( D_{(p,m,k)} \). Composition results for cocyclic PCDs such as [21, Theorem 15.8.4] enable us to find infinite families of indexing groups when \( k \) is large, using known indexing groups for small values of \( k \). The following is a simple example along these lines, for real Sylvester matrices.

3.1.1 Lemma. Suppose that \( G \) is an indexing group for the cocyclic Hadamard matrix \( H_n \). Then \( H_{n+i} \) is cocyclic over \( G \times C_i^2 \) for all \( i \geq 0 \).

Let \( U = V_1 \cong C_p^m \). Recall the isomorphism \( \Theta \) defined after Theorem 2.3.2 and the group \( \Theta_U \) defined by (2.5.2). By Theorem 2.5.2, \( G \) is an indexing group of \( D_{(p,m,k)} \) if for some \( \psi \in Z^2(G, U) \) there is a centrally regular embedding \( E_\psi \hookrightarrow \text{PAut}(E_{D_{(p,m,k)}}) \).

3.2. Automorphism group actions

To prepare for the next section, in this section we explain in more detail how the automorphisms of a generalized Sylvester matrix act.

We first show that \( \text{PAut}(D_{(p,m,k)}) \cong \text{GL}(k, \mathbb{F}) \).

3.2.1 Lemma. Let \((P,Q) \in \text{PAut}(D_{(p,m,k)}) \), where

\[
    P = [\delta_y^{\pi(x)}]_{x,y \in V_k} \quad \text{and} \quad Q = [\delta_y^{\phi(x)}]_{x,y \in V_k}
\]
for some $\pi, \phi \in \text{Sym}(V_k)$. Then there is $A \in \text{GL}(k, \mathbb{F})$ such that

$$\pi(x) = xA \quad \text{and} \quad \phi(x) = x(A^{-1})^\top \quad \forall x \in V_k.$$  

**Proof.** First,

$$[xy^\top]_{x,y \in V_k} = PD_{(p,m,k)}Q^\top = [\delta_t^{\pi(x)}]_{x,t} [ks^\top]_{t,s} [\delta_y^{\phi(y)}]_{s,y}$$

$$= \sum_t \delta_t^{\pi(x)} [ts^\top]_{x,s} [\delta_y^{\phi(y)}]_{s,y}$$

$$= \sum_s \pi(x)s^\top [\delta_y^{\phi(y)}]_{x,y}$$

$$= [\pi(x)\phi(y)]_{x,y},$$

and so $\pi(x)\phi(y)^\top = xy^\top$. For any $a, b \in \mathbb{F}$ and $t \in V_k$ it then follows that

$$\pi(ax + bt)\phi(y)^\top = a\pi(x)\phi(y)^\top + b\pi(t)\phi(y)^\top.$$}

As this holds universally, we must have $\pi(ax + bt) = a\pi(x) + b\pi(t)$; i.e., $\pi$ is $\mathbb{F}$-linear on $V_k$. In similar fashion, so too is $\phi$. Hence there are $A, B \in \text{GL}(k, \mathbb{F})$ such that $\pi(x) = xA$ and $\phi(x) = xB$. Then $xy^\top = xAB^\top y^\top$ for all $x, y$ implies that $AB^\top$ is the identity matrix. ♦

### 3.2.2 Theorem.** PAut(D(p,m,k)) $\cong$ GL(k, F).

**Proof.** Retaining the notation of Lemma [3.2.1] define a map $f : \text{PAut}(D_{(p,m,k)}) \to \text{GL}(k, \mathbb{F})$ by $f : (P, Q) \mapsto A$. Let $(R, S) \in \text{PAut}(D_{(p,m,k)})$, say $R = [\delta_y^{\mu(x)}]_{x,y \in V_k}$ and $f((R, S)) = B$. Now $PR = [\delta_y^{\mu(x)}]_{x,y \in V_k}$ and $\mu\pi(x) = xAB$. Thus $f$ is a homomorphism:

$$f((P, Q)(R, S)) = f((P, QS)) = AB = f((P, Q))f((R, S)).$$

If $A = B$ then $\pi = \mu$, so $P = R$; and then $Q = S$ by Lemma [3.2.1]. Finally, we see that $f$ is surjective. For if $C \in \text{GL}(k, \mathbb{F})$ then $\eta : x \mapsto xC$ and $\nu : x \mapsto x(C^{-1})^\top$ are permutations of $V_k$, and

$$([\delta_y^{\mu(x)}]_{x,y \in V_k}, [\delta_y^{\nu(x)}]_{x,y \in V_k})$$

25
3. The generalized Sylvester matrix

is an automorphism of $D_{(p,m,k)}$. ♦

Let $M$ be a $p^{mk} \times p^{mk}$ matrix indexed by $V_k$ and let $\rho_1$ and $\rho_2$ be the projection homomorphisms of $\text{Aut}(M)$ onto first and second components respectively. Recall that $\Sigma_k$ embeds naturally in $\text{PAut}(M)$ if $(P_{\pi v}, P_{\pi -v}) \in \text{PAut}(M)$ for all $v \in V_k$, where $P_{\phi} = [\delta_{\phi(y)}]_{x,y \in V_k} \in \text{Perm}(p^{mk})$ in our usual notation. More generally, we say that $\Sigma_k$ acts naturally on the rows of $M$ if $\Sigma_k \leq \rho_1(\text{Aut}(M))$; the definition of natural action by $\Sigma_k$ on columns replaces $\rho_1$ by $\rho_2$.

3.2.3 Lemma. $\Sigma_k$ does not embed naturally in $\text{PAut}(D_{(p,m,k)})$.

Proof. Apply Lemma 2.6.2 since $D_{(p,m,k)}$ is normalized, it cannot be group-developed. ♦

3.2.4 Remark. $\Sigma_{2k}$ embeds naturally in $\text{PAut}(K_{2k})$ where $K_{2k}$ is Kantor’s design (see Example 2.3.1).

Of course, as an abstract group, $\Sigma_k$ may embed in $\text{PAut}(D_{(p,m,k)})$ non-naturally. The next lemma pinpoints when this occurs.

3.2.5 Lemma. $\text{PAut}(D_{(p,m,k)})$ has a subgroup isomorphic to $C_p^{mk}$ if and only if $k \geq 4$.

Proof. We use Theorem 3.2.2. For $i \neq j$ and $1 \leq i, j \leq n$, let $t_{ij}(a) \in \text{GL}(k, \mathbb{F})$ be the matrix (transvection) with a main diagonal of 1s, $a$ in position $(i,j)$, and zeros elsewhere. If $i \neq l$ and $j \neq k$ then $t_{ij}(a)$ commutes with $t_{kl}(b)$. Let \{1, $\alpha$, ..., $\alpha^{m-1}$\} be a GF($p$)-basis of $\mathbb{F}$.

Suppose that $k \geq 4$. Then the set

$$\{t_{1j}(1), t_{2j}(1), t_{1j}(\alpha), t_{2j}(\alpha), \ldots, t_{1j}(\alpha^{m-1}), t_{2j}(\alpha^{m-1}) \mid 3 \leq j \leq k\}$$

generates an elementary abelian $p$-group of rank $(2k-4)m$, which for $k \geq 4$ certainly contains a subgroup of rank $mk$.

If $1 \leq k \leq 2$ then $C_p^{mk}$ is larger than any $p$-subgroup of $\text{GL}(k, \mathbb{F})$; whereas a Sylow $p$-subgroup of $\text{GL}(3, \mathbb{F})$ has order $p^{3m}$, but is non-abelian. This completes the proof. ♦

3.2.6 Remark. We already knew that $\text{Aut}(D_{(2,1,2k)})$ has a subgroup isomorphic to $C_2^{2k}$, because $D_{(2,1,2k)}$ is Hadamard equivalent to $K_{2k}$. 26
Although PAut($D_{(p,m,k)}$) does not contain regular subgroups, $\Sigma_k$ has separate induced regular actions on the rows and (by duality) on the columns of $D_{(p,m,k)}$.

3.2.7 Lemma. There are diagonal matrices $B_v$ such that $\{(P_{\pi_v}, B_v) \mid v \in V_k\} \leq \text{Aut}(D_{(p,m,k)})$. Also, $\Sigma_k$ is isomorphic to a subgroup of $\text{Aut}(D_{(p,m,k)})$ acting regularly on the rows (resp., columns) of $D_{(p,m,k)}$, but not moving any column (resp., row).

Proof. Take $B_v$ to be the $V_k$-indexed diagonal matrix with $-v \cdot y$ in position $y$ on its main diagonal. Then 

$$P_{\pi_v}D_{(p,m,k)}B_v^* = \left[ \delta_{\pi_v(t)}^x \cdot t \cdot y \right]_{t,y}B_v^*$$

$$= \sum_t \delta_{\pi_v(t)}^x \cdot t \cdot y \cdot B_v^*$$

$$= \left[ (x-v) \cdot y \right]_{x,y}B_v^*$$

$$= \left[ x \cdot y - v \cdot y + v \cdot y \right]_{x,y} = D_{(p,m,k)},$$

working over $\mathbb{Z}V_1$. Thus $(P_{\pi_v}, B_v)$ is an automorphism of $D_{(p,m,k)}$. All such pairs clearly form a subgroup of $\text{Aut}(D_{(p,m,k)})$. The latter claim follows. ♦

We write the zero vector of $V_k$ as $0$. Usually we let $0$ label the first row, and label the columns in the same order as the rows. Let $M$ be a $p^{mk} \times p^{mk}$ matrix indexed by $V_k$. Let $\Gamma$ be the stabilizer in $\rho_1(\text{PAut}(M))$ of the row of $M$ labeled by $0$. The stabilizer in $\rho_2(\text{PAut}(M))$ of the $0$-column may be the same as $\Gamma$ (if, e.g., $M$ is normalized), or it may be different.

3.2.8 Lemma. Let $M$ be as above, and suppose that $\Sigma_k$ acts naturally on the rows of $M$. If $(P,Q) \in \text{PAut}(M)$ then $P = P_\phi$ where $\phi \in \text{Sym}(V_k)$ is uniquely expressible as $\pi_vg$ for some $\pi_v \in \Sigma_k$ and $g \in \Gamma$.

Proof. We have $\pi_{-\phi(0)} \phi \in \Gamma$, so $\phi \in \Sigma_k \Gamma$. Uniqueness is straightforward. ♦

3.2.9 Remark. Since the choice of row to label with the zero vector can be arbitrary, we could just as well have redefined $\Gamma$ so that $\Gamma$ stabilizes the row labeled $u$ for any vector $u \in V_k$.

3.2.10 Lemma. Assume the hypotheses of Lemma 3.2.8. Then $\Gamma$ acts additively on the rows of $M$ if and only if $\rho_1(\text{PAut}(M)) = \Sigma_k \rtimes \Gamma$. 

27
3. The generalized Sylvester matrix

Proof. By Lemma 3.2.8, $\rho_1(\text{PAut}(M)) = \rho_1(\Sigma_k)^\Gamma$. If $\Gamma$ acts additively, then for all $g \in \Gamma$ and $x \in V_k$,

$$g^{-1}\pi_v g(x) = g^{-1}(g(x) + v) = x + g^{-1}(v) = \pi_{g^{-1}(v)}(x).$$

Thus $\rho_1(\Sigma_k) \trianglelefteq \rho_1(\text{PAut}(M))$, i.e., $\rho_1(\text{PAut}(M)) = \Sigma_k \rtimes \Gamma$.

Next suppose that $\Gamma$ normalizes $\rho_1(\Sigma_k)$. So, given any $g \in \Gamma$ and $v \in V_k$, there is $u$ such that $g\pi_v g^{-1} = \pi_u$. Consequently $u = \pi_u(0) = g\pi_v g^{-1}(0) = g(v)$. Then

$$g(v) + g(x) = \pi_u(g(x)) = g\pi_v g^{-1}(g(x)) = g(v + x)$$

implying that $\Gamma$ acts additively, as required. ♦

The symmetric matrix $\mathcal{E}_{D(p,m,k)}$ possesses a row/column duality. In particular, many statements about induced actions on rows and columns of the expanded design hold after swapping the roles of rows and columns. Also note that the projections $\rho_i$ of $\text{PAut}(\mathcal{E}_{D(p,m,k)})$ onto first and second components are each isomorphisms. This follows from the definition of the map $\Theta$ and the fact that the projections of $\text{Aut}(D(p,m,k))$ onto first and second components are isomorphisms.

Hereafter we write $v \circ x$ for the concatenation of vectors $v$ and $x$.

3.2.11 Proposition. $\text{PAut}(\mathcal{E}_{D(p,m,k)}) = N \rtimes L$ where

(i) $N \cong C_p^{m(k+1)}$ acts in the natural way as $\Sigma_{k+1}$ on the rows of $\mathcal{E}_{D(p,m,k)}$.

(ii) $L \cong \text{AGL}(k, \mathbb{F})$ acts additively and as $\Gamma$ on the rows of $\mathcal{E}_{D(p,m,k)}$.

(iii) $N = N_1 \times N_2$ where $N_1 \cong C_p^m$ fixes column $rp^{mk} + 1$ for $0 \leq r \leq p^m - 1$, and $N_2$ permutes these columns regularly amongst themselves.

(iv) Each set of $p^{mk}$ successive columns of $\mathcal{E}_{D(p,m,k)}$ forms a single orbit under $L$, which acts on each set as $\text{AGL}(k, \mathbb{F})$ in the same way (i.e., $g \in L$ sends column $i$ to column $j$, $1 \leq i, j \leq p^{mk}$, if and only if $g$ sends column $rp^{mk} + i$ to column $rp^{mk} + j$ for all $1 \leq r \leq p^m - 1$).

Proof. Select orderings of $V_k$ and $\mathbb{F}$ (starting at the zero element), which then impose the ordering of $V_{k+1} = \{v \circ x \mid v \in V_k, x \in \mathbb{F}\}$ defined by $v_1 \circ x_1 < v_2 \circ x_2 \iff x_1 < x_2$ or $x_1 = x_2$ and $v_1 < v_2$. Label rows and columns of $\mathcal{E}_{D(p,m,k)}$ by the elements of $V_{k+1}$ under this ordering.
The center $Z$ of $\text{Aut}(D_{(p,m,k)})$ is all scalars in $\text{Mat}(p^{mk}, \mathbb{F})$. Here $\Theta(Z)$ is $\Theta_U$ as in (2.5.2). We see from the definition of $\Theta$ in Section 2.3.1 that $\Theta$ maps $(xI_{p^{mk}}, xI_{p^{mk}})$ to a permutation automorphism of $E_{D_{(p,m,k)}}$ that acts as $P_{\pi_0, \pi_{-x}}$ on rows and $P_{\pi_0, x}$ on columns.

Let $W$ be the group $\{(P_{\pi_v}, B_v) \mid v \in V_k\}$ of Lemma 3.2.7. Since $\theta_1(P_{\pi_v})$ is a block diagonal matrix with $P_{\pi_v}$ down its main diagonal, $\Theta(W)$ acts on rows of the expanded design as translations $P_{\pi_v, 0}$. On the other hand, $\theta_2(B_v)$ fixes columns labeled by vectors $0 \circ x$. Thus we have verified (i) and (iii) for $N = \Theta((W, Z))$.

By the discussion after equation (3.1.1), $\text{Aut}(D_{(p,m,k)})$ splits over $Z \times W$, with a complement that fixes the zero row and acts as $\text{AGL}(k, \mathbb{F})$ on the columns of $D_{(p,m,k)}$. So this complement is mapped by $\Theta$ to $L$ fixing the zero row, and acting on the columns of $E_{D_{(p,m,k)}}$ as indicated. Then Lemma 3.2.10 finishes the proof.

3.2.12 Remark. Note that $L$ does not act transitively on columns; it has $p^m$ column orbits of length $p^{mk}$.

3.3. Indexing groups of $D_{(p,m,k)}$

An indexing group of $D_{(p,m,k)}$ is isomorphic to a subgroup of the central quotient $C_{p^{mk}} \rtimes \text{AGL}(k, \mathbb{F})$ of $\text{Aut}(D_{(p,m,k)})$. In the case $p = 2$ and $m = 1$, ‘O Catháin and Röder [62] classified the cocyclic Hadamard matrices of orders less than 40, giving a complete classification of the indexing groups of $D_{(2,1,k)}$ and their extension groups for $k \leq 4$. In this section we obtain a comparatively more general description of the indexing groups of $D_{(p,m,k)}$ for all $m, k \geq 1$ and primes $p$. Infinite families of indexing groups of $D_{(p,m,k)}$ are easily constructed using Kronecker multiplication and existing classifications at small orders. This might indicate that groups of smaller exponent are more likely to be indexing groups. The next couple of results show that this is indeed the case.

3.3.1 Lemma. If $G$ is a $p$-subgroup of $\text{GL}(k, \mathbb{F})$ then its exponent divides $p^{\lceil\log_p k\rceil}$.

Proof. This is well-known (see, e.g., [68, p. 192]).

3.3.2 Proposition. A $p$-subgroup of $\text{PAut}(E_{D_{(p,m,k)}})$, and thus any extension group of $D_{(p,m,k)}$, have exponent at most $p^{\lceil\log_p (k+1)\rceil+1}$. ♦
3. The generalized Sylvester matrix

Proof. First note that $\text{AGL}(k, \mathbb{F})$ is isomorphic to a subgroup of $\text{GL}(k+1, \mathbb{F})$. Therefore, if $A$ is a $p$-subgroup of $\text{PAut}(E_{D(p,m,k)})$ then $A/(A \cap N) \cong AN/N$ has exponent dividing $p^{\log_p(k+1)}$ by Proposition 3.2.11 and Lemma 3.3.1. Since $N$ is elementary abelian, the assertion is now clear.

3.3.3 Remark. Ito proves that an extension group of a cocyclic Hadamard matrix of order $2^k > 2$ is not cyclic nor dihedral [49 Propotions 6 and 7]. Restricting our attention to the Sylvester matrices, Proposition 3.3.2 improves on this for $k > 4$.

Write $\text{PAut}(E_{D(p,m,k)}) = N_k \rtimes G$ as in Proposition 3.2.11. Let $c_x = 0 \circ x$ for $x \in \mathbb{F}$, and let $C$ be the set of all such $c_x$. For $R \leq \text{Sym}(V_{k+1})$ we define a subgroup $f(R)$ of $\text{PAut}(E_{D(p,m,k)})$ by putting $\rho_1(f(\alpha)) = P_{\alpha} = [\delta_{\alpha(u)}]_{u,v \in V_{k+1}}$. Suppose that $f(R)$ is centrally regular. Thus $R$ acts regularly on $V_{k+1}$ and the center of $R$ contains $\{\pi_{c_x} \mid c_x \in C\}$ where $f(\pi_{c_x}) \in \Theta(Z)$.

3.3.4 Lemma. $R = \{\pi_v g_v \mid v \in V_{k+1}\}$ where $g_v \in \Gamma$. Furthermore, $g_v(c_x) = c_x$ for all $c_x \in C$ and $g_v$ such that $\pi_v g_v \in R$.

Proof. Each element of $R$ is of the form $\pi_v g_v$ where $\pi_v \in \Sigma_{k+1}$ and $g_v \in \Gamma$, by Lemma 3.2.8. Transitivity of $R$ proves the first claim. By the proof of Lemma 3.2.10, $g_v \pi_{c_x} = \pi_{g_v c_x} g_v = \pi_{c_x} g_v$ and thus $g_v(c_x) = c_x$.

3.3.5 Corollary. With reference to Proposition 3.2.11, $R \leq \Sigma_{k+1} \rtimes K$ where $K \leq \Gamma$ stabilizes $c_x$ for all $c_x \in C$.

3.3.6 Corollary. If $\pi_v g_v \in R$ then $\pi_v + c_x g_v \in R$ for all $c_x \in C$.

Let $e_{c_x}$ denote the column of $E_{D(p,m,k)}$ labeled by $c_x$. If $f(R)$ is centrally regular then it must act regularly on the columns of $E_{D(p,m,k)}$. As per Lemma 3.3.4, $R = \{\pi_v g_v \mid v \in V_{k+1}\}$ where $g_{c_x} = 1_R$. Let $\Lambda = \{g_v \mid \pi_v g_v \in R\}$. By Corollary 3.3.6, there are at most $p^{mk}$ distinct elements in $\Lambda$ as $g_v = g_{v+c_x}$ for all $c_x \in C$, i.e., $|\Lambda| \leq p^{mk}$. We have seen that $N_k = \{f(\pi_v) \mid v \in V_{k+1}\}$ acts so that columns $e_{c_x}$ for $c_x \in C$ are all in a single orbit of size $p^m$. Also, $f(g_v)$ for $g_v \in \Lambda$ acts as $\text{AGL}(k, \mathbb{F})$ on sets of $p^{mk}$ columns of $E_{D(p,m,k)}$ as stated in Proposition 3.2.11. Thus in order for $f(R)$ to act regularly on the columns, $\{f(g_v) \mid g_v \in \Lambda\}$ should act transitively on the first $p^{mk}$ columns (and transitively on every subsequent set of $p^{mk}$ columns as a consequence). This implies that for all $v \in V_{k+1} \setminus C$, $g_v \neq 1$, and that $|\Lambda| = p^{mk}$.
3.3.7 Lemma. \( \Lambda \) is a group of order \( p^{mk} \).

Hereafter we write \( V_k \circ x = \{ v \in V_{k+1} \mid v_{k+1} = x \} \), \( x \in \mathbb{F} \).

3.3.8 Lemma. If \( g_v \in \Lambda \setminus \{1\} \) and \( g_v(V_k \circ 0) = V_k \circ 0 \), then \( f(R) \) does not act regularly on the columns of \( E_{D(p,m,k)} \).

Proof. By hypothesis, \( P_{g_v} \) fixes \( e_0 \), and \( P_{\pi_v} \) either fixes \( e_0 \), or sends it to \( e_{c_x} \) for some \( c_x \in C \). Since \( \{ \pi_{c_x} \} \subseteq R \), the orbit of \( e_0 \) is not of length \( p^{mk+1} \), i.e., \( f(R) \) does not act transitively on the columns of \( E_{D(p,m,k)} \).

Let \( \varphi : \Lambda \rightarrow R/\langle \{ \pi_{c_x} \} \rangle \) be such that \( \varphi(g_v) = \pi_v g_v \langle \{ \pi_{c_x} \} \rangle \). Since \( |\Lambda| = p^{mk} \) by Lemma 3.3.7, the map \( \varphi \) is bijective, and it is clearly a homomorphism.

3.3.9 Theorem. \( \Lambda \cong R/\langle \{ \pi_{c_x} \} \rangle \), i.e., \( \Lambda \) is isomorphic to an indexing group of \( D_{(p,m,k)} \).

Let \( b_{x \circ a} \) denote the set of vectors labeling rows of \( E_{D(p,m,k)} \) that have \( 0_F \) in the column labeled \( x \circ a \), where \( x \) runs over \( V_k \) and \( a \) runs over \( \mathbb{F} \). Thus \( b_{0 \circ a} = \{ x \circ (-a) \mid x \in V_k \} \). Now let \( X_a = \{ b_{x \circ a} \mid x \in V_k \} \).

3.3.10 Lemma. If \( f(R) \) is regular on the columns of \( E_{D(p,m,k)} \) then \( \Lambda \) is transitive on \( X_0 \).

Proof. For \( x \in V_k \), the blocks \( \{ b_{x \circ a} \mid a \in \mathbb{F} \} \) comprise a single orbit under \( \Sigma_{k+1} \). Also, \( \Lambda \) fixes \( X_0 \) setwise. So if \( \Lambda \) does not act transitively on the elements of \( X_0 \) then \( f(R) \) does not act transitively on the columns of \( E_{D(p,m,k)} \).

We need the following well-known fact about the affine group (over a field \( \mathbb{K} \)).

3.3.11 Theorem. \( AGL(k, \mathbb{K}) \) is isomorphic to a subgroup of \( GL(n, \mathbb{K}) \) if \( n > k \).

Proof. The map

\[
\mu : \pi_v A \rightarrow \begin{bmatrix} A & v^\top \\ 0_{1 \times k} & 1 \end{bmatrix}
\]

is a monomorphism \( \mu : AGL(k, \mathbb{K}) \rightarrow GL(k + 1, \mathbb{K}) \).
3. The generalized Sylvester matrix

Since \( g_v(c_x) = c_x \) for all \( v \in V_{k+1} \) and \( c_x \in C \),

\[
\Lambda \leq \mu(AGL(k, \mathbb{F}))
\]

where \( \mu \) is as defined in the proof of Theorem 3.3.11. That is, \( g_v \) corresponds to an element of \( GL(k+1, \mathbb{F}) \) of the form

\[
\begin{bmatrix}
A & u_g^T \\
0_{1 \times k} & 1
\end{bmatrix}
\]

for some \( u_g \in V_k \).

3.3.12 Lemma. Let \( \Lambda \) be as above and suppose \( f(R) \) is a regular subgroup of \( PAut(E_D(p,m,k)) \), where each \( g_v \) corresponds to \( \begin{bmatrix} A & u_g^T \\ 0_{1 \times k} & 1 \end{bmatrix} \) in \( GL(k+1, \mathbb{F}) \). Then \( \{u_{g_v} \mid g_v \in \Lambda\} = V_k \).

Proof. Suppose that \( g_a = \begin{bmatrix} A & u_{g_a}^T \\ 0_{1 \times k} & 1 \end{bmatrix} \neq \begin{bmatrix} B & u_{g_b}^T \\ 0_{1 \times k} & 1 \end{bmatrix} = g_b \) where \( u_{g_a} = u_{g_b} \).

Then \( g = g_a^{-1}g_b = \begin{bmatrix} A^{-1}B & 0_{k \times 1} \\ 0_{1 \times k} & 1 \end{bmatrix} \in \Lambda \). But \( g \) fixes \( b_{0 \times 0} \) and thus \( \Lambda \) does not act transitively on \( X_0 \). Thus if \( \{x_{g_v} \mid g_v \in \Lambda\} \neq V_k \), then there are distinct \( g_a, g_b \in \Lambda \) such that \( x_{g_a} = x_{g_b} \). Thus by Lemma 3.3.10 \( f(R) \) is not regular on the columns of \( E_{D(p,m,k)} \). ♦

Finally we can prove the main theorem of the chapter.

3.3.13 Theorem. If \( G \) is an indexing group of \( D_{(p,m,k)} \) then \( G \) is isomorphic to a regular subgroup of \( AGL(k, \mathbb{F}) \).

Proof. By Theorem 3.3.9 \( G \cong R/\langle \pi_{c_i} : c_i \in C \rangle \cong \Lambda \leq \mu(AGL(k, \mathbb{F})) \), so \( G \) is isomorphic to a subgroup of \( AGL(k, \mathbb{F}) \). By Lemma 3.3.12 \( \mu^{-1}(\Lambda) = \{\pi_vg'_v \mid \pi_v \in \Sigma_k\} \) where \( g'_v \in GL(k, \mathbb{F}) \), i.e., \( \mu^{-1}(\Lambda) \) is regular. ♦

The converse of Theorem 3.3.13 does not necessarily hold, that is, it is not necessarily true that a regular subgroup of \( AGL(k, \mathbb{F}) \) is isomorphic to an indexing group of \( D_{(p,m,k)} \). We verify this using some experimental data in the next section.

3.3.1. Experimental results

On the whole, classifying regular subgroups of \( AGL(k, \mathbb{F}) \) is a difficult problem. While related classifications have been obtained (e.g., the authors of [58] consider the problem of determining finite primitive permutation groups with a
regular subgroup), computational investigations are limited to small degrees and fields. We discuss subgroups of $\text{AGL}(k, p)$ in the final section of this chapter.

For various $p$, $m$, $k$, we carried out a series of **Magma** computations of the centrally regular subgroups of $\text{PAut}(\mathcal{E}_{D(p,m,k)})$, and thereby found all indexing groups of $D_{(p,m,k)}$. Table 3.3.1 displays the resulting data.

Table 3.3.1. Indexing groups

<table>
<thead>
<tr>
<th>$m$</th>
<th>$p$</th>
<th>$k$</th>
<th>$r$</th>
<th>$r'$</th>
<th>$r''$</th>
<th>$s$</th>
<th>$s'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>113</td>
<td>34</td>
<td>12</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>56</td>
<td>9</td>
<td>4</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>12</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>28</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>502</td>
<td>39</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>23</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

$r$: number of conjugacy classes of the centrally regular subgroups of $\text{PAut}(\mathcal{E}_{D(p,m,k)})$

$r'$: number of isomorphism types of the centrally regular subgroups of $\text{PAut}(\mathcal{E}_{D(p,m,k)})$

$r''$: number of isomorphism types of the indexing groups of $D_{(p,m,k)}$

$s$: number of conjugacy classes of the regular subgroups of $\text{AGL}(k, \mathbb{F})$

$s'$: number of isomorphism types of the regular subgroups of $\text{AGL}(k, \mathbb{F})$

The quaternion group of order 8 provides the sole disparity between the sixth and eighth columns of Table 3.3.1. This is the only example that we have discovered of a regular subgroup of $\text{AGL}(k, \mathbb{F})$ not isomorphic to an indexing group of $D_{(p,m,k)}$.

**3.4. Existing subgroups of $\text{AGL}(k, p)$**

For this final section of the chapter, we let $m = 1$ and write $D_{(p,k)}$ for $D_{(p,1,k)}$.

We present evidence to support our empirical observation (based on Table 3.3.1 above) that most groups of order $p^k$ satisfying the exponent bound in
3. The generalized Sylvester matrix

Proposition 3.3.2 are isomorphic to indexing groups of $D_{(p,k)}$. As products of indexing groups for PCDs are indexing groups for larger PCDs, groups of low exponent are likely to be indexing groups of $D_{(p,k)}$.

Let $S$ be a Sylow $p$-subgroup of $AGL(k,p)$. The exponent of $S$ is $p^{\lceil \log_p(k+1) \rceil} = p^m$. A Sylow $p$-subgroup $W_m$ of $Sym(p^m)$ is the wreath product of $m$ copies of $C_p$ [63, 1.6.19]. If $W_m$ is isomorphic to a subgroup of $AGL(k,p)$ then it is isomorphic to a subgroup of $AGL(k+i,p)$ for all $i \geq 0$. Adhering to Lemma 3.3.1, the exponent of a Sylow $p$-subgroup of $AGL(k,p)$ is $p$ times that of a Sylow $p$-subgroup of $AGL(k-1,p)$ when $k = p^n$ for any $n$; otherwise these Sylow subgroups have the same exponent.

3.4.1 Lemma. Suppose that $W_m$ is isomorphic to a subgroup of $AGL(k,p)$. Then $W_{m+1}$ is isomorphic to a subgroup of $AGL(pk,p)$.

Proof. Denote the elements of the isomorphic copy of $W_m$ in $AGL(k,p)$ by $\pi_{v_i}g_i$, $1 \leq i \leq n$. By definition $W_{m+1} = W_m \wr C_p = W_{m}^p \rtimes C_p$. Let $S_p$ be the set of sequences of length $p$ with entries in $\{1, \ldots, n\}$ and let $g_{e_1} \ldots g_{e_p}$ be the block diagonal matrix with $g_{e_i}$ in the $i$th block, where $e_i \in \{1, \ldots, n\}$.

Let $\pi_{v_1} \ldots \pi_{v_p}$ be the translation of $V_{pk}$ that acts by adding $v_{e_1}$ to the first $k$ entries, $v_{e_2}$ to the next $k$ entries, and so on. Then the subgroup $G = \{\pi_s g_s \mid s \in S_p\}$ of $AGL(pk,p)$ is isomorphic to $W_{k}^p$.

Now let $h$ be any block circulant $kp \times kp$ matrix with $I_p$ in some non-initial block and zeros elsewhere. Then $h(\pi_s g_s) h^{-1} \in G$ for all $s \in S_p$ and thus $G \rtimes C_p \leq AGL(pk,p)$.

3.4.2 Lemma. Let $p^m$ be the exponent of a Sylow $p$-subgroup of $AGL(k,p)$. Then a Sylow $p$-subgroup of $Sym(p^m)$ is isomorphic to a subgroup of $AGL(k,p)$.

Proof. Sylow $p$-subgroups of $AGL(1,p)$ and $Sym(p)$ are isomorphic to $C_p$. The result follows by Lemma 3.4.1 and induction.

3.4.3 Theorem. Every $p$-subgroup of $Sym(p^{\lceil \log_p(k+1) \rceil})$ is isomorphic to a subgroup of $AGL(k,p)$.

Proof. Lemma 3.4.2 ensures that $Sym(p^{\lceil \log_p(k+1) \rceil}) \leq AGL(k,p)$.
4. Automorphisms of Kantor’s design

In this chapter we shift our attention to Kantor’s design $K_{2n}$. As it is Hadamard equivalent to the Sylvester matrix $H_{2n}$, the overall cocyclic development of $K_{2n}$ is identical to that of $H_{2n}$. However, $K_{2n}$ is group-developed, whereas $H_{2n}$ is not. We derive conditions for groups over which $K_{2n}$ is developed, analogous to the results of Chapter 3.

From Kantor’s paper [52] we can see that $\text{PAut}(K_{2n})$ is isomorphic to $\Sigma_{2n} \rtimes \text{Sp}(2n, 2)$. In Section 4.1 we describe the action of $\Sigma_{2n}$ and its symplectic complement on the rows of $K_{2n}$. Then in Section 4.2 we independently verify Kantor’s result; that is, we prove that the complement to $\Sigma_{2n}$ in $\text{PAut}(K_{2n})$ is isomorphic to $\text{Sp}(2n, 2)$. For the remainder of the chapter we discuss some computational results, including a classification of the regular subgroups of $\text{PAut}(K_6)$. The latter extends some work of Ó Catháin and Röder [62].

Throughout this chapter, $V_{2n}$ is the $2n$-dimensional vector space over GF(2), and $\mathbf{0}$ denotes the zero vector of $V_{2n}$.

4.1. Actions of the translation group on $K_{2n}$

We index $K_{2n}$ by the elements of $V_{2n}$, usually labeling the first row $\mathbf{0}$, and labeling columns in the same order as the rows. Despite $H_{2n}$ and $K_{2n}$ being Hadamard equivalent, $\text{PAut}(K_{2n}) \not\cong \text{PAut}(H_{2n})$.

4.1.1 Theorem ([52]). $\text{PAut}(K_{2n}) \cong V_{2n} \rtimes \text{Sp}(2n, 2)$.

Thus $\Sigma_{2n}$ is isomorphic to a normal subgroup of $\text{PAut}(K_{2n})$.

4.1.2 Remark. $\text{PAut}(K_2) \cong \text{Sym}(4)$.

4.1.3 Remark. If square matrices $X$ and $Y$ are group-developed over $G$ and $H$ respectively, then $X \otimes Y$ is group-developed over $G \times H$.
4. Automorphisms of Kantor's design

4.1.4 Lemma. $\Sigma_{2n}$ is isomorphic to a regular subgroup of $\text{PAut}(K_{2n})$.

Proof. $K_{2n}$ is group-developed over $V_{2n} \cong \Sigma_{2n}$.

Let $C = \langle a \mid a^4 = 1 \rangle \cong C_4$, and define $\phi : C \to \{\pm 1\}$ by

$$\phi(1) = \phi(a) = \phi(a^2) = 1 \quad \text{and} \quad \phi(a^3) = -1.$$  

Then $K_2$ is group-developed over $C$ by this $\phi$. Thus by Remark 4.1.3 and Lemma 4.1.4, $K_{2n}$ is group-developed over $C_2^{2n}$ and $C_4^n$ for all $n \geq 1$.

4.1.5 Lemma. For all $i$ such that $0 \leq i \leq n$, $\text{PAut}(K_{2n})$ has a regular subgroup isomorphic $C_i^4 \times C_2^{(n-i)}$. Thus $\text{PAut}(K_{2n})$ has at least $n + 1$ non-isomorphic abelian regular subgroups.

Denote by $\Gamma_{2n}$ the stabilizer in $\rho_1(\text{PAut}(K_{2n}))$ of the row labeled by 0. Recalling Lemma 3.2.10, we have $\text{PAut}(K_{2n}) \cong \Sigma_{2n} \rtimes \Gamma_{2n}$ where $\Gamma_{2n}$ acts linearly on $V_{2n}$.

4.1.6 Lemma. (i) $\Gamma_{2n}$ is transitive on $V_{2n} \setminus \{0\}$, and (ii) $\text{PAut}(K_{2n})$ is 2-transitive on rows.

Proof. This was known to Block [7, Theorem 4] so we just sketch a proof here.

It is easily checked that $\Gamma_2 \cong \text{Sym}(3)$ acts transitively on $V_2 \setminus \{0\}$. Assume a labeling of the rows of $K_{2n}$ with the vectors of $V_{2n}$ in reverse lexicographical order. To see that $\Gamma_4$ is transitive on $V_4 \setminus \{0\}$, let

$$N_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad N_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad N_3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

For each $1 \leq i \leq 3$, the permutation matrix $P_i$ that moves the row labeled by $x$ to the row labeled $xN_i$ preserves the set of columns, i.e., there is $Q_i$ such that $(P_i, Q_i) \in \text{PAut}(K_4)$. Also, the matrix group $G$ generated by the $N_i$ is transitive on $V_4 \setminus \{0\}$, and is conjugate to $\text{Sp}(4,2)$.

For $n > 2$, it is then possible to generate a matrix group that acts transitively on $V_{2n} \setminus \{0\}$ as follows. Let $T$ be a subgroup of $\Gamma_{2n-2}$ that is transitive on
Let \( V_{2n-2} \setminus \{0\} \). Then let

\[
N = \left\{ \begin{bmatrix} t & 0_{2n \times 2} \\ 0_{2 \times 2n} & I_2 \end{bmatrix}, \begin{bmatrix} I_2 & 0_{2n \times 2} \\ 0_{2 \times 2n} & t \end{bmatrix} \mid t \in T \right\}.
\]

The elements of \( N \) correspond to automorphisms of \( K_{2n} \), and the group generated by \( N \) is transitive on \( V_{2n} \setminus \{0\} \). We now get part (i) by induction. Part (ii) is a direct consequence of part (i).

The following is a well-known theorem of Burnside; see, e.g., [27, Theorem 7.2E] or [1, Theorem 5.15].

4.1.7 Theorem (Burnside’s Theorem). A 2-transitive permutation group has a unique non-trivial minimal normal subgroup. If that subgroup is regular then it is elementary abelian; otherwise, it is primitive and non-abelian simple.

For any proper subgroup \( S \) of \( \Sigma_{2n} \), there is \( v \in V_{2n} \) such that \( \pi_v \notin S \). But by transitivity of \( \Gamma_{2n} \), there is \( g \in \Gamma_{2n} \) such that for \( \pi_u \in S \), \( g^{-1}\pi_u(0) = g^{-1}(u) = v \). Thus \( g^{-1}\pi_ug \notin S \). So \( \Sigma_{2n} \) is the unique minimal normal subgroup of \( \text{PAut}(K_{2n}) \).

4.1.8 Corollary. \( \Sigma_{2n} \) is the only normal regular subgroup of \( \text{PAut}(K_{2n}) \).

Proof. Since any regular subgroup must be of order \( 2^{2n} \), this result is a direct consequence of Burnside’s theorem.

The socle of a group is the subgroup generated by its minimal normal subgroups.

4.1.9 Lemma. \( \Sigma_{2n} \) is isomorphic to the socle of \( \text{PAut}(K_{2n}) \).

4.1.1. The symplectic complement

By Theorem 4.1.1 a complement \( \Gamma_{2n} \) of \( \Sigma_{2n} \) in \( \text{PAut}(K_{2n}) \) is isomorphic to \( \text{Sp}(2n,2) \). Let \( B \) be a non-degenerate skew-symmetric bilinear form on \( V_{2n} \). Let \( \tau \in \text{GL}(2n,2) \) preserve \( B \), i.e.,

\[
B(\tau u, \tau v) = B(u, v) \quad \forall \, u, v \in V_{2n}.
\]

The set of all such \( \tau \) forms a subgroup \( \text{Sp}(2n,2) \leq \text{GL}(2n,2) \). Since any two non-degenerate alternating forms \( B_1 \) and \( B_2 \) on \( V_{2n} \) are equivalent [30] Corollary
4. Automorphisms of Kantor’s design

2.12], any symplectic subgroup of GL(2n, 2) isomorphic to Sp(2n, 2) is conjugate to Sp(2n, 2).

The following result may be surprising.

**4.1.10 Lemma.** For \( n \geq 2 \), \( \Gamma_{2n} \cong \text{Sp}(2n, 2) \) does not act transitively on the set of columns of \( K_{2n} \) not labeled by 0.

Proof. \( \Gamma_{2n} \) stabilizes the first row of \( K_{2n} \). Therefore \( \Gamma_{2n} \) can only permute the columns beginning with a \(-1\) (or a 1 respectively) amongst themselves. Thus, for \( n > 1 \), \( \Gamma_{2n} \) is intransitive on columns not labeled by the zero vector. ♦

By Lemma 4.1.10, \( \Gamma_{2n} \) cannot act naturally as \( \text{Sp}(2n, 2) \) on the columns of \( K_{2n} \) for \( n \geq 2 \). However, \( \Gamma_{2n} \) acts linearly on the vectors labeling the rows of \( K_{2n} \). Therefore it is possible to find a subgroup of GL(2n, 2) isomorphic to \( \text{Sp}(2n, 2) \) which acts naturally on the rows of \( K_{2n} \).

**4.2. Kantor’s design as a 2-(\( v, k, \lambda \))-design**

In this section we independently verify Theorem 4.1.1. That is, we show that \( \Gamma_{2n} \) is indeed isomorphic to \( \text{Sp}(2n, 2) \).

Kantor [52] describes \( K_{2n} \) as a 2-(\( v, k, \lambda \))-design with parameters

\[
v = 2^{2n}, \quad k = 2^{2n-1} + \epsilon 2^{n-1}, \quad \lambda = 2^{2n-2} + \epsilon 2^{n-1}
\]

where \( \epsilon = \pm 1 \). So \( v \) is the number of points, \( k \) is the size of each block, and \( \lambda \) is the number of points each pair of blocks has in common. What we call Kantor’s design is the incidence matrix \( M \) of the 2-(\( v, k, \lambda \))-design above (with \( \epsilon = 1 \)) where each 0 is replaced with \(-1\). That is, \( K_{2n} = 2M - J_{2n} \). So let \( \mathcal{D} = (V_{2n}, \mathcal{B}) \) be the design above, and let \( D = (V_{2n}, \mathcal{B}, I) \) be an incidence structure with incidence matrix \( M \).

**4.2.1 Lemma.** \( \text{Aut}(M) \cong \text{PAut}(K_{2n}) \).

Proof. See, e.g., [61, Lemma 2.33] ♦

An isomorphism of \( D \) onto its dual \( D^* \) of order 2 is a polarity. A polarity \( \theta \) is symplectic if and only if each point is incident with its image under \( \theta \).
We set \( m = k - \lambda \), and fix a block \( B \in \mathcal{B} \) such that \( B \) is the block representing the column labeled by the zero vector of \( V_{2n} \), which we set to be the first column. Thus \( 0 \in B \). Now for blocks \( X \neq B \) and \( Y \) define

\[
H_X = \{ Y \mid |(B \cup X) \cap (B \cap X)^c \cap Y| = m \} = \{ B, X \} \cup \{ Y \mid |B \cap X \cap Y| = \lambda - \frac{1}{2}m \}
\]

where the superscript \( c \) denotes complement. Call \( H_X \) a hyperplane. A set \( \mathcal{A} \) together with an underlying vector space \( V \), and a group action on \( V \), is called the affine space. Let \( \mathcal{A} \) be an affine space where \( V_{2n} \) is the underlying vector space, such that the points of \( \mathcal{A} \) are the blocks of \( \mathcal{D} \). The group action is addition of blocks, as follows.

Regarding \( B \) as the origin, \( X + B = X \) for all \( X \). By [52, Lemma 2] we have that for \( X, Y \neq B \), \( X + Y = B \Delta X \Delta Y \) if \( Y \in H_X \) and \( X + Y = (B \Delta X \Delta Y)^c \) if \( Y \notin H_X \), where \( X \Delta Y \) is the symmetric difference \( (X \cup Y) \cap (X \cap Y)^c \).

Let \( f : \mathcal{B} \times \mathcal{B} \to \text{GF}(2) \) be defined by letting \( f(Y, X) = 0 \) if \( Y \in H_X \), and \( f(Y, X) = 1 \) otherwise. Equivalently we write \( f(Y, X) = 0 \) if \( Y \in H_X \) since \( Y \in H_X \iff X \in H_Y \) and thus \( f(X, Y) = f(Y, X) \). The definition of \( H_X \) shows that the map \( \theta : X \to H_X \), \( X \neq B \), defines a symplectic polarity of the projective space \( \mathcal{A} - \{ B \} \), where \( \theta(X) = \{ Y \mid f(Y, X) = 0 \} \) for blocks \( X \) and \( Y \). A symplectic polarity is induced by an alternating bilinear form; \( \theta \) is induced by \( f \), thus \( \theta \) is the associated symplectic polarity of \( f \), and \( f \) is alternating bilinear. Now

\[
B \Delta X \Delta Y = B \Delta((X \cup Y) \cap (X \cap Y)^c)
= B \Delta((X \cup Y) \cap (X^c \cup Y^c))
= (B \cup ((X \cup Y) \cap (X^c \cup Y^c))) \cap (B \cap ((X \cup Y) \cap (X^c \cup Y^c)))^c
= (B \cup ((X \cap Y^c) \cup (X^c \cap Y))) \cap (B^c \cup ((X^c \cap Y^c) \cup (X \cap Y))).
\]

Thus

\[
0 \in B \Delta X \Delta Y \iff 0 \in (X^c \cap Y^c) \cup (Y \cap X) \tag{4.2.1}
\]

and

\[
0 \in (B \Delta X \Delta Y)^c \iff 0 \in (X^c \cap Y^c)^c \cap (Y \cap X)^c. \tag{4.2.2}
\]

Let \( Q : \mathcal{B} \to \text{GF}(2) \) be defined by letting \( Q(X) = 0 \) if \( 0 \in X \), and \( Q(X) = 1 \)
4. Automorphisms of Kantor’s design

otherwise.

4.2.2 Lemma. For all blocks $X, Y \in \mathcal{B}$, $f(X, Y) = Q(X + Y) + Q(X) + Q(Y)$.

Proof. We simply verify the lemma for a few scenarios. Suppose that $Y \in H_X$, so $f(X, Y) = 0$.

- $Q(X) = Q(Y) = 0$, i.e., $0 \in X, Y$. By (4.2.1), $0 \in X + Y$, so $Q(X + Y) = 0$.

- $Q(X) = Q(Y) = 1$, i.e., $0 \notin X, Y$. By (4.2.1), $0 \in X + Y$, so $Q(X + Y) = 0$.

- $Q(X) = 0$ and $Q(Y) = 1$. By (4.2.1), $0 \notin X + Y$, so $Q(X + Y) = 1$.

- $Q(X) = 1$ and $Q(Y) = 0$. By (4.2.1), $0 \notin X + Y$, so $Q(X + Y) = 1$.

The proof for $Y \notin H_X$ is similar, referring to (4.2.2). ♦

Now $\Gamma_{2n}$ is symplectic if $f(g(X), g(Y)) = f(X, Y)$ for all blocks $X$ and $Y$ and $g \in \Gamma_{2n}$. Equivalently $\Gamma_{2n}$ is symplectic if

$$Q(g(X) + g(Y)) + Q(g(X)) + Q(g(Y)) = Q(X + Y) + Q(X) + Q(Y)$$

for all $g \in \Gamma_{2n}$, $X, Y \in \mathcal{B}$. Choose any $g \in \Gamma_{2n}$. We know that $g$ acts linearly on $V_{2n}$. Since $g$ fixes the zero vector, clearly $Q(X) = Q(g(X))$ for all $X$, and we need only verify that $Q(g(X) + g(Y)) = Q(X + Y)$. We will use that $g(X \cup Y) = g(X) \cup g(Y)$ and $g(X \cap Y) = g(X) \cap g(Y)$. Either $Y \in H_X$ or $Y \notin H_X$. We deal with each case individually.

If $Y \in H_X$ then by (4.2.1),

$$0 \in X + Y \iff 0 \in (X^c \cap Y^c) \cup (X \cap Y)$$

$$\iff 0 \in (X^c \cap Y^c) \cup (X \cap Y)$$

$$\iff 0 \in g((X^c \cap Y^c) \cup (X \cap Y))$$

$$\iff 0 \in g(X^c) \cap g(Y^c) \cup (g(X) \cap g(Y))$$

$$\iff 0 \in g(X) + g(Y).$$
If $Y \notin H_X$ then by (4.2.2),

$$0 \in X + Y \iff 0 \in (X^c \cap Y^c)^c \cap (Y \cap X)^c$$
$$\iff 0 \in (X \cap Y^c) \cup (X^c \cap Y)$$
$$\iff 0 \in g((X \cap Y^c) \cup (X^c \cap Y))$$
$$\iff 0 \in (g(X) \cap g(Y^c)) \cup (g(X^c) \cap g(Y))$$
$$\iff 0 \in g(X) + g(Y).$$

So $Q(g(X) + g(Y)) = Q(X + Y)$ and thus $f(g(X), g(Y)) = f(X, Y)$ for all $X, Y$. Hence $\Gamma_{2n} \leq \text{Sp}(2n, 2)$, i.e., $\Gamma_{2n}$ is symplectic.

Since $\text{PAut}(K_{2n})$ is 2-transitive on $V_{2n}$ and has abelian socle by Lemma 4.1.9, $\Gamma_{2n}$ must have a subgroup isomorphic to $\text{Sp}(2n, 2)$ by the classification of 2-transitive affine permutation groups (see, e.g., [27, Chapter 7.7]). Therefore $\text{PAut}(K_{2n}) \cong \Sigma_{2n} \rtimes \text{Sp}(2n, 2)$, completing our proof of Theorem 4.1.1.

### 4.3. Regular subgroups of $\text{PAut}(K_{2n})$

Kantor observed that there are at least $n + 1$ regular subgroups of $\text{PAut}(K_{2n})$. All but two of the groups of order 16 are regular subgroups of $\text{PAut}(K_4)$, namely the cyclic and dihedral groups. Lemma 4.1.5 accounts for the $n + 1$ groups that Kantor observed. We now introduce a restriction on the exponent of any subgroup of $\text{PAut}(K_{2n})$, which excludes any group with a cyclic maximal subgroup for $n \geq 3$. This is analogous to Proposition 3.3.2.

#### 4.3.1 Proposition. The maximal order of any element of $\text{PAut}(K_{2n})$ is bounded above by $2^{\lceil \log_2(2n) \rceil + 1}$.

**Proof.** The argument is similar to Proposition 3.3.2. ♦

By Proposition 4.3.1, we see that for $n > 1$, $\text{PAut}(K_{2n})$ cannot have a cyclic regular subgroup; and for $n > 2$, it cannot have a regular subgroup with cyclic maximal subgroup.

Let $R$ be a regular subgroup of $\Sigma_{2n} \rtimes \text{Sp}(2n, 2)$. Since $R$ is transitive on $V_{2n}$, we have $R = \{ \pi_v g_v \mid v \in V_{2n} \}$ where $g_v \in \text{Sp}(2n, 2)$. Here it is not necessarily the case that the elements of the multiset $\Lambda = \{ g_v \mid \pi_v g_v \in R \}$ are unique. For example we know that $\Lambda$ may contain only the identity, as possibly $R = \Sigma_{2n}$. So let $m$ be the value such that $C_2^m \cong S = \{ \pi_v \mid \pi_v \in R \} \leq \Sigma_{2n}$.
4. Automorphisms of Kantor’s design

4.3.2 Lemma. \( R \cong S \rtimes T \) where \( T \) is isomorphic to a subgroup of \( \text{Sp}(2n, 2) \) of order \( 2^{2n-m} \).

Proof. First, since \( S \leq \Sigma_{2n} \) and \( \Sigma_{2n} \) is normalized by \( \text{Sp}(2n, 2) \), we have that \( S \leq R \). Let \( T \) be a complement of \( S \) in \( R \). The elements \( g_v \) where \( \pi_v g_v \in T \) are unique, and thus constitute a group isomorphic to \( T \).

4.3.1. Group-developed Hadamard matrices of order 64

Using Magma [8], we can compute the regular subgroups of the full automorphism group of \( K_{2n} \); this can be computationally expensive due to the size of \( \text{Aut}(K_{2n}) \). Of course, a regular subgroup of \( \text{PAut}(K_{2n}) \) is a regular subgroup of \( \text{Aut}(K_{2n}) \). We computed \( \text{PAut}(K_6) \) and searched for its regular subgroups. We found that \( K_6 \) is group-developed over 171 of the 267 groups of order 64. All of these have exponent 2, 4, or 8. Interestingly none of these groups are of exponent 16, which is the upper bound we derive from Proposition 4.3.1. This is in accordance with [26]. We are unable to calculate the regular subgroups of \( \text{PAut}(K_8) \) at present.
Part II.

Shift representations on $\mathbb{Z}$-cocycles
5. Shift actions

The shift action of a finite group on sets of its cocycles was first defined by Horadam in [45]; see also [44, 46, 56] and [43, Chapter 8]. We review some of this previous work, and develop the theory further. This includes the solution of previously open problems about fixed points under the shift action.

Much of this chapter and the next has already been published in the paper [35] co-authored with Dane Flannery.

5.1. Shift actions

Let $G$ and $U$ be finite non-trivial groups, with $U$ abelian. Let $Z(G,U)$ and $B(G,U)$ denote the cocycle and coboundary groups, as defined in Section 2.5. The shift action of $G$ on $Z(G,U)$ is defined by

$$\psi \cdot a = \psi \partial \psi a$$ \hspace{1cm} (5.1.1)

for $\psi \in Z(G,U)$ and $a \in G$, where $\psi a := \psi(a, -) \in \text{Fun}(G,U)$. Equation (5.1.1) clearly defines an action that preserves cohomological equivalence; and hence induces an action of $G$ on each cocycle class in $H(G,U)$. From now on, we write $\psi a$ for $\psi \cdot a$.

A cocycle $\psi \in Z(G,U)$ is said to be multiplicative in its left (resp., right) component if $\psi(g,k)\psi(h,k) = \psi(gh,k)$ (resp., $\psi(g,h)\psi(g,k) = \psi(g,hk)$) for all $g, h, k \in G$. Using (2.5.1) it can be shown that $\psi$ is multiplicative in one component if and only if it is multiplicative in both. (Also, any element of $\text{Fun}(G^2, U)$ multiplicative in both components is a cocycle. Thus one familiar instance of a multiplicative cocycle is a bilinear form on a vector space over a field of prime size.) The set of all multiplicative cocycles forms a subgroup $M(G,U)$ of $Z(G,U)$.

For $H \leq G$, $\text{Fix}(H)$ will denote the set of $H$-fixed points in $Z(G,U)$ under
5. Shift actions

the shift action.

5.1.1 Lemma. \( \psi \in Z(G, U) \) is multiplicative if and only if \( \psi \in \text{Fix}(G) \).

Proof. \( \psi \) is multiplicative \( \iff \psi_a \in \text{Hom}(G, U) \iff \partial \psi_a \) is trivial \( \iff \psi a = \psi \) for all \( a \in G \).

We note the link to algebraic design theory. A cocycle \( \psi \in Z(G, U) \) is orthogonal if

\[
|\{ h \in G \mid \psi(g, h) = u \}| \tag{5.1.2}
\]

is constant for all \( g \in G \setminus \{1\} \) and \( u \in U \). A necessary condition for \( Z(G, U) \) to possess orthogonal cocycles is that \( |G| \) be divisible by \( |U| \). In particular, if \( U = \langle -1 \rangle \) then \( \psi \) is orthogonal if and only if \( [\psi(g, h)]_{g, h \in G} \) is Hadamard; here the frequency \( \text{[5.1.2]} \) is \( |G|/2 \) (of course we know then that \( |G| > 2 \) must be divisible by 4).

5.1.2 Lemma. If \( \psi \in Z(G, U) \), \( a \in G \), and \( \varphi = \psi \partial \psi_a \), then \( \varphi \) is orthogonal if and only if \( \psi \) is orthogonal.

Proof. See [43, Lemma 8.4].

Lemma 5.1.2 is one motivation for the study of shift actions: each shift orbit in \( Z(G, U) \) either is comprised entirely of orthogonal elements, or it contains none at all. Observe, however, that a shift orbit has comparatively small maximal size, viz. \( |G| \); and, because \( |Z(G, U)| \) grows exponentially with \( |G| \), so too does the number of shift orbits.

In the next chapter, we introduce the idea of linear shift representations, which reduces the shift degree and enables us to calculate with the action using tools of matrix group theory.

5.2. Fixed points

To prove our results about reducibility of shift representations in the next chapter, we first need to consider fixed points (i.e., multiplicative cocycles) under the shift action. We do so in this section. In the process, we address Research Problem 55 (1) of [43].

Let \( \text{Fix}(G) \), \( \text{Fix}_B(G) \) denote the set of \( G \)-fixed points in \( Z(G, U) \), \( B(G, U) \) respectively.
5.2.1 Lemma.  (i) Each element of $\text{Fix}(G)$ is trivial in both components on $G'$.

(ii) If $\text{Hom}(G, U)$ is trivial then so too is $\text{Fix}(G)$.

Proof. (Cf. [43, Corollary 8.44, p. 188].) Both parts are consequences of the fact that $\psi(g, -), \psi(-, g) \in \text{Hom}(G, U)$ for all $g \in G$ if $\psi \in \text{Fix}(G)$. ♦

Let $N \trianglelefteq G$. The inflation homomorphism $\text{inf} : \text{Fun}((G/N)^k, U) \rightarrow \text{Fun}(G^k, U)$ defined by

$$\text{inf}(f)(g_1, \ldots, g_k) = f(g_1N, \ldots, g_kN)$$

is injective. If $f \in Z(G/N, U)$ or $B(G/N, U)$ then $\text{inf}(f) \in Z(G, U)$ or $B(G, U)$ respectively. Thus $\text{inf}$ induces a homomorphism $H(G/N, U) \rightarrow H(G, U)$. This is not necessarily injective.

5.2.2 Lemma. $\text{Fix}(G) \cong \text{Fix}(G/G')$.

Proof. For $\psi \in \text{Fix}(G)$ we set $\tilde{\psi}(gG', hG') = \psi(g, h)$; then $\tilde{\psi} \in \text{Fun}(G/G', U)$ by Lemma 5.2.1 (i). Moreover, it is easily checked that $\tilde{\psi} \in \text{Fix}(G/G')$, and that the assignment $\psi \mapsto \tilde{\psi}$ defines an isomorphism with inverse $\text{inf} : Z(G/G', U) \rightarrow Z(G, U)$ on $\text{Fix}(G/G')$. ♦

5.2.3 Remark. Although $\text{Fix}_B(G/G')$ is isomorphic to a subgroup of $\text{Fix}_B(G)$ via inflation, the isomorphism $\text{Fix}(G) \rightarrow \text{Fix}(G/G')$ in the proof of Lemma 5.2.2 need not map $\text{Fix}_B(G)$ into $B(G/G', U)$.

5.2.4 Proposition. Suppose that $U$ is a cyclic $p$-group, and $G$ is a finite abelian $p$-group of rank $r$. Then $\text{Fix}(G) \cong U^r$.

Proof. Let $G = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle$ and $|U| = p^s$. If $\psi \in \text{Fix}(G)$ then

$$\psi \left( \prod_{i=1}^{r} x_i^{a_i}, \prod_{j=1}^{r} x_j^{b_j} \right) = \prod_{i,j=1}^{r} \psi(x_i, x_j)^{a_i b_j},$$

using that $\psi$ is multiplicative. This implies that the map $\text{Fix}(G) \rightarrow \text{Mat}(r, U)$ defined by $\psi \mapsto (\psi(x_i, x_j))_{i,j}$ is an injective homomorphism of abelian groups, viewing $U$ and then $\text{Mat}(r, U)$ additively.

In the opposite direction, for each $M \in \text{Mat}(r, U)$ define $\psi_M : C_p^r \times C_p^r \rightarrow U$ by $\psi_M(x, y) = \epsilon(x)M\epsilon(y)^\top$, where $\epsilon(z) = (a_1, \ldots, a_r)$ is the exponent vector of
5. **Shift actions**

\[ z = (x_1^{a_1}, \ldots, x_r^{a_r}), \ 0 \leq a_i \leq p - 1. \] That is, \( \psi_M \in \text{Fix}(C_p^r) \) is the bilinear form corresponding to \( M \), working over the ring \( U \cong \mathbb{Z}_p \). We obtain the obvious injection of \( \text{Mat}(r, U) \) into \( \text{Fix}(C_p^r) \). By the previous paragraph, \( \text{Fix}(C_p^r) \) has order at most \( p^{sr^2} \); so it has order exactly \( p^{sr^2} \). Since inflation embeds \( \text{Fix}(C_p^r) \) into \( \text{Fix}(G) \), we are done. ♦

Let \( S \) be the set of common prime divisors of \( |U| \) and \( |G : G'| \), \( r_p \) be the rank of the Sylow \( p \)-subgroup of \( G / G' \), and \( U_p \) be the Sylow \( p \)-subgroup of \( U \).

5.2.5 **Theorem.** \( \text{Fix}(G) \cong \prod_{p \in S} U_p^r \).

**Proof.** Additivity of \( Z(K, -) \) and Lemmas 5.2.1(ii), 5.2.2 permit us to assume that \( G \) is abelian and replace \( U \) by \( \prod_{p \in S} U_p \). Also, restriction of \( \text{Fix}(X \times Y) \) to \( \text{Fix}(X) \) is an isomorphism if \( |Y| \) and \( |U| \) are coprime. Now use Proposition 5.2.4. ♦

5.2.6 **Remark.** Theorem 5.2.5 and Theorem 5.2.9 below answer most of Research Problem 55 (1) in [43].

Having dealt with \( \text{Fix}(G) \), we move on to analyzing \( \text{Fix}_B(G) \). (This task is not so straightforward; recall Remark 5.2.3.) We need the explicit version of Theorem 2.5.1 as justified in [34 Section 3]: \( H(G, U) = I(G, U) \times T(G, U) \) where \( I(G, U) \) is the isomorphic image of \( \text{Ext}(G / G', U) \) under \( \inf : H(G / G', U) \to H(G, U) \), and \( T(G, U) \) is the image of \( \text{Hom}(H_2(G), U) \) under a ‘transgression’ embedding.

5.2.7 **Lemma.** Suppose that \( U \) is a cyclic \( p \)-group for an odd prime \( p \) dividing \( |G : G'| \) but not \( |G'| \). Then \( \left[ \psi \right] \cap \text{Fix}(G) = \emptyset \) for all non-trivial \( \left[ \psi \right] \in I(G, U) \).

**Proof.** We first recap some material from [36 Section 2]. Let \( U = \langle u \rangle \) and \( P / G' = \langle g_1 G' \rangle \times \cdots \times \langle g_n G' \rangle \) be the Sylow \( p \)-subgroup of \( G / G' \), where \( g_i G' \) has order \( p^{e_i} \geq p \) in \( G / G' \). Suppose that \( G / G' = P / G' \times K / G' \). Define \( M_i \) to be the \( p^{e_i} \times p^{e_i} \) matrix

\[
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & 1 \\
1 & 1 & 1 & \cdots & 1 & u & u \\
1 & 1 & 1 & \cdots & 1 & u & u \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
1 & 1 & u & \cdots & u & u & u \\
1 & u & u & \cdots & u & u & u \\
\end{bmatrix}
\]
Then put
\[ N_i = J_{p^{e_1}+\ldots+p^{e_n-1}} \otimes M_i \otimes J_{p^{e_{i+1}}+\ldots+p^{e_n}} \otimes J_{|K|}, \]

\[ J_d \] denoting the \( d \times d \) all 1s matrix. The rows and columns of \( M_i \) are indexed \( 1, g_i, \ldots, g_i^{p^{e_i}-1} \); while \( N_i \) is indexed by the ‘Kronecker product’
\[ \{1, g_1, \ldots, g_1^{p_1-1}\} \otimes \cdots \otimes \{1, g_n, \ldots, g_n^{p_n-1}\} \otimes K \]
of ordered sets in \( G \) (under an obvious interpretation). The matrix \( N_i \) designates a cocycle \( \psi_i \in Z(G,U) \), and \( I(G,U) = \langle [\psi_i] : 1 \leq i \leq n \rangle \).

Suppose that \( \psi \in \langle \psi_i : 1 \leq i \leq n \rangle \) and \( \psi \partial \phi \in \text{Fix}(G) \setminus B(G,U) \). Then we must have \( \psi \partial \phi(g_k, g_k) = \psi \partial \phi(g_k, g_k) = u^m \) say, for some \( k, m \) and \( 1 \leq s < \min\{p^s, |u|\} \). Write \( g \) for \( g_k \) and \( e \) for \( e_k \). Since row \( g \) of \( N_k \) has \( u \) in column \( g^{p^e-1} \) and 1 in column \( g_j \) for \( j < p^e-1 \),
\[ \partial \phi(g, g^{p^e-1}) = u^{m(p^e-1)} \psi_k^s(g, g^{p^e-1})^{-1} = u^{(p^e-1)m-s} \]
whereas \( \partial \phi(g, g^j) = u^{m_j} \). Hence
\[ \prod_{j=1}^{p^e-1} \partial \phi(g, g^j) = u^{(\sum_{j=1}^{p^e-1} j)m-s}. \]

Furthermore \( \sum_{j=1}^{p^e-1} j \equiv 0 \mod p^e \). So
\[ \prod_{j=1}^{p^e-1} \phi(g)^{-1} \cdot \prod_{j=1}^{p^e-1} \phi(g^j)^{-1} \cdot \prod_{j=1}^{p^e-1} \phi(g^{j+1}) = u^{-s}U^{p^e} \]
\[ = \phi(g)^{-p^e} \cdot \prod_{j=2}^{p^e-1} \phi(g^j)^{-1} \cdot \prod_{j=2}^{p^e} \phi(g^j) \in u^{-s}U^{p^e} \]
\[ \Rightarrow \phi(g^{p^e}) \in u^{-s}U^{p^e}. \]
Now \( h = g^{p^e} \in G' \), and therefore
\[ \partial \phi(h, h^j) = \psi \partial \phi(h, h^j) = \psi \partial \phi(g, h^j)^{p^e} \]
because \( \psi \) is inflated from \( Z(G/G', U) \). Hence \( \partial \phi(h, h^j) \in U^{p^e} \). Induction on \( j \)
5. Shift actions

yields \( \phi(h^j) \in \phi(h^j)U^{p^r} \). If \(|h| = r\) then

\[
u^{-rs} \in \phi(h)^r U^{p^r} = \phi(h^r)U^{p^r} = U^{p^r}.
\]

Since \( r \) is coprime to \( p \), this implies that \( u^s \in U^{p^r} \): a contradiction. Thus we cannot have \( \psi \partial \phi \in \text{Fix}(G) \setminus B(G, U) \) for non-trivial \( [\psi] \in I(G, U) \), proving the lemma.  

\[\Box\]

5.2.8 Remark. As further preparation for the next result, we note that when \( G \) is an abelian 2-group, and \( \psi_i, s \) are as in the above proof, \( [\psi^s] \cap \text{Fix}(G) = \emptyset \) if and only if \( e_i > 1 \) or \(|U| > 2\).

At this juncture, it is useful to identify certain subgroups of \( Z(G, U) \). A cocycle \( \psi \) is symmetric if \( \psi(g, h) = \psi(h, g) \) for all \( g, h \in G \). The set of all symmetric cocycles forms a subgroup \( S(G, U) \) of \( Z(G, U) \). We say that \( \psi \) is almost symmetric if \( \psi(g, h) = \psi(h, g) \) whenever \( g \) and \( h \) commute. Denote the subgroup of almost symmetric cocycles in \( Z(G, U) \) by \( \text{AS}(G, U) \). Clearly \( S(G, U) \leq \text{AS}(G, U) \leq Z(G, U) \), and \( B(G, U) \leq \text{AS}(G, U) \). (Incidentally, the latter inclusion shows that \( \text{AS}(G, U) \) is invariant under the shift action.) If \( G \) is abelian then \( \text{AS}(G, U) = S(G, U) \) and every coboundary is symmetric. In that case it is known that \( \text{AS}(G, U)/B(G, U) \cong \text{Ext}(G/G', U) \). It is unknown whether or not this statement holds in general for non-abelian \( G \).

5.2.9 Theorem. Let \( G \) be abelian. In the notation defined just before Theorem 5.2.5, \( \text{Fix}_B(G) \cong \prod_{p \in S} U_p^{s_p} \) where

(i) \( s_p = \left( \frac{r^p + 1}{2} \right) \) if \( p \) is odd or \(|U_p| > 2\),

(ii) \( s_2 = \left( \frac{r_2^2 + 1}{2} \right) - k \) if \(|U_2| = 2\) and the largest elementary abelian subgroup over which the Sylow 2-subgroup of \( G \) splits has rank \( k \).

Proof. (Cf. Theorem 5.2.5 and its proof.) Since

\[
\text{Fix}_B(G) \cong \prod_{p \in S} \text{Fix}_{B(G_p, U_p)}(G_p)
\]

where \( G_p \) is the Sylow \( p \)-subgroup of \( G \), we assume that \( G, U \) are \( p \)-groups with \( U \) cyclic. Next, \( I(G, U) = \text{AS}(G, U)/B(G, U) \) and \( \text{Fix}_B(G) \leq F := \)}
Fix($G$) \cap AS($G, U$). As the proof of Proposition 5.2.4 shows, there is a bijective
mapping from $F$ to the set of symmetric elements of Mat($r, U$). Now everything
follows from Lemma 5.2.7 and Remark 5.2.8. ♦

5.2.10 Remark. According to [43, Theorem 6.10,p. 122], if $G \cong C_p^r$ then there
exist multiplicative orthogonal cocycles in $Z(G, C_p)$, and there are $|GL(r, p)|$
of these ($|M(G, C_p)| = p^{r^2}$ and GL($r, p$) has a Sylow $p$-subgroup of rank $(\binom{r}{2})$.)
Comparing this count with the one in Proposition 5.2.4, we realize that the
orthogonal multiplicative cocycles for elementary abelian $G$ are not entirely
coboundaries.

We discuss Fix$_B(G)$ for non-abelian $G$ further in the next subsection.

5.2.1. Fixed coboundaries for non-abelian groups

Assume that $U = \langle u \rangle \cong C_p$. The value $s_p$ in Theorem 5.2.9
is a lower bound on the dimension of Fix$_B(G)$ for any $G$. Although inflation embeds Fix$_B(G/G')$
into Fix$_B(G)$, Remark 5.2.3 indicates that elements of Fix$_B(G)$ need not all be
inflated from Fix$_B(G/G')$. Indeed, as we will see, a cocycle in an element of
$H(G/G', U) \setminus I(G/G', U)$ might inflate to a coboundary. Thus the dimension
of Fix$_B(G)$ can be greater than $s_p$; Table 6.6.1 in Section 6.6.1 lists examples
of such $G$. In this subsection we explore how the dimension bound for Fix$_B(G)$
can be exceeded.

Let $r$ be the rank of the Sylow $p$-subgroup of $G/G'$. Recall that Fix($G/G'$)
is in one-to-one correspondence with Mat($r, U$). Label the rows and columns
of $M = [m_{ij}] \in$ Mat($r, U$) by the generators $a_1, \ldots, a_r$ of the Sylow $p$-subgroup
of $G/G'$, and let $\psi$ be a multiplicative cocycle corresponding to $M$, where
$\psi(a_i, a_j) = m_{ij}$. The diagonal matrices in Mat($r, U$) correspond to fixed cocy-
cles in elements of $I(G/G', U)$. The remaining symmetric matrices correspond
to fixed coboundaries. The non-symmetric matrices correspond to the fixed
cocycles in elements of $H(G/G', U) \setminus I(G/G', U)$. The matrices $e_{ij}$ with $u$
in position $(i, j)$ and $1$ elsewhere additively generate Mat($r, U$), and the fixed
cocycles in elements of $H(G/G', U) \setminus I(G/G', U)$ correspond to the subgroup
generated by the $e_{ij}$ for $i < j$. Let $j > i$ and let $\mu$ be the cocycle corresponding
to $e_{ij}$. We now consider when inf($\mu$) = $\psi \in Z(G, U)$ can be a coboundary.
5. Shift actions

5.2.11 Lemma. Suppose that $|G'|$ is coprime to $p$, and that $G$ splits over $G'$; say $G = G' \rtimes R$. Then the lower bound $s_p$ on $\text{Fix}_B(G)$ is attained.

Proof. Let $a_1, \ldots, a_r$ be the generators of the Sylow $p$-subgroup of $G/G'$ and let $b_i = \pi(a_i)$ where $\pi$ is natural surjection $G/G' \to R$. Suppose for $\psi = \inf(\mu)$ that $\psi(b_i, b_j) = u$, $\psi(b_j, b_i) = 1$. If $\psi = \partial \phi$ then $\phi(b_i b_j) = \phi(b_j b_i)$. Also $b_j b_i = g b_i b_j$ for some $g \in G'$. Thus $\phi(b_i b_j) \neq \phi(g b_i b_j)$. Since $\psi(b_i, b_j) = \psi(g b_i, b_j)$ we have $\phi(b_i) \neq \phi(g b_i)$, which implies that $\phi(g) = u^k$ for some $k$; otherwise $\partial \phi(g, b_i) = \phi(g)^{-1} \phi(b_i)^{-1} \phi(g b_i) \neq 1$. It is straightforward to verify that if $\partial \phi(g, g^m) = 1$ for all $m$ then $\phi(g^m) = u^{mk}$ for all $m$. If $|g| = n$ is coprime to $p$ then $\phi(1) = u^{nk} \neq 1$; a contradiction. Thus we cannot have that $\psi = \inf(\mu)$ and $\psi(b_i, b_j) = u$, $\psi(b_j, b_i) = 1$. ♦

In contrast to Lemma 5.2.11, the next example illustrates what can happen when $p$ divides $|G'|$.

5.2.12 Example. Let $G$ be the dihedral group $\langle x, y \mid x^8 = y^2 = 1, x^4 y = x^{-1} \rangle$ of order 16; and let $U = \langle u \rangle \cong C_2$. By Theorem 5.2.9 the dimension of $\text{Fix}_B(G)$ is at least 1. In fact the dimension is 2. In this case $G' = \langle x^2 \rangle$ and $G/G' = \langle x G', y G' \rangle \cong C_2^2$. Let $\mu \in \text{Fix}(G/G')$ be such that $\mu(x G', y G') = u$ and $\mu(x^5 G', x G') = \mu(y G', x G') = \mu(y G', y G') = 1$. Note that $\mu$ is not a coboundary. Define $\phi : G \to U$ by

$$\phi(g) = \begin{cases} 
1 & \text{if } g \in \{1, x, x^4, x^5, xy, x^2y, x^5y, x^6y\} \\
u & \text{otherwise.} \end{cases}$$

Then $\inf(\mu) = \partial \phi$. Thus a fixed point in a non-trivial element of $T(G/G', U)$ is mapped by $\inf$ into $\text{Fix}_B(G)$. 52
6. Linear shift representations

This chapter carries on directly from Chapter 5. We introduce the concept of (linear) shift representation. After giving some basic facts, we comprehensively describe reducibility of these representations. We apply our new theory to the search for orthogonal cocycles. An algorithm for computing shift representations is described, which we have implemented in Magma [8], and used to significantly extend earlier computational work of Horadam and LeBel [43, 56, 57].

6.1. Shift representations

Denote the permutation representation $G \to \text{Sym}(Z(G,U))$ corresponding to the shift action of $G$ on $Z(G,U)$ by $\Gamma$. That is, $\psi \Gamma(a) = \psi a$, for $\psi \in Z(G,U)$, $a \in G$. This is the shift representation of $G$ on $Z(G,U)$. If $S \subseteq Z(G,U)$ is $\Gamma(G)$-invariant then $\Gamma_S$ will denote the restricted representation of $G$ in $\text{Sym}(S) \subseteq \text{Sym}(Z(G,U))$. In particular, for $\mu \in Z(G,U)$, $\Gamma_{\mu B}$ denotes the representation of $G$ in $\text{Sym}(S) \subseteq \text{Sym}(\mu B(G,U))$.

6.1.1 Lemma. If $S$ is a $\Gamma(G)$-invariant subgroup of $Z(G,U)$ then $\Gamma_S$ is a homomorphism $G \to \text{Aut}(S)$.

Proof. Cf. [43] Lemma 8.34.

It turns out that $\Gamma$ is almost always faithful.

6.1.2 Lemma. Suppose that $|G| \geq 5$. For any $\mu \in Z(G,U)$, $\Gamma_{\mu B}$ is faithful. Hence $\Gamma$ is faithful.

Proof. If $\Gamma_{\mu B}(a) = 1$ then $\psi(a,g)^{-1}\psi(a,h)^{-1}\psi(a,gh) = 1$ for all $g, h \in G$ and $\psi \in B(G,U)$, so $\psi_a$ is a homomorphism for all $\psi \in B(G,U)$. Thus

$$\phi(a)^{-1}\phi(g)^{-1}\phi(ag)\phi(a)^{-1}\phi(h)^{-1}\phi(ah) = \phi(a)^{-1}\phi(gh)^{-1}\phi(agh)$$
6. Linear shift representations

giving

\[ \phi(ag)\phi(ah)\phi(gh) = \phi(a)\phi(g)\phi(h)\phi(agh) \quad (6.1.1) \]

for all \( \phi \in \text{Fun}(G, U) \) and \( g, h \in G \). By first setting \( g = a^{-1} \) in (6.1.1), and then setting \( h = a^{-1} \) in (6.1.1), and combining, we get

\[ \phi(g)\phi(\text{ga}^{-1}) = \phi(a^{-1}g)\phi(aga^{-1}) \quad (6.1.2) \]

Suppose that \( g \in G \setminus C_G(a) \), and choose \( \phi \) so that \( \phi(g) = \phi(a^{-1}g) = \phi(aga^{-1}) = 1 \). Now if \( a \neq 1 \) then \( ga^{-1} \notin \{1, g, a^{-1}, aga^{-1}\} \), so we can further insist that \( \phi(ga^{-1}) \neq 1 \). Since this contradicts (6.1.2), we conclude that \( a \in Z(G) \).

Let \( g \notin \{1, a^{-1}\} \), \( h \notin \{1, a, g, ag\} \), and \( \phi(ag) \neq 1 \). If \( a \neq 1 \) then \( ag \notin S := \{ah, gh, a, g, h, agh\} \), so we are free to choose \( \phi \) to be 1 on \( S \). But then \( \phi(ag) = 1 \) by (6.1.1). Thus if \( |G| \geq 5 \) and \( \psi_a \) is a homomorphism for all \( \psi \in B(G, U) \) we arrive at a contradiction, i.e., \( \Gamma_{\mu B} \) is faithful.

6.1.3 Remark. It is easily checked that for \( |G| < 5 \), \( \Gamma \) is faithful if and only if \( G \cong C_3 \) or \( G \cong C_4 \) or \( U \) is not an elementary abelian 2-group. If \( G \cong C_2 \) or \( C_2 \times C_2 \) and \( U \) is an elementary abelian 2-group then \( \Gamma \) is trivial.

6.1.4 Corollary. Suppose that \( |G| \geq 5 \). If \( S \) is a subgroup of \( Z(G, U) \) containing \( B(G, U) \) then \( \Gamma_S \) is a faithful representation of \( G \) in \( \text{Aut}(S) \).

By Theorem 2.5.1 \( Z(G, U) \cong U^{[G]} \times \text{Hom}(H_2(G), U) \). If \( U \cong C_p \) then we may treat the additive group \( Z(G, U) \) as a vector space of dimension \( |G| + r - 1 \) over \( \mathbb{F}_p \), the finite field of order \( p \), where \( r \) is the rank of the Sylow \( p \)-subgroup of \( H_2(G) \). It follows that \( \text{Aut}(Z(G, U)) \cong \text{GL}(n, \mathbb{F}_p) \), where \( n = |G| + r - 1 \). Also by Theorem 2.5.1 \( B(G, U) \) is an \( \mathbb{F}_p \)-vector space of dimension \( |G| - s - 1 \) where \( s \) is the rank of the Sylow \( p \)-subgroup of \( G/G' \). Hence the following theorem, which is crucial.

6.1.5 Theorem. Suppose that \( G \) has order \( m \geq 5 \) and \( U \) has prime order \( p \). With the notation above,

(i) \( \Gamma \) is a faithful representation of \( G \) in \( \text{GL}(m + r - 1, p) \).

(ii) \( \Gamma_B \) is a faithful representation of \( G \) in \( \text{GL}(m - s - 1, p) \).

6.1.6 Example. \( \Gamma_{AS(G, C_p)} \) has degree at least \( |G| - 1 \).
6.1.7 Example. \(\Gamma_{M(G,U)}\) is trivial.

Recall from Lemma 5.1.2 that elements of an orbit under the shift action are either all orthogonal, or all not orthogonal, and thus a search for orthogonal cocycles in \(Z(G,C_p)\) can run over a set of representatives for the shift orbits of lines (1-dimensional subspaces). In this important context, and more generally, the notion of shift representation enables us to use tools of linear group theory in our study of shift actions. So we are now going to consider linear shift representations of \(G\) derived from the actions on \(Z(G,U)\) and \(B(G,U)\).

We determine when \(\Gamma\) and \(\Gamma_B\) are irreducible or completely reducible. We examine how module and orbit properties interact, and the orbit structure within \(Z(G,U)\) and \(B(G,U)\).

6.2. Shift representations via linear groups

It is necessary first to recall some relevant standard definitions and results from linear group theory (as in, e.g., [28, Chapters 1 and 2]). Let \(H \leq \text{GL}(n,K)\), \(K\) a field, and let \(V\) be the underlying space for \(\text{GL}(n,K)\). A \(H\)-invariant subspace \(W\) is a \(H\)-module (\(H\)-submodule of \(V\)). If \(W\) has a proper non-zero \(H\)-submodule then \(W\) is reducible; otherwise it is irreducible. We also call \(H\) irreducible if \(V\) is. Note that \(H\) is conjugate in \(\text{GL}(n,K)\) to a group of block triangular matrices with irreducible diagonal blocks (‘irreducible parts’ of \(H\)).

A completely reducible \(H\)-module is a direct sum of irreducible submodules; call \(H\) completely reducible if \(V\) is. In that event \(H\) has a block diagonal conjugate in \(\text{GL}(n,K)\) with irreducible diagonal blocks.

6.2.1 Theorem (Clifford). A normal subgroup of a completely reducible group is completely reducible.

6.2.2 Theorem (Maschke). A finite subgroup of \(\text{GL}(n,K)\) of order coprime to \(\text{char } K\) is completely reducible.

Suppose that \(\text{char } K = p\) henceforth.

6.2.3 Lemma. A \(p\)-subgroup \(P \neq 1\) of \(\text{GL}(n,K)\) is reducible but not completely reducible. In particular, \(P\) has non-trivial fixed points in \(V\), and any irreducible \(P\)-module is 1-dimensional.
6. Linear shift representations

6.2.4 Corollary. If $H$ has a non-trivial normal $p$-subgroup then $H$ is not completely reducible.

6.2.5 Corollary. A nilpotent subgroup $H$ of $\text{GL}(n, K)$ is completely reducible if and only if $p$ does not divide $|H|$.

We state below some well-known facts about irreducible abelian linear groups that are needed later.

6.2.6 Lemma. Let $K$ be finite of size $q$. A cyclic subgroup $G$ of $\text{GL}(n, K)$ is irreducible if and only if $|G|$ divides $q^n - 1$ but does not divide $q^k - 1$ for $1 \leq k < n$. At each possible order, there is a single conjugacy class of irreducible cyclic subgroups of $\text{GL}(n, K)$.

We now focus on shift representations. Assuming $\Gamma$ to be faithful, we identify $G \neq 1$ with $\Gamma(G)$. Remember that orthogonal cocycles in $Z(G, U)$ can exist only if $|U|$ divides $|G|$.

6.2.7 Lemma. Suppose that $U$ is an elementary abelian $p$-group of rank $r$. Then $Z(G, U) \cong \bigoplus_{j=1}^{r} Z(G, C_p)$ as $G$-modules.

Proof. Say $U = U_1 \times \cdots \times U_r$ where $U_i \cong C_p$. Each subgroup $Z(G, U_i)$ of $Z(G, U)$ is a $G$-module, because it consists of the cocycles that map into $U_i$. ♦

In the situation of Lemma 6.2.7, $G$ is conjugate in $\text{GL}(d, p)$ to a matrix group in block diagonal form $\{\text{diag}(\alpha(g), \ldots, \alpha(g)) \mid g \in G\}$ where $d = \dim_{\mathbb{F}_p}(Z(G, U))$ and $\alpha$ is a homomorphism $G \to \text{GL}(d/r, p)$. This shows explicitly how the shift representation theory of $Z(G, U)$ reduces to that of $Z(G, C_p)$. If $U$ is not elementary abelian then we must deal with shift action on $Z(G, C_{p^a})$ for $a \geq 2$; depending on $G$, this may or may not lead to shift representations in $\text{GL}(n, \mathbb{Z}_{p^a})$.

6.2.8 Lemma. If $|G|$ and $|U|$ are coprime then $Z(G, U) = B(G, U)$.

Proof. See, e.g., [21, Lemma 20.6.3, p. 246]. ♦

Observe that $B(G, C_p) = 0$ if and only if $p = 2$ and $G \cong C_2$. Thus $Z(G, C_p)$ is reducible whenever $H(G, C_p)$ is non-trivial. As preliminary results on complete reducibility of shift representations, we have the following.
6.2.9 Lemma. Suppose that $Z(G, C_p)$ is completely reducible. Then there exists a $G$-submodule $W$ of $Z(G, C_p)$ isomorphic (as groups) to $H(G, C_p)$ such that $Z(G, C_p) = B(G, C_p) \oplus W$. In fact, $W$ consists entirely of fixed points; hence, each non-trivial cocycle class contains non-trivial fixed points.

Proof. Since $Z(G, C_p)$ is completely reducible, $Z(G, C_p) = B(G, C_p) \oplus W$ for some $G$-submodule $W$. The elements of $W \cong H(G, C_p)$ are therefore pairwise non-cohomologous. For all $\psi \in W$ and $a \in G$, $\psi a \in W$ is cohomologous to $\psi$: thus $\psi a = \psi$.

6.2.10 Corollary. If $p$ is an odd prime dividing $|G : G'|$ but not $|G'|$ then $Z(G, C_p)$ is not completely reducible.

Proof. Apply Lemmas 5.2.7 and 6.2.9.

We explore reducibility of shift representations in depth in the next section.

6.3. Completely reducible representations

Throughout this section $U = \langle u \rangle \cong C_p$. Our first results concern reducibility of the coboundary submodule.

6.3.1 Proposition. Suppose that $B(G, U)$ is irreducible. Then $|G|$ is not divisible by $p$.

Proof. Assume that $p$ divides $|G|$. By Corollary 6.2.5, $G$ is not abelian; and by Lemma 6.2.3, there is non-zero $\psi \in B(G, U)$ such that $|\text{Stab}_G(\psi)| \geq p$. Also $\psi G$ contains at least $|G| - s - 1$ distinct elements, where $s$ is the rank of the Sylow $p$-subgroup of $G/G'$. Thus

$$|G| \geq p|G : \text{Stab}_G(\psi)| \geq p|G| - p(s + 1),$$

implying that $s \neq 0$. Then

$$p^s \leq |G : G'| < |G| \leq \frac{p}{p - 1}(s + 1).$$

Hence $p^{s-1}(p - 1) < s + 1$, which is a contradiction for $p$ odd. If $p = 2$ then by the inequality above $s \leq 2$; but $s = 2$ forces $|G| \leq 6$, and $s \leq 1$ for all such $G$. Nothing survives the condition $s = 1$, because it implies that $|G| = 4$ and $G \leq \text{GL}(2, 2) \cong \text{Sym}(3)$. 

57
6. Linear shift representations

6.3.2 Lemma. If \( N \triangleleft G \) then the shift action of \( G/N \) on \( B(G/N, U) \) extends naturally to a \( G \)-action under which \( B(G/N, U) \) is naturally isomorphic to a \( G \)-invariant subgroup of \( B(G, U) \).

Proof. The composite of the isomorphism \( B(K, U) \cong B(G/N, U) \) and inflation \( B(G/N, U) \rightarrow B(G, U) \) maps \( B(K, U) \) onto a \( G \)-invariant subgroup of \( B(G, U) \).

6.3.3 Corollary. If \( Z(G, U) \) (resp. \( B(G, U) \)) is a completely reducible \( G \)-module then each \( G/N \)-submodule of \( Z(G/N, U) \) (resp. \( B(G/N, U) \)) is completely reducible.

6.3.4 Corollary. If \( B(G, U) \) is irreducible then \( G \) is simple.

Order the elements of \( G \setminus \{1\} \) as \( g_1, \ldots, g_n \). Define \( \phi_i \in \text{Fun}(G, U) \) by \( \phi_i(g_j) = u^{\delta_{ij}} \). Clearly the \( \phi_i \)s form a basis of the \( \mathbb{F}_p \)-space \( \text{Fun}(G, U) \). The subspace \( \text{Hom}(G, U) \) of \( \text{Fun}(G, U) \) has a basis \( \{\phi^1_1 \cdots \phi^1_n, \ldots, \phi^s_1 \cdots \phi^n_s\} \) say, where \( 0 \leq \epsilon_{i,j} \leq p-1 \) for \( 1 \leq i \leq s \) and \( 1 \leq j \leq n \). Thus \( B(G, U) \) has presentation

\[
\langle \varphi_1, \ldots, \varphi_n \mid \varphi_i^p = [\varphi_i, \varphi_j] = 1, \quad 1 \leq i, j \leq n \\
\varphi_1^{\epsilon_{1,1}} \cdots \varphi_n^{\epsilon_{1,n}} = \cdots = \varphi_1^{\epsilon_{s,1}} \cdots \varphi_n^{\epsilon_{s,n}} = 1 \rangle
\]

where \( \varphi_i = \partial \phi_i \), from which we extract a basis \( B(G, U) = \{\partial \mu_1, \ldots, \partial \mu_m\} \) of \( B(G, U) \).

6.3.5 Lemma. For any \( a \in G \) and \( \phi \in \text{Fun}(G, U) \), \( (\partial \phi)a = \partial \overline{\phi} \) where \( \overline{\phi}(g) = \phi(ag)\phi(a)^{-1} \) for all \( g \in G \).

We find \( \Gamma_B(a) \in \text{GL}(n, p) \) for each \( a \in G \) with respect to \( B(G, U) \) as follows. Write \( \overline{\mu_i} \in \text{Fun}(G, U) \) in terms of the basis elements \( \phi_i \) of \( \text{Fun}(G, U) \). The relations in \( \text{Hom}(G, U) \) may be used to rewrite this expression in terms of the \( \mu_i \)s, say \( \mu_i^{n_1} \cdots \mu_i^{n_n} \). Then the \( i \)th row of the matrix in \( \text{GL}(n, p) \) representing \( \Gamma_B(a) \) with respect to the basis \( B(G, U) \) is the exponent vector \( \eta_{i,1} \eta_{i,2} \ldots \eta_{i,n} \).

6.3.6 Lemma. Suppose that \( \text{Hom}(G, U) \) is trivial. Row \( j \) of \( \Gamma_B(g_j) \) is all \(-1\)s; row \( i \) of \( \Gamma_B(g_j) \) for \( i \neq j \) has a single non-zero entry, 1, in column \( l \) where \( g_l = g_j^{-1} g_i \).
Proof. Here \( \mathcal{B}(G, U) = \{ \partial \phi_i \mid 1 \leq i \leq n \} \). By Lemma 6.3.5, \( \bar{\phi}_i(g_k) = \phi_i(g_j g_k) \)
if \( i \neq j \), whereas \( \bar{\phi}_i(g_k) = u^{-1} \) if \( i = j \). That is, \( \bar{\phi}_i = \phi_i \) where \( g_i = g_j g_k \) in the former case, and \( \bar{\phi}_i = \phi_1^{-1} \cdots \phi_n^{-1} \) in the latter.

The determination of irreducible shift representations \( \Gamma_B \) is now easily done. As in the proof of Proposition 6.3.1, we are assisted by the maximal degree of such representations for given \( |G| \).

6.3.7 Theorem. \( \mathcal{B}(G, U) \) is irreducible if and only if \( G \) is cyclic of prime order \( q \), where \( q \) divides \( p^n - 1 \) but not \( p^k - 1 \) for \( 1 \leq k \leq n - 1 \).

Proof. Suppose that \( \mathcal{B}(G, U) \) is irreducible. By Proposition 6.3.1, \( \text{Hom}(G, U) = 1 \). If \( \exp(G) = 2 \) then \( G \cong C_2 \) by Corollary 6.3.4. So choose \( g \in G \) such that \( |g| = t > 2 \). Assume that our ordering of the elements of \( G \) begins with \( g, g^2, \ldots, g^{t-1} \), and let \( \alpha \) be the unimodular vector with 1 in position \( t - 1 \) and 0 everywhere else. By Lemma 6.3.6 if \( t < |G| \) then \( \beta = \alpha + \alpha g + \cdots + \alpha g^{t-1} \) is non-zero; indeed \( \beta = (0, \ldots, 0, -1, \ldots, -1) \) where the first \(-1\) occurs in position \( t \). Clearly \( \beta \) is fixed by \( \langle g \rangle \). Thus \( |\beta G| \leq |G|/3 \), implying that \( \beta G \) spans a non-zero \( G \)-module of dimension less than \( n \); i.e., \( G \) is reducible, a contradiction. Therefore we must have that \( |G| = t \), i.e., \( G \) is cyclic, and by Corollary 6.3.4 \( t = q \) is prime. Lemma 6.2.6 completes the proof.

Our next goal is to show that \( \Gamma(G) \) is almost never completely reducible.

Let \( H \leq \text{GL}(d, \mathbb{K}) \) with underlying space \( V \). The dual module \( V^* \) of \( V \) is the \( d \)-dimensional \( \mathbb{K} \)-space \( \text{Hom}_{\mathbb{K}}(V, \mathbb{K}) \), where the action of \( H \) on \( V^* \) is defined by \( fg(v) = f(v g^{-1}) \) for \( f \in V^* \) and \( g \in H \). This action gives rise to a (‘contragredient’) representation \( \Lambda : H \to \text{GL}(d, \mathbb{K}) \). For a suitable choice of basis of \( V^* \), \( \Lambda(g) = (g^{-1})^\top \). Note that \( V^* \) is completely reducible if and only if \( V \) is, (see e.g., [2]).

6.3.8 Lemma. If \( \text{Hom}(G, U) = 1 \) and \( p \) divides \( |G| \) then \( \mathcal{B}(G, U)^* \) has non-trivial fixed points.

Proof. It is evident from Lemma 6.3.6 that \( \Lambda(G) = \Gamma_B(G)^\top \) fixes every element in the subspace spanned by the all 1s vector.

6.3.9 Lemma. Let \( V \) be a completely reducible \( H \)-module. Then \( V \) has non-trivial \( H \)-fixed points if and only if \( V^* \) does.
6. Linear shift representations

Proof. Let $W$ be the submodule of $V$ spanned by a non-trivial fixed point $w$. We have $V = W \oplus X$ for some $H$-submodule $X$. The assignment $aw + x \mapsto a$ for $a \in \mathbb{K}$, $x \in X$ then defines a non-trivial fixed point in $V^\ast$. Since $V^\ast$ is completely reducible and $V \cong V^{**}$, the lemma is proved.

For the rest of this section we assume that $p$ divides $|G|$.

6.3.10 Proposition. If $\text{Hom}(G, U) = 1$ then $B(G, U)$ is not completely reducible.

Proof. This is a consequence of Lemmas 5.2.1 (ii), 6.3.8 and 6.3.9.

6.3.11 Theorem. Suppose that $|G : G'| \geq 5$, or $G/G' \cong C_4$, or both $G/G' \cong C_3$ and $p \neq 3$. Then $\Gamma_B(G)$ is not completely reducible.

Proof. With the aid of Lemma 6.3.5 it may be confirmed that $|\Gamma_B(C_4)| \geq 2$ and $\Gamma_B(C_3) = 1$ if and only if $p = 3$. Therefore, by hypothesis and Lemma 6.1.2 $G$ (resp. $G/G'$) acts faithfully on $B(G, U)$ (resp. $B(G/G', U)$), except perhaps when $G/G' \cong C_4$. Now if $p$ does not divide $|G/G'|$ then we appeal to Proposition 6.3.10. Otherwise, Corollaries 6.2.5 and 6.3.3 give the result.

6.3.12 Theorem. Suppose that $\Gamma(G) \neq 1$, and either $p > 2$ or $G/G' \not\cong C_2, C_2^2$. Then $\Gamma(G)$ is not completely reducible.

Proof. The approach used to prove Theorem 6.3.11 carries over, mutatis mutandis (heeding Remark 6.1.3).

6.3.13 Remark. Cf. Corollary 6.2.10. Since $\Gamma(G)$ completely reducible implies $\Gamma_B(G)$ completely reducible, most of this result follows from Theorem 6.3.11 anyway.

Despite the major restrictions on $G$ imposed by Theorem 6.3.12, there does exist a non-trivial infinite family of groups of order divisible by $|U| = 2$ with completely reducible shift representations. These are the groups $G \cong K \times \langle h \mid h^2 = 1 \rangle$ where $K$ is odd order abelian and $h$ inverts $K$ elementwise. These groups include, for example, the dihedral groups of order $2m$ for odd $m$. We now embark on a proof of this claim.

6.3.14 Lemma. If $\text{Hom}(K, U) = 1$ then the kernel $W = \{ \partial \lambda \mid \lambda_K = 1 \}$ of the restriction map $B(G, U) \twoheadrightarrow B(K, U)$ is a $K$-submodule of $B(G, U)$.
6.3.15 Lemma. Let $U \cong C_2$, and suppose that $G \cong K \times \langle h \rangle$ where $|K|$ is odd and $|h| = 2$. Denote the $K$-module $B(K,U)$ naturally embedded in the $G$-module $V = B(G,U)$ via Lemma 6.3.14 by $N$. Then $V$ is the direct sum $N \oplus Nh$ of $K$-submodules.

Proof. First,

$$\dim_{F_2}(N) = \dim_{F_2}(Nh) = |K| - 1 = \frac{1}{2} \dim_{F_2}(V).$$

It remains to show that $N \cap Nh$ is trivial. To see this, we note by Lemma 6.3.5 that $(\partial \hat{\phi})h = \partial \mu$ where $\mu(g) = \hat{\phi}(hg)\hat{\phi}(h)$; and then $\partial \mu \in N$ implies that $\partial \mu = \partial(\mu_K)$, i.e., $\partial \mu = 1$ by Lemma 6.3.14.

For the remainder of the section we assume the hypotheses of Lemma 6.3.15.

6.3.16 Corollary. $V$ is a direct sum $\sum_{i=1}^r (N_i \oplus N_i h)$ of $G$-modules $N_i \oplus N_i h$ where $N_1, \ldots, N_r$ are irreducible $K$-submodules of $N$.

Proof. By Maschke’s theorem $N$ is a completely reducible $K$-module, say $N = \sum_{i=1}^r N_i$; then the rest of the assertion is clear from Lemma 6.3.15.

6.3.17 Lemma. Let $\pi$ be the canonical surjection of $N_i \oplus N_i h$ onto $N_i$, and suppose that $X$ is a proper non-zero $G$-submodule of $N_i \oplus N_i h$. Then $\pi$ restricted to $X$ is a $K$-module isomorphism of $X$ onto $N_i$.

Proof. Since $X \cap N_i h$ is a $K$-submodule of the irreducible $K$-module $N_i h$, either $X \cap N_i h = 0$ or $X \cap N_i h = N_i h$. The latter is ruled out because it implies that $N_i h \subseteq X$ and thus $N_i \subseteq X$, i.e., $X$ is not proper. Hence $\pi$ is an isomorphism of $X$ onto $\pi(X)$. Since $\pi(X)$ is a $K$-submodule of the irreducible $K$-module $N_i$, and $X \neq 0$, we have $X \cong N_i$.

We will now prove that $M := N_i \oplus N_i h$ is a completely reducible $G$-module, under the further assumption that $K$ is abelian, and that $h$ inverts every element in $K$ (we do not invoke this assumption until later). To do this, we suppose that $X$ is a proper non-zero $G$-submodule of $M$ and manufacture a $G$-submodule $Y$ such that $M = X \oplus Y$.

Select $v \in N_i$ and $g \in K$ such that $vg \neq v$. Since projection of $M$ onto $N_i h$ restricted to $X$ is a surjection, there exists $u \in N_i$ such that $u + vh \in X$. Define
6. Linear shift representations

Let \( Y \) be the \( \mathbb{F}_2 \)-linear span of \( \{ac \mid c \in K\} \) where \( a := ug + vgh \). Note that \( a \not\in X \): if \( a \in X \) then together with \( ug + vhg = (u + vh)g \in X \) and the fact that the projection \( \pi \) onto \( N_i \) is one-to-one, we would have \( vgh = vhg \), i.e., \( vg^2 = v \), so that \( vg = v \) because \( |K| \) is odd. Thus \( Y \) is a non-zero \( K \)-submodule of \( M \) not contained in \( X \).

6.3.18 Lemma. With the notation above, and further assuming that \( K \) is abelian, we have \( ah \in Y \). Consequently \( Y \) is a \( G \)-submodule of \( M \).

Proof. Since \( u \neq 0 \), the irreducible \( K \)-module \( N_i \) is spanned by the \( uc \) as \( c \) ranges over \( K \), so there exist scalars \( e_c \in \mathbb{F}_2 \) such that

\[
v = \sum_{c \in K} e_c uc.
\]  

(6.3.1)

Therefore

\[
v + \sum_{c \in K} e_c vc h = \sum_{c \in K} e_c (u + vh)c \in X.
\]

Also, because \( X \) is a \( G \)-module, \( uh + v = (u + vh)h \in X \). Since \( \pi \) is one-to-one, this means that \( uh = \sum_{c \in K} e_c vc h \), i.e.,

\[
u = \sum_{c \in K} e_c vc h^{-1}.
\]  

(6.3.2)

Hence

\[
ah = ugh + vg
\]

\[
= \left( \sum_{c \in K} e_c vc h \right) + vg \quad \text{by (6.3.2)}
\]

\[
= \left( \sum_{c \in K} e_c vghc \right) + \sum_{c \in K} e_c ugc \quad \text{by (6.3.1) and using that } K \text{ is abelian}
\]

\[
= \sum_{c \in K} e_c (vgh + ug)c
\]

\[
= \sum_{c \in K} e_c ac \in Y
\]

as desired. \( \diamond \)

Let \( d \) be the \( \mathbb{F}_2 \)-dimension of \( N_i \), so that \( Y \) and \( X \) have this common dimension \( d \) too, by Lemmas 6.3.17 and 6.3.18. For exactly the same reasons, \( Y \cap X \)
has dimension $d$ if it is non-zero: but if this were so then $Y$ would equal $X$, contradicting $Y \not\leq X$. Thus $X \cap Y = 0$, and so $M = X + Y = X \oplus Y$ by dimensions.

In summary, we have shown that any proper non-zero $G$-submodule of $M = N_i \oplus N_i h$ is complemented in $M$. In other words, $M$ is a completely reducible $G$-module. Since $V$ is a direct sum of these completely reducible $G$-modules, we finally obtain

**6.3.19 Theorem.** Suppose that $G = K \rtimes \langle h \rangle$ where $K$ is odd order abelian, and the involution $h$ inverts every element of $K$. Then $B(G, C_2)$ is a completely reducible $G$-module.

**6.3.20 Lemma.** Assume the hypotheses of Theorem 6.3.19. Then $K = G'$.

*Proof.* For any $k \in K$, $k^{-1} h^{-1} k h = k^{-2}$ and thus for all $k \in K$, $k^2 \in G'$. As $|K|$ is odd, this gives the result. ♦

**6.3.21 Theorem.** Assume the hypotheses of Theorem 6.3.19. Then $Z(G, C_2)$ is a completely reducible $G$-module.

*Proof.* Here $Z(G, C_2) = B(G, C_2) \oplus \text{Fix}(G)$ where $\text{Fix}(G)$ is 1-dimensional. ♦

### 6.4. Orbits in $B(G, U)$

Shift orbits in modules are discussed in [43, Section 8.5], based on LeBel's observation that the shift action on coboundaries is captured by the $G$-module structure of a group ring $R[G]$. We briefly outline his approach, which is quite different from our own. See also [57, Section 2].

Let $R$ be a commutative ring. Denote by $RG^{(0)}$ the standard left $R[G]$-module with underlying additive group $R[G]$, with left $G$-action given by

$$g \cdot \left( \sum_{x \in G} a(x) x \right) = \sum_{x \in G} a(x)(gx) = \sum_{x \in G} a(g^{-1}x)x, \quad \forall g \in G, \quad \sum_{x \in G} a(x)x \in R[G].$$

Then define $RG^{(j)}$ to be the quotient of $RG^{(j-1)}$ by its submodule of $G$-fixed points. LeBel shows that $RG^{(2)}$ and $B(G, R)$ are isomorphic, and that the induced left $G$-action on $B(G, R)$ is precisely the shift action, and thus the orbits under this action are the shift orbits. This is a more general approach in
6. Linear shift representations

the sense that it is useful for studying \( RG^{(j)} \) for any \( j \); however, it is limited to the study of \( B(G, R) \) when \( j = 2 \). Some data on the shift orbits in \( B(G, R) \) is given in [43, Example 8.5.2], for \( G \) an elementary abelian 2-group and \( R \cong C_2 \). We verify and expand upon these results to all of \( Z(G, R) \); see Section 6.6.3.

Let \( G = \langle g \rangle \times \langle h \rangle \cong D_p \), the dihedral group of order \( 2p \), where \( |g| = p \) for an odd prime \( p \). Also let \( U = \langle u \rangle \cong C_2 \). This is an interesting test case satisfying the hypotheses of Theorem 6.3.19.

6.4.1 Lemma. Non-zero orbits in \( B(G, U) \) have length \( p \) or \( 2p \).

Proof. We have \( \text{Fix}(G) \cong C_2 \) by Corollary 5.2.5 and the single non-trivial multiplicative cocycle is inflated from \( \text{Ext}(G/G', U) \), so is not a coboundary. Hence all non-zero orbits in \( B(G, U) \) have length greater than 1. If there were an orbit \( \{ u, v \} \) of length 2 then \( u + v \) would be a non-zero fixed point.

6.4.2 Lemma. \( B(G, U) \) contains at least one orbit of length \( p \), and at least one non-zero submodule of dimension less than \( p \).

Proof. By Lemma 6.4.1 there must be an orbit of length \( p \), say \( \{ u_0, \ldots, u_{p-1} \} \). Since \( u_0 + \cdots + u_{p-1} \) will then be fixed by every element in \( G \), the \( u_i \) are linearly dependent, proving the latter claim.

6.4.3 Lemma. In each orbit of length \( p \) in \( B(G, U) \), \( h \) fixes precisely one element.

Proof. Let \( u_0, \ldots, u_{p-1} \) be the \( p \) elements in the orbit, where \( u_i g = u_{i+1} \) reading subscripts modulo \( p \). Since \( h \) is a transposition, it fixes at least one of these elements. Relabeling if necessary, assume that \( h \) fixes \( u_{(p-1)/2} \). Since \( u_{(p-1)/2} h = u_{(p-1)/2} h g^{-1} \), we then get \( u_{i+(p-1)/2} h = u_{-i+(p-1)/2} \). Thus \( u_i h = u_{p-i-1} \) for \( 0 \leq i \leq p-1 \).

6.4.4 Lemma. \( \Gamma_B(h) \) has exactly \( 2^{p-1} \) fixed points in \( B(G, U) \).

Proof. Let \( \phi_x \) for \( x \in X := G \setminus \{ 1 \} \) be the characteristic function that maps \( x \) to \( u \) and \( y \neq x \) to 1. Since \( \text{Hom}(G, U) \cong C_2 \) is generated by \( \phi_{hg} \cdots \phi_h \), \( B(G, U) \) has basis

\[
\partial \phi_g, \partial \phi_g^2, \ldots, \partial \phi_g^{p-1}, \partial \phi_{hg}^{-1}, \partial \phi_{hg^2}, \ldots, \partial \phi_{hg^{p-1}}.
\]

(6.4.1)
Using Lemma 6.3.5 we check that \((\partial \phi_x)h = \partial \phi_{hx}\). Thus \(\Gamma_B(h) \in \text{GL}(2p - 2, 2)\) with respect to the basis (6.4.1) of \(B(G, U)\) is a symmetric permutation matrix with zero main diagonal. So \(\Gamma_B(h)\) fixes any symmetric vector \(v\), i.e., \(v_i = v_{2p-1-i}\) for \(1 \leq i \leq p - 1\).

\[\Diamond\]

**6.4.5 Corollary.** There are precisely \(2^{p-1} - 1\) orbits of length \(p\) in \(B(G, U)\).

**Proof.** Apply Lemmas 6.4.3 and 6.4.4

\[\Diamond\]

For \(G \cong D_p\) and \(U \cong C_2\), we have found that the orbit structure of \(B(G, U)\) is as follows:

- one trivial fixed point,
- no orbits of length 2,
- \(p(2^{p-1} - 1)\) elements in orbits of length \(p\),
- \(2^{2p-2} - p(2^{p-1} - 1) - 1\) elements in orbits of length \(2p\).

An advantage of using the shift representation approach is that it enables us to analyze the orbit structure of any \(B(G, U)\) where \(G\) and \(U\) are of manageably small order. Sample computational results are given below.

### 6.5. Computing with shift representations

In this section we briefly describe the computation of shift representations of \(G\), principally in the case of an elementary abelian coefficient group. In contrast to previously available machinery (cf. [36, Section 8.5]), we have implemented procedures to compute in the full cocycle space \(Z(G, U)\), rather than just the coboundary subspace \(B(G, U)\).

We discussed computing \(B(G, U)\) in Section 6.3 (see the paragraph before Lemma 6.3.5). To extend to \(Z(G, U)\), we first find representative cocycles \(\psi_1, \ldots, \psi_m\) for the elements of a basis of \(H(G, U)\), as per [36, Section 2]. Let \(\mathcal{B} = \{\partial \mu_1, \ldots, \partial \mu_n\}\) be a basis of \(B(G, U)\). Then \(\psi_1, \ldots, \psi_m, \partial \mu_1, \ldots, \partial \mu_n\) is a basis of \(Z(G, U)\). If \(\psi_ia = \psi_i\partial \phi\) for \(\partial \phi = \mu_1^{n_1} \cdots \mu_n^{n_n}\) then we get an \((m + n) \times (m + n)\) matrix of the form

\[
\Gamma(a) = \begin{bmatrix}
I_m & A \\
0 & \Gamma_B(a)
\end{bmatrix}
\]
6. Linear shift representations

where $A$ is an $m \times n$ matrix, in which the $i$th row is the exponent vector

$$\eta_{i,1} \ \eta_{i,2} \ \ldots \ \eta_{i,n}$$

corresponding to the coboundary $\partial \phi$ such that $\psi \cdot a = \psi \cdot \partial \phi$.

These procedures have been implemented in MAGMA by the author, Dane Flannery, and Eamonn O’Brien. We remark that this work involved fixing a bug in the MAGMA intrinsic used to compute Ext($G/G'$, $U$); see [9].

The MAGMA intrinsic for computing Hom($G$, $U$) assumes that $G$ is abelian. Now inflation $\text{inf} : \text{Hom}(G/G', U) \rightarrow \text{Hom}(G, U)$ is an isomorphism. We also have a procedure to compute inflation on second cohomology, which is readily modified to compute inflation on first cohomology. By the preceding comments, this furnishes in turn a procedure for computing Hom($G$, $U$) for any finite group $G$.

6.6. Further computational results

Using our MAGMA implementations of the algorithms from Section 6.5, we have collected exhaustive data on shift representations of $G$ on $B(G, C_p)$ and $Z(G, C_p)$. The data suggests possible avenues of further research on fixed points, complete reducibility, and orbit structure.

Assume for the rest of this section that $|U| = p$ is prime and divides $|G|$ unless stated otherwise.

6.6.1. Fixed points

Let $r$ be the rank of the Sylow $p$-subgroup of $G/G'$, and suppose that Fix$_B(G) \cong U^s$. By Remark 5.2.3 we have a lower bound $l_s$ for $s$, given by $l_s = \left(\frac{r+1}{2}\right)$ and $l_s = \left(\frac{r+1}{2}\right) - k$ in cases (i), (ii) respectively of Theorem 5.2.9. There are certainly groups $G$ where $s > l_s$. Some examples drawn from the MAGMA SmallGroups library, are given in Table 6.6.1 using the internal numbering from the library, ($Q_m$ is the dicyclic group of order $m$).

In Section 5.2.1 we explained how $s$ can be greater than $l_s$. We hope to achieve a full characterization of the groups where $s = l_s$. We would also like to be able to calculate the true value for $s$ for any group, without relying on a complete search for fixed points.
### Table 6.6.1. Dimensions of fixed coboundary spaces

<table>
<thead>
<tr>
<th>$G$</th>
<th>$\text{SmallGroups library}$</th>
<th>$p$</th>
<th>$l_s$</th>
<th>$s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_8$</td>
<td>(16,7)</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$C_3 \rtimes Q_8$</td>
<td>(24,4)</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$C_2^2 \rtimes C_2$</td>
<td>(32,27)</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>$(C_3 \times C_3) \rtimes C_3$</td>
<td>(27,3)</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$(C_9 \times C_3) \rtimes C_3$</td>
<td>(81,3)</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$C_5 \rtimes (C_5 \times C_5)$</td>
<td>(125,3)</td>
<td>5</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

### 6.6.2. Completely reducible representations

By Theorem 6.3.12, $G$ rarely has a completely reducible shift representation $\Gamma$, but Theorem 6.3.21 demonstrates their existence when restrictions are imposed on $G$. The results of computational searches suggest that these restrictions are both necessary and sufficient. That is, we have the following conjecture.

**6.6.1 Conjecture.** $\Gamma(G) \neq 1$ is completely reducible if and only if $|G : G'| = p = 2$ and $G'$ is abelian of odd order.

Regarding $\Gamma_B$, that the other possibility, $G/G' \cong U \cong C_3$, is unaccounted for by Theorem 6.3.11 prompted more searches. The evidence leads to a very similar conjecture (see Corollary 6.2.10).

**6.6.2 Conjecture.** Let $U$ be cyclic of order 3. Then $\Gamma_B$ is completely reducible if and only if $|G : G'| = 3$ and $G'$ is abelian of order not divisible by 3.

These conjectures are supported by MAGMA computations for all $G$ of order at most 150.

### 6.6.3. Orbit structure

In [57], Section 4, shift orbits in $B(G,U)$ are enumerated for small elementary abelian and cyclic $G$. We have confirmed those listings, and add new examples in the full cocycle space for non-abelian $G$ in the tables below. The first row gives the length of an orbit and the second row gives the number of orbits of that length.

<table>
<thead>
<tr>
<th>$B(C_2^3,C_3)$</th>
<th>$Z(C_2^3,C_3)$</th>
<th>$Z(C_9,C_3)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 3 9</td>
<td>1 3 9</td>
<td>1 3 9</td>
</tr>
<tr>
<td>27 0 78</td>
<td>81 216 2106</td>
<td>3 8 726</td>
</tr>
</tbody>
</table>
6. Linear shift representations

<table>
<thead>
<tr>
<th>$B(C_2^3 \times C_3, C_3)$</th>
<th>1 2 3 4</th>
<th>6</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3 15 24 12</td>
<td>360</td>
<td>4728</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$B(D_4, C_2)$</th>
<th>1 2 4 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4 4 1 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Z(D_4, C_2)$</th>
<th>1 2 4 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>16 16 36 8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Z(D_8, C_2)$</th>
<th>1 2 4 8 16</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>16 16 100 968 3584</td>
</tr>
</tbody>
</table>

6.6.4. Orthogonality

First, we remark that in searching for orthogonal cocycles we may take $U \cong C_p$. For if $\psi \in Z(G, U)$ is orthogonal then the restriction $\psi_j$ to each summand $Z(G, C_i_j)$ is orthogonal. (The converse need not be true. Horadam and LeBel [55, Proposition 3.2] show that it is also necessary for every non-trivial $\mathbb{F}_p$-linear combination of the $\psi_j$ to be orthogonal in $Z(G, U)$). Thus, while stipulating that $U \cong C_p$ does not seriously constrain the abstract study of shift representations, it may complicate the picture with regard to orthogonality. However, if we discover $t$ orthogonal cocycles in $Z(G, C_i_1)$, then we merely test a space of cocycles mapping into $U = C_i_1 \times \cdots \times C_i_r$ of size $t^r$ to locate all orthogonal elements of $Z(G, U)$. In the case $|U| = p$ and $G$ is an elementary abelian $p$-group, existence is known; see Remark 5.2.10.

We now present the results of searches for orthogonal cocycles (cf. [56, 57]). The linear group setting enables us to calculate $G$-orbits efficiently, even if their number grows exponentially with $|G|$. We test a single element from each orbit for orthogonality. Tables 6.6.2 and 6.6.3 display the total number $n$ of orthogonal cocycles (i.e., cocyclic Hadamard matrices) for a selection of small abelian and non-abelian groups $G$ with $|U| = 2$. In Table 6.6.4 we state the number of orthogonal cocycles detected for various groups $G$ with $|U| = 3$.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$C_2 \times C_4$</th>
<th>$C_2^2 \times C_3$</th>
<th>$C_2^2 \times C_4$</th>
<th>$C_4 \times C_4$</th>
<th>$C_2^3 \times C_5$</th>
<th>$C_2 \times C_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>16</td>
<td>24</td>
<td>1984</td>
<td>192</td>
<td>120</td>
<td>96</td>
</tr>
</tbody>
</table>

Table 6.6.2. $G$ abelian, $|U| = 2$

We find no orthogonal cocycles when $p = 5$ and $|G| \in \{10, 15, 20\}$; nor do we find any when $p = 7$ and $|G| \in \{14, 21\}$ (cf. Section 7.4). Orthogonal cocycles in $Z(C_p, C_p)$ are already accounted for by Horadam’s result (Remark 5.2.10).
Table 6.6.3. $G$ non-abelian, $|U| = 2$

<table>
<thead>
<tr>
<th>$G$</th>
<th>$D_4$</th>
<th>$Q_8$</th>
<th>$D_6$</th>
<th>$\text{Alt}(4)$</th>
<th>$D_8$</th>
<th>$Q_{16}$</th>
<th>$D_{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>32</td>
<td>0</td>
<td>72</td>
<td>96</td>
<td>768</td>
<td>128</td>
<td>2200</td>
</tr>
</tbody>
</table>

Table 6.6.4. $|U| = 3$

<table>
<thead>
<tr>
<th>$G$</th>
<th>$C_6$</th>
<th>$D_3$</th>
<th>$C_9$</th>
<th>$C_2^2$</th>
<th>$C_{12}$</th>
<th>$C_3 \rtimes C_4$</th>
<th>$\text{Alt}(4)$</th>
<th>$D_6$</th>
<th>$C_2^2 \times C_3$</th>
<th>$C_{15}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>144</td>
<td>0</td>
<td>288</td>
<td>48</td>
<td>0</td>
<td>96</td>
<td>0</td>
</tr>
</tbody>
</table>

All cocyclic Hadamard matrices of orders less than 40 were classified by Ó Catháin and Röder [62]. Tables 6.6.2 and 6.6.3 agree with the data in that paper. In the next chapter we make use of this data in our classification of cocyclic Butson Hadamard matrices.

Many cocycles in our tables correspond to Hadamard equivalent matrices. For example, it is known that there is a unique Hadamard matrix of order 12 up to equivalence; but there are exactly 192 orthogonal cocycles when $|G| = 12$. Thus $\text{Alt}(4)$, $D_6$ and $C_2^2 \times C_3$ are all indexing groups of the same Hadamard matrix of order 12.

We observe that most orthogonal cocycles tend to be in orbits of maximal length $|G|$. When $U \cong C_2$ and $G \cong C_2^2 \times C_m$ for $m \in \{3, 5\}$, all orthogonal cocycles are in orbits of length $|G|$, and are of the form $\psi_1 \cdots \psi_m \partial \phi$ where $\{[\psi_1], \ldots, [\psi_m]\}$ is a basis of $H(G, U)$. This is consistent with a conjecture of Baliga and Horadam [5]. The orthogonal cocycles for $G \cong D_6$ or $D_{10}$ also lie in maximal-length orbits. In light of [57, Theorem 12], this is perhaps not surprising; although that result requires $G$ to be a $p$-group.

As we discuss in the next chapter, we have used our algorithms to find several previously unknown Butson Hadamard matrices. However, calculating shift orbits remains a difficult task. Thus complete orbit-by-orbit searches for orthogonal cocycles are impossible if $G$ is large enough. But selective searches are still feasible. For instance, we can easily find the orthogonal cocycles in $Z(C_p^k, C_p)$, because we know that they are fixed under the shift action (and of course we can generate them via Remark 6.2.10). With a better understanding of the shift orbit structure, in particular of those orbits containing orthogonal cocycles, it would be possible to develop our machinery further to carry out targeted searches when $|G|$ is large.
Part III.

Cocyclic Butson Hadamard matrices
7. Classification of small cocyclic BH\((n, p)\)s

In this chapter we completely classify, up to equivalence, the Butson Hadamard matrices of order \(n\) over \(p\)th roots of unity, for any odd prime \(p\) and \(np \leq 100\). Much of this chapter appears in [31] as joint work with Dane Flannery and Padraig Ó Catháin.

The classification was motivated by the need to augment known libraries of complex Hadamard matrices. Indeed, we found several matrices that were not equivalent to any of those previously listed at the main online library [11].

We rely on the coincidence between BH\((n, p)\) and generalized Hadamard matrices over cyclic groups of prime order. This relationship allows us to apply some of the shift representation machinery from Chapter 6. We also extend Magma [8] and GAP [37] procedures implemented previously for 2-cohomology and relative difference sets [36, 62, 64] to construct the matrices and sort them into equivalence classes. A new equivalence testing algorithm is described in Section 7.1.1. Non-existence results for cocyclic generalized Hadamard matrices and Butson Hadamard matrices are proved in Section 7.4. Finally, the classification is laid out in Section 7.5. Further details, such as an explicit list of matrices representing the different equivalence classes together with information about their automorphism groups and indexing groups, are available at [32].

Throughout this chapter, \(p\) is a prime and \(G, K\) are finite groups. We write \(\zeta_k\) for \(e^{2\pi i/k}\).
7. Classification of small cocyclic BH\((n,p)\)s

7.1. Equivalence of generalized Hadamard and Butson Hadamard matrices

In this section we provide a new algorithm to decide equivalence of Butson Hadamard matrices. The problem is reduced to deciding graph isomorphism, which we carry out using \textit{Nauty} \cite{Nauty}; and subgroup conjugacy and intersection problems, routines for which are available in \textsc{Magma}.

We recall notions of \(\Lambda\)-equivalence in the context of generalized Hadamard and Butson Hadamard matrices. Let \(X, Y\) be \(\text{GH}(n,K)\)s. We say that \(X\) and \(Y\) are equivalent if \(MXN = Y\) for monomial matrices \(M, N\) with non-zero entries in \(K\). If \(X, Y\) are \(\text{BH}(n,k)\)s then they are equivalent if \(MXN = Y\) for monomials \(M, N\) with non-zero entries from \(\langle \zeta_k \rangle\). As usual, equivalence in either situation is denoted \(X \approx Y\), and permutation equivalence is denoted \(X \sim Y\).

If \(H\) is a normalized \(\text{GH}(n,K)\) then \(H\) is row-balanced: each element of \(K\) appears with the same frequency, i.e., \(n/|K|\), in each non-initial row. Similarly, \(H\) is column-balanced. Unless \(k\) is prime, neither property is necessarily held by a normalized \(\text{BH}(n,k)\).

7.1.1. Automorphism groups, the expanded design, and the associated design

We further recall some definitions specifically in the context of Butson Hadamard matrices. The direct product \(\text{Mon}(n,\langle \zeta_k \rangle) \times \text{Mon}(n,\langle \zeta_t \rangle)\) of monomial matrix groups acts on the (presumably non-empty) set of \(\text{BH}(n,k)\)s via \((M,N)H = MHN^*\). The orbit of \(H\) is its equivalence class; the stabilizer is its full automorphism group \(\text{Aut}(H)\). The permutation automorphism group \(\text{PAut}(H) \leq \text{Aut}(H)\) is comprised of all \((P,Q) \in \text{Aut}(H)\) such that \(P, Q\) are permutation matrices.

The full automorphism group \(\text{Aut}(H)\) acts on the expanded design \(\mathcal{E}_H = [\zeta_k \zeta_t^*]^*\) via the isomorphism \(\Theta\) of \(\text{Aut}(H)\) onto \(\text{PAut}(\mathcal{E}_H)\) described in Section 2.3.1 (see also \cite{1998}*Theorem 9.6.12\).

7.1.1 Proposition. \textbf{If} \(H_1\) \textbf{and} \(H_2\) \textbf{are equivalent} \(\text{BH}(n,k)\)s \textbf{then} \(\mathcal{E}_{H_1} \sim \mathcal{E}_{H_2}\); \textbf{therefore} \(\text{Perm}(\mathcal{E}_{H_1})\) \textbf{and} \(\text{Perm}(\mathcal{E}_{H_2})\) \textbf{are isomorphic, as conjugate subgroups of} \(\text{Perm}(nk)^2\).
Proof. See [21, Corollary 9.6.10].

A converse of Proposition 7.1.1 also holds, which we might use as a criterion to distinguish Butson Hadamard matrices. For computational purposes, it is preferable to work with the associated design $A_H$ obtained from $E_H$ by setting its non-identity entries to zero. Then we also need an analog of Proposition 7.1.1 for the associated design. Denote the image of $\text{Mon}(n, \langle \zeta_k \rangle)^2$ under $\Theta$ by $M(n, k)$.

7.1.2 Proposition. Let $H_1, H_2$ be BH($n, k$)s. We have $H_1 \approx H_2$ if and only if $A_{H_1} = XA_{H_2}Y^\top$ for some $(X, Y) \in M(n, k)$.

Proof. Suppose that $\theta(1)(P)A_{H_2}\theta(2)(Q)^\top = A_{H_1}$, and write $E_{H_i} = \sum_{r \in \langle \zeta_k \rangle} rH_{i,r}$ (so $A_{H_i} = H_{i,1}$). By Theorem 9.6.7 and Lemma 9.8.3 of [21],

$$H_{1,r} = \theta(1)(P)H_{2,r}\theta(2)(Q)^\top.$$

Therefore $E_{H_1} = E_{PH_2Q^*}$ by [21, Lemma 9.6.8]. This implies that $H_1 = PH_2Q^*$. ♦

We also use the following simple fact.

7.1.3 Lemma. Let $A, B$ be subgroups and $x, y$ be elements of a group $G$. Then either $xA \cap yB = \emptyset$, or $xA \cap yB = g(A \cap B)$ for some $g \in G$.

Proof. Suppose there is $g \in xA \cap yB$. Then since $g \in xA$ if and only if $x \in gA$, we have $xA = gA$. Similarly $yB = gB$. Thus $xA \cap yB = gA \cap gB = g(A \cap B)$. ♦

7.1.2. The equivalence testing algorithm

We now present our algorithm to decide equivalence of Butson Hadamard matrices $H_1$ and $H_2$ of order $n$ and phase $k$.

1. Compute $G_1 = \text{PAut}(A_{H_1})$ with Nauty.

2. Attempt to find $\sigma \in \text{Perm}(nk)^2$ such that $\sigma A_{H_1} = A_{H_2}$.

   If no such $\sigma$ exists then return false.

3. Compute $U = G_1 \cap M(n, k)$ and a transversal $T$ for $U$ in $G_1$.

4. If there exists $t \in T$ such that $\sigma t \in M(n, k)$ then return true;

   else return false.

75
7. Classification of small cocyclic BH\((n,p)\)s

If \(H_1 \approx H_2\) then \(\sigma G_1 \cap M(n,k) \neq \emptyset\) by Proposition \[7.1.2\], so by Lemma \[7.1.3\] we must find a \(t\) as in step 4. A report of \textit{false} is then correct by Proposition \[7.1.2\]; a report of \textit{true} is clearly correct. Note also that if the algorithm returns \textit{true} then we find an element \(\Theta^{-1}(\sigma t)\) mapping \(H_1\) to \(H_2\).

The main bottleneck is step 1, although it is feasible for graphs on several hundred vertices. Equivalence testing is therefore practicable for most BH\((n,k)\) that have been considered in the literature.

7.2. Central relative difference sets

The correspondence between cocyclic Butson Hadamard matrices and central relative difference sets is given in the following theorem (cf. Theorem \[2.7.1\]).

7.2.1 Theorem. There exists a cocyclic BH\((n,p)\) with cocycle \(\psi\) if and only if there is a relative difference set in \(E_\psi\) with parameters \((n,p,n,n/p)\) and central forbidden subgroup \(\langle (1, \zeta_p) \rangle\).

Proof. See \[21, Corollary 15.4.2\] or \[60, Theorem 4.1\].

We explain one direction of the correspondence in Theorem \[7.2.1\]. Let \(E\) be a central extension of \(U \cong C_p\) by \(G\), say \(\iota : U \rightarrow Z(E)\) is an embedding and \(\pi : E \rightarrow G\) is an epimorphism with kernel \(\iota(U)\). Suppose that \(R = \{d_1 = 1, d_2, \ldots, d_n\} \subseteq E\) is an \((n,p,n,n/p)\)-relative difference set with forbidden subgroup \(U\); i.e., the multiset of quotients \(d_i d_j^{-1}\) for \(j \neq i\) contains each element of \(E \setminus \iota(U)\) exactly \(n/p\) times, and contains no element of \(\iota(U)\). Since \(R\) is a transversal for the cosets of \(\iota(U)\) in \(E\), we have \(G = \{g_i := \pi(d_i) : 1 \leq i \leq n\}\). Put \(\tau(g_i) = d_i\), and define \(\psi_\tau \in Z(G,U)\) by \(\psi_\tau(x,y) = \tau(x)\tau(y)\tau(xy)^{-1}\). Then \([\psi_\tau(x,y)]_{x,y \in G}\) is balanced, hence a BH\((n,p)\).

7.3. Cocyclic Butson Hadamard matrices

7.3.1 Theorem. Let \(G, U\) be finite groups with \(U\) abelian and \(n = |G|\) divisible by \(|U|\). Let \(\psi \in Z(G,U)\) and \(M = [\psi(x,y)]_{x,y \in G}\). Then \(M\) is a GH\((n,U)\) if and only if it is row-balanced. In this case \(M\) is column-balanced too.

Proof. The first claim follows from \[43, Lemma 6.6\], which generalizes a phenomenon first observed for cocyclic real Hadamard matrices (see, e.g., \[21, Theorem 16.2.1\]).

\[76\]
In light of Theorem 7.3.1 our classification of cocyclic BH\((n, p)\) begins by searching for orthogonal cocycles in \(Z(G, C_p)\) for \(p|G| \leq 100\).

In general, a cocyclic BH\((n, k)\) need not be balanced.

7.3.2 Lemma. Let \(\psi \in Z(G, \langle \zeta_k \rangle)\). Then \(H = [\psi(x, y)]_{x,y \in G}\) is a BH\((n, k)\) if and only if every non-initial row sum of \(H\) is zero (in \(C\)).

A special kind of Butson Hadamard matrix that exists at every order \(n\) is the so-called Fourier matrix, viz. \([\zeta_n^{rs}]_{0 \leq r, s \leq n-1}\).

7.3.3 Lemma. The Fourier matrix of order \(n\) is a cocyclic BH\((n, n)\) with indexing group \(C_n\). It is equivalent to a group-developed matrix if and only if \(n\) is odd.

7.3.4 Proposition ([11]). Every circulant BH\((p, p)\) is equivalent to the Fourier matrix of order \(p\).

7.3.5 Proposition. For \(p \leq 17\), the Fourier matrix of order \(p\) is the unique BH\((p, p)\) up to equivalence. It is group-developed over \(C_p\), i.e., equivalent to a circulant.

\textit{Proof.} See [42, Theorem 1.1].

7.4. Non-existence of generalized Hadamard matrices

Certain number-theoretic conditions exclude various odd \(n\) as the order of a generalized Hadamard matrix; see, e.g., [15, 18, 72]. The main general result of this kind that we need is due to de Launey [18].

7.4.1 Theorem. Let \(K\) be abelian, and \(r, n\) be odd, where \(r\) is a prime dividing \(|K|\). If a GH\((n, K)\) exists then every integer \(m \equiv 0 \mod r\) that divides the square-free part of \(n\) has odd multiplicative order modulo \(r\).

7.4.2 Remark. Thus, BH\((n, p)\) do not exist for \((n, p) \in \{(15, 3), (33, 3), (45, 3), (15, 5), (35, 5), (21, 7), (35, 7)\}\).
7. Classification of small cocyclic BH\((n,p)\)s

7.4.1. Non-existence of cocyclic Butson Hadamard matrices

As we expect, there are restrictions on the order of a group-developed Butson Hadamard matrix.

7.4.3 Lemma. Set \( r_j = \text{Re}(\zeta_k^j) \) and \( s_j = \text{Im}(\zeta_k^j) \). A BH\((n,k)\) with constant row and column sums exists only if there are \( x_0, \ldots, x_{k-1} \in \{0,1,\ldots,n\} \) satisfying

\[
\left( \sum_{j=0}^{k-1} r_j x_j \right)^2 + \left( \sum_{j=0}^{k-1} s_j x_j \right)^2 = n \tag{7.4.1}
\]

and \( \sum_{j=0}^{k-1} x_j = n \).

**Proof.** Let \( H \) be a BH\((n,k)\) with every row and column summing to \( s \). There are non-negative integers \( x_0, \ldots, x_{k-1} \) such that \( s = \sum_{j=0}^{k-1} x_j \zeta_k^j = a + bi \), say. We have \( J_n = \frac{1}{n} I_n H H^* = \frac{a}{n} J_n H^* = \frac{a}{n} I_n \). Hence \( n = a^2 + b^2 \). ♦

When \( k = p \) is prime, we can impose upper bounds on the values of the \( x_i \) in Lemma 7.4.3, by taking advantage of the orthogonality of \( H \).

7.4.4 Lemma. Let \( H \) be a BH\((n,p)\) and let \( x_0, \ldots, x_{p-1} \) satisfy the properties of Lemma 7.4.3. Then

\[
\sum_{k=0}^{p-1} x_k^2 - x_k = \frac{n}{p}(n-1).
\]

**Proof.** Since \( p \) is prime, each \( p \)th root of unity arises equally often \( (n/p \text{ times}) \) as a quotient \( H_{i,l} H_{j,l}^{-1} \) for any fixed \( i,j, i \neq j \) and \( 1 \leq l \leq n \). In particular \( H_{i,l} H_{j,l}^{-1} = 1 \) exactly \( n/p \) times for \( i \neq j \) and \( 1 \leq l \leq p \). So as \( l \) runs from 1 to \( n \) and \( j \) runs from 2 to \( n \), \( H_{i,l} H_{j,l}^{-1} = 1 \) exactly \( \frac{n}{p}(n-1) \) times. In each of the \( x_k \) columns beginning with \( \zeta_p^k \), the entry \( \zeta_p^k \) appears \( x_k - 1 \) times in subsequent rows. The result follows. ♦

7.4.5 Example. In a BH\((21,7)\), the maximal value of \( x_k \) for \( 0 \leq k \leq 6 \) is 8. Otherwise, if \( x_k \geq 9 \), we get \( x_k^2 - x_k \geq 72 > 60 \).

Now suppose that each element of \( \langle \zeta_p \rangle \) appears equally often as a quotient \( H_{i,l} H_{j,l}^{-1} \) for \( i \neq j \) where \( l \) runs from 1 to \( n \). Thus in any pair of distinct rows \( i \) and \( j \) and for any \( b \in \{0, \ldots, p-1\} \), as \( l \) runs from 1 to \( n \), we have \( H_{i,l} H_{j,l}^{-1} = \zeta_p^a \zeta_p^{-(a-b)} = \zeta_p^b \) for some \( a \in \{0, \ldots, p-1\} \) precisely \( n/p \) times.
7.4.6 Corollary. Assume the hypotheses of Lemma 7.4.4. Then

\[ p - 1 \sum_{i=0}^{p-1} x_{i+j} = \frac{n}{p} (n - 1) \]

for all \(1 \leq j \leq p - 1\), where subscripts are read modulo \(p\).

Proof. We proceed as in the proof of Lemma 7.4.4, but in this case taking the \(x_i\) columns beginning with \(\zeta_p^i\), and noting that \(\zeta_p^{i+j}\) appears in each column \(x_{i+j}\) times. ♦

7.4.7 Remark. If \(k = 2\) then (7.4.1) just gives that \(n\) must be a perfect square, which is well-known. If \(k = 4\) then \(n\) is the sum of two integer squares. One readily computes other excluded orders, by Lemma 7.4.4 and Corollary 7.4.6; e.g., the following values of \(n\) and \(p\) are ruled out for a group-developed BH\((n, p)\).

(i) \(p = 3 < n \leq 100\): 6, 15, 18, 24, 30, 33, 42, 45, 51, 54, 60, 66, 69, 72, 78, 87, 90, 96, 99.

(ii) \(p = 5 < n \leq 75\): 10, 15, 30, 35, 40, 50, 60, 65, 70, 75.

(iii) \(p = 7, n \leq 42\): 21, 35, 42.

Some of these orders are also ruled out by general results (see Remark 7.4.2).

7.4.8 Lemma. Let \(k = p^t\) and \(n = p^rm\) where \(p \nmid m\). Suppose that \(H\) is a cocyclic BH\((n, k)\) with indexing group \(G\) such that \(G/G'\) has a cyclic subgroup of order \(p^r\). Then any cocycle \(\psi \in I(G, C_k)\) of \(H\) is in \(I(G, C_k)p\).

Proof. (Cf. [43, Corollary 7.44].) As we know, \(\psi = \psi_1\partial \phi\) for some \(\psi_1\) inflated from \(Z(G/G', C_k)\) and map \(\phi\). Assume that \(\psi_1 \notin I(G, C_k)p\). Then, recalling Lemma 5.2.7 \([\psi_1(x, y)]_{x, y \in G}\) has a row with \(m\) occurrences of \(\zeta_k\) and every other entry equal to 1. Label this row \(a\). Now

\[
\prod_{y \in G} \partial \phi(a, y) = \left( \prod_{y \in G} \phi(a)^{-1} \right) \left( \prod_{y \in G} \phi(y)^{-1} \right) \left( \prod_{y \in G} \phi(ay) \right) = \phi(a)^{-n} \in \langle \zeta_k^p \rangle.
\]

So, if we multiply together all the entries along row \(a\) of \([\psi(x, y)]_{x, y \in G}\) then we get \(\zeta_k^m \phi(a)^{-n}\), an element of \(\langle \zeta_k \rangle \setminus \langle \zeta_k^p \rangle\). But this is a contradiction. For suppose
7. Classification of small cocyclic BH\((n,p)\)s

that \(\sum_{i=0}^{k-1} c_i \zeta_k^i = 0\). Since the \(k\)th cyclotomic polynomial \(\sum_{i=0}^{p-1} x^{i(p^{-1})}\) divides \(\sum_{i=0}^{k-1} c_i x^i\), we have \(c_j = c_{p^i-1+j} = \cdots = c_{(p-1)p^{i-1}+j}, 0 \leq j \leq p^{k-1} - 1\). It is then straightforward to verify that \(\prod_{i=0}^{k-1} c_i \zeta_k^i \in \langle \zeta_p^k \rangle\).

As a consequence of Lemma [7.4.8] if \(k = p = 2\) i.e., in the real case, we eliminate several groups as indexing groups for Hadamard matrices. These include each of the groups of orders 12, 20 and 28 that are not found to be indexing groups of a Hadamard matrix of that order, in the classification of cocyclic Hadamard matrices of order less than 40 by Ó Catháin and Röder [62]. Each of these groups has trivial Schur multiplier by [53, Corollary 2.1.3]. At those orders, the groups \(C_2^2 \times C_q\) and \(D_2^q\) for \(q \in \{3, 5, 7\}\) all turn up as indexing groups.

7.4.9 Corollary. If \(n\) is \(p\)-square-free then a cocyclic BH\((n,p)\) is equivalent to a group-developed matrix.

Proof. Let \(G\) be the indexing group of a cocyclic BH\((n,p)\). Either \(p\) divides \(|G’|\) or Lemma [7.4.8] applies, and thus \(I(G, C_p) = B(G, C_p)\). Also \(\text{Hom}(H_2(G), C_p) = 1\) by [53, Theorem 2.1.5].

7.4.10 Corollary. The only cocyclic BH\((p,p)\) up to equivalence is the Fourier matrix.

Proof. Here \(\text{Hom}(H_2(C_p), C_p)\) is trivial, and thus by Corollary [7.4.9], a cocyclic BH\((p,p)\) is equivalent to a circulant matrix. Then use Proposition [7.3.4].

7.4.11 Remark. By Remark [7.4.7] and Corollary [7.4.9] for \((n, p) = (10, 5)\) or \(p = 3\) and \(n \in \{6, 24, 30\}\), there are no cocyclic BH\((n,p)\) at all (thus, Butson’s construction [12] is not cocyclic). Furthermore, a cocyclic BH\((12, 3)\), BH\((21, 3)\), BH\((20, 5)\), or BH\((14, 7)\), if one exists, is equivalent to a group-developed matrix.

7.4.2. Non-existence of cocyclic BH\((n,4)\) for \(n \equiv 2 \mod 4\)

In this section, \(H\) is a BH\((n,4)\) where \(n \equiv 2 \mod 4\). The matrix \(H\) is group-developed only if \(n\) is the sum of two squares (Lemma [7.4.3]). For a group \(G\) of order \(n\), if \(C_2 \leq G/G’\) then \(H(G, C_4)\) contains one non-trivial class in \(I(G, C_4)\); otherwise all cocycles are coboundaries. So if \(H\) is cocyclic with indexing group \(G\) and \(H\) is not group-developed then \(H \approx [\psi \partial \phi(g, h)]\) where
\[ [\psi(g, h)] = \begin{bmatrix} J_{n/2} & J_{n/2} \\ J_{n/2} & -J_{n/2} \end{bmatrix}, \] by Lemma 7.4.8. In this instance the rows and columns are labeled by the elements \( g_1, \ldots, g_{n/2}, g_1a, \ldots, g_{n/2}a \) of \( G \) in that order, for \( a \in G \) of order 2.

Suppose that \( H = [\psi(g, h)\phi(gh)]_{g, h \in G} \). The group-developed matrix \( \phi(gh) \) is of the form \( \begin{bmatrix} A & B \\ C & D \end{bmatrix} \), where each quadrant has constant row and column sum, and the row/column sum \( s_1 \) of \( A \) is the same as that of \( D \). Similarly, the row/column sum \( s_2 \) of \( B \) is the same as that of \( C \). We then have \( H = \begin{bmatrix} A & B \\ C & -D \end{bmatrix} \).

Enforcing \( nJ_n = J_nHH^* \) yields

\[ (s_1 + s_2)\bar{s}_1 + (s_2 - s_1)\bar{s}_2 = n \quad \text{and} \quad (s_1 + s_2)\bar{s}_2 - (s_2 - s_1)\bar{s}_1 = n. \]

Combining these equations we get \( s_1\bar{s}_1 + s_2\bar{s}_2 = n \). Hence \( n \) is the sum of four squares (two even, two odd), and

\[ s_2\bar{s}_1 - s_1\bar{s}_2 = 0. \quad (7.4.2) \]

Let \( s_1 = a + bi \) and \( s_2 = c + di \). Then \( ad = bc \) by \( (7.4.2) \). This proves the following.

7.4.12 Lemma. A cocyclic non-group-developed BH(\( n, 4 \)) exists for \( n \equiv 2 \) mod 4 only if there are integers \( a, b, c, d \) such that \( a^2 + b^2 + c^2 + d^2 = n \) and \( ad = bc \).

7.4.13 Corollary. There is no cocyclic BH(\( n, 4 \)) for \( n \in \{6, 14, 22, 30, 38, 42, 46, 54, 62, 66, 70, 78, 86, 94\} \).

7.4.3. Existence of cocyclic BH(\( n, p \)), np ≤ 100

Henceforth \( p \) is an odd prime. The table below summarizes existence of matrices in our classification.

<table>
<thead>
<tr>
<th>( p )</th>
<th>( \frac{n}{p} )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>F</td>
<td>NC</td>
<td>E</td>
<td>E</td>
<td>N</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>NC</td>
<td>E</td>
<td>NC</td>
<td>N</td>
</tr>
<tr>
<td>5</td>
<td>F</td>
<td>NC</td>
<td>N</td>
<td>E</td>
<td>S</td>
<td>N</td>
<td>S</td>
<td>S</td>
<td>NC</td>
<td>E</td>
<td>NC</td>
<td>N</td>
</tr>
<tr>
<td>7</td>
<td>F</td>
<td>NC</td>
<td>S</td>
<td>E</td>
<td>S</td>
<td>N</td>
<td>S</td>
<td>S</td>
<td>NC</td>
<td>E</td>
<td>NC</td>
<td>N</td>
</tr>
</tbody>
</table>

Table 7.4.1. Existence of BH(\( n, p \))

N: no Butson Hadamard matrices by Theorem 7.4.1
NC: no cocyclic Butson Hadamard matrices by Remark 7.4.11
7. Classification of small cocyclic BH\((n, p)\)s

E: cocyclic Butson Hadamard matrices exist: see Section 7.5.

S: no cocyclic Butson Hadamard matrices according to a relative difference set search.

S\(^o\): no cocyclic Butson Hadamard matrices according to an orthogonal cocycle search.

F: the Fourier matrix is the only Butson Hadamard matrix by Proposition 7.3.5.

7.4.14 Remark. There are non-cocyclic BH\((6, 3)\) and BH\((10, 5)\) by [12]. Non-existence of cocyclic BH\((6, 3)\) is verified by computer in [43, Example 7.4.2].

We relied on computation of relative difference sets only for parameter values not ruled out by any other result. Nevertheless, those calculations were not onerous: the search for a central relative difference set with parameters \((14, 7, 14, 2)\) ran over the groups of order 98 in under an hour. The test for an RDS\((20, 5, 20, 4)\) ran for all groups of order 100 in about a day, with most time being spent on \(C_{100}\). We note additionally that there are theoretical obstructions to the existence of an RDS\((21, 3, 21, 7)\): the system of diophantine signature equations that such a difference set must satisfy does not admit a solution—see [65].

7.5. The full classification

The only remaining cases to settle within the scope of our investigation are \((n, p) \in \{(9, 3), (12, 3), (27, 3)\}\). In this section we discuss our complete and irredundant classification of such BH\((n, p)\). The explicit matrices are listed at [32].

Our overall task splits into two steps. We first compute a set of cocyclic BH\((n, p)\) containing representatives of every equivalence class; then we test equivalence of the matrices produced. Since our method for the second step has already been discussed, and the orders involved pose no computational difficulties, we need not discuss this step further.

We used two complementary methods for the first step: checking shift orbits for orthogonal cocycles using the machinery of Chapter 6, and constructing relative difference sets.

7.5.1 Example. Recall Table [6.6.4] which lists the number of orthogonal elements of \(Z(G, C_3)\) for \(6 \leq \lvert G \rvert \leq 15\). Note that none were found when \(\lvert G \rvert = 18\).

We also refer the reader to [62, Section 6], which discusses a classification of (real) cocyclic Hadamard matrices via relative difference sets. The algorithm
that we used to construct difference sets is identical to the one there, and was likewise carried out using the GAP package RDS \cite{64}.

7.5.1. BH(9, 3).

There are precisely three equivalence classes of cocyclic BH(9, 3).

One class contains BH(3, 3) \(\otimes\) BH(3, 3), which has indexing group \(C_3^2\) and cocycle that is not a coboundary. Some matrices \(H_1\) in this class are also group-developed over \(C_3^2\). No \(H_1\) has indexing group \(C_9\).

A second equivalence class contains group-developed matrices with indexing group \(C_9\). No matrix \(H_2\) in this class has indexing group \(C_3^2\); hence the cocycles of \(H_2\) are all coboundaries by Lemma 7.4.8. This class is not represented in \cite{11}, but turns out to be an example of the construction in \cite{19} (see also \cite{10}).

A representative of this equivalence class has rows obtained as cyclic permutations of \((1, 1, 1, 1, \zeta_3, \zeta_2^3, 1, \zeta_2^3, \zeta_3)\).

The third class contains matrices \(H_3 \approx H_3^*\) that are cocyclic with indexing group \(C_9\). Again, \(H_3\) is equivalent to a circulant, does not have indexing group \(C_3^2\), every one of its cocycles is a coboundary, and it is not in \cite{11}.

By Proposition 7.1.1, \(\text{PAut}(\mathcal{E}_{H_2}) \cong \text{PAut}(\mathcal{E}_{H_3})\), and this is solvable.

7.5.2. BH(12, 3).

There are just two equivalence classes of cocyclic BH(12, 3), which form a single Hermitian pair, that is, the classes are \([H]\) and \([H^*]\). All are equivalent to group-developed matrices (Remark 7.4.11) over \(C_3 \times C_4, C_2^2 \times C_3\), or \(C_2^3 \times C_3\). Their automorphism groups have order 864.

We note that this is the only order \(n\) in our classification which is not a prime power and for which cocyclic BH\((n, p)\) exist. On the other hand, there exists a BH\((12, 6)\); e.g., the character table of \(C_2^3 \times C_3\). Perhaps it is not surprising that the same group indexes a group-developed BH\((12, 3)\).

7.5.3. BH(27, 3).

Predictably, order 27 was the most challenging one that we faced in our computations. An exhaustive search for orthogonal cocycles was not possible, so this order was classified exclusively by the relative difference sets method.

There are sixteen equivalence classes of cocyclic BH(27, 3) in total. Some are Kronecker products of cocyclic BH(9, 3) with the unique BH(3, 3), but the ma-
7. Classification of small cocyclic BH\((n, p)\)s

Majority are not of this form. Each matrix is equivalent to its transpose. There are two classes that are self-equivalent under the Hermitian, with the rest occurring in distinct Hermitian pairs.

We observe that every non-cyclic group of order 27 is an indexing group of at least one BH\((27, 3)\). However, there are no circulants.

Apart from the generalized Sylvester matrix, whose automorphism group is not solvable, the automorphism group of a BH\((27, 3)\) has order \(2^a 3^b\).

7.5.4. Concluding comments

It is noteworthy that all matrices in our classification are equivalent to group-developed ones (non-trivial cohomology classes occur too). This may be compared with [62], which features many equivalence classes not containing group-developed real Hadamard matrices. Also, while there exist circulant BH\((p^r, p)\) for all odd \(p\) and \(r \leq 2\) [10, 19], we have not found a circulant BH\((n, p)\) when \(n\) is not a \(p\)-power.

Some inevitable composition results should be noted.

7.5.2 Lemma. Suppose for \(i = 1, 2\) that \(H_i\) is a cocyclic BH\((n_i, k)\) with cocycle \(\psi_i\). Then \(H_1 \otimes H_2\) is a cocyclic BH\((n_1 n_2, k)\) with cocycle \(\psi \in Z(G_1 \times G_2, C_k)\) defined by \(\psi((a, b), (x, y)) = \psi_1(a, x) \psi_2(b, y)\). We have \(\psi \in B(G_1 \times G_2, C_k)\) if and only if \(\psi_i \in B(G_i, C_k), 1 \leq i \leq 2\).

7.5.3 Corollary. For all \(a \geq 1, b \geq a,\) and \(K \in \{C_3 \times C_4, C_2^2 \times C_3, C_2^3 \times C_3\}\), there exists a group-developed BH\((2^{2a} 3^b, 3)\) with indexing group \(K^a \times C_3^{-a}\).

7.5.4 Corollary. Cocyclic BH\((3^a, 3)\) indexed by \(C_3^a\) with cocycles that are not coboundaries exist for all \(a \geq 2\) (although they are also equivalent to group-developed matrices).

Corollary 7.5.3 (i) was proved previously by de Launey [20, Corollary 3.10], albeit only for indexing groups \(C_2^a \times C_3^b\).
8. Cocyclic development via
dihedral and dicyclic groups

In this chapter we synthesize some known approaches to cocyclic development of Hadamard matrices, inspired by the papers [50, 51, 33, 67]. We begin by discussing cocyclic Hadamard matrices with dihedral indexing groups $D_{4t}$ of order $4t$. In [33] it is shown that such a cocyclic Hadamard matrix exists if there is a central relative $(4t, 2, 4t, 2t)$-difference set (CRDS) in $Q_{8t}$, the dicyclic group of order $8t$ (see also [22 Theorem 2.4]). In Section 8.2 we review parts of [67]. Schmidt proves the existence of a CRDS in $Q_{8t}$ for $1 \leq t \leq 46$. In Section 8.3 we take another approach to the problem of finding these difference sets, similar to that of Ito [51]. We introduce a method of searching for a CRDS in $Q_{8t}$ by using a relationship between the CRDS and a pair of binary sequences with certain autocorrelation properties. We also demonstrate how our method is strongly related to the methods of Flannery [33] and Schmidt [67].

The perspective afforded by this chapter might lead to new existence results in further support of Ito’s conjecture that a $(4t, 2, 4t, 2t)$-CRDS exists in $Q_{8t}$ for all $t$; and consequently that Horadam and de Launey’s conjecture is likewise true: there exists a cocyclic Hadamard matrix of order $4t$ for all $t$. Note that our method enables computation of all $(4t, 2, 4t, 2t)$-CRDS in $Q_{8t}$ for $t \leq 9$.

8.1. Cocyclic development over dihedral groups

The paper [33] treats cocyclic development over $D_{2t}$, the dihedral group of order $4t$. Here we summarize some of the main results, which are used in Section 8.3. Let $D_{2t} = \langle a, b \mid a^{2t} = b^2 = 1, ba = a^{-1}b \rangle$.

A representative $\psi$ of $[\psi] \in H(D_{2t}, C_2) \cong C_2^{(3)}$ can be represented as a triple
8. Cocyclic development via dihedral and dicyclic groups

\((A, B, K)\), where \(A, B, K \in \{\pm 1\}\). Explicitly,

\[
\psi(a^i, a^j b^k) = \begin{cases} 
A^{ij} & i + j < 2t \\
A^{ij} K & i + j \geq 2t
\end{cases}
\]

\[
\psi(a^i b^1, a^j b^k) = \begin{cases} 
A^{ij} B^k & i \geq j \\
A^{ij} B^k K & i \leq j
\end{cases}
\]

Since it appears to be a likely class to contain orthogonal cocycles, we focus on \((A, B, K) = (1, -1, -1)\). In this case, a cocyclic Hadamard matrix is equivalent to

\[
\begin{bmatrix}
M & N \\
ND & -MD
\end{bmatrix}
\]

where \(M\) and \(N\) are back circulant, and \(D\) is obtained by negating each non-initial column of the back circulant \(2t \times 2t\) permutation matrix with 1 in position \((1, 1)\). Let \(P\) be the \(2t \times 2t\) circulant permutation matrix with 1 in the last position of the first row. For \(1 \leq i \leq 2t\) let \(W_i\) be the \(2t \times 2t\) diagonal matrix with main diagonal \((1, 1, \ldots, 1, -1, \ldots, -1)\) where the last entry 1 occurs in position \(2t - i\). Finding orthogonal cocycles for \((A, B, K) = (1, -1, -1)\) then reduces to the following (\(\vec{m}\) and \(\vec{n}\) are the first rows of \(M\) and \(N\) respectively).

Find a pair of \(2t\)-tuples \(\vec{m}\) and \(\vec{n}\) with entries \(\pm 1\) such that \(\vec{m}(\vec{m} P^i W_i)\top = -\vec{n}(\vec{n} P^i W_i)\top\) for \(1 \leq i \leq t - 1\).

The corresponding central extension of \(C_2\) by \(D_{2t}\) is isomorphic to \(Q_{st}\). Table 4 of [33] shows that these orthogonal cocycles exist for \(1 \leq t \leq 11\). In the next section we summarize work of Schmidt [67] which proves existence for the much larger range \(1 \leq t \leq 46\).

8.2. Cocyclic Hadamard matrices with dicyclic extension groups

Hereafter \(Q_{st} = \langle a, b \mid a^{4t} = 1, b^2 = a^{2t}, a^b = a^{-1}\rangle\); so \(Q_{st}\) has element set \(\{a^i b^j \mid 0 \leq i \leq 4t - 1, 0 \leq j \leq 1\}\). In this chapter, the default parameters for a CRDS in \(Q_{st}\) are \((4t, 2, 4t, 2t)\). Ito conjectures that there exists such a CRDS in \(Q_{st}\) with forbidden subgroup \(N = \langle b^2 \rangle\) for all \(t\).
As well as difference sets in $\mathbb{Q}_t$, Schmidt [67] studies the existence of Williamson matrices, and the interplay between these objects. We are primarily interested in the results concerning CRDSs alone, such as the following.

8.2.1 Lemma (Lemma 3.1, [67]). A CRDS in $\mathbb{Q}_t$ relative to the central subgroup $N = \langle b^2 \rangle$ exists if and only if there are polynomials $f(x), g(x)$ of degree $2t - 1$ with coefficients $\pm 1$, such that

$$f(x)f(x^{-1}) + g(x)g(x^{-1}) \equiv 4t \mod (x^{2t} + 1).$$

8.2.2 Theorem (Corollary 3.6, [67]). Let $m$ be a positive integer such that $2m - 1$ or $4m - 1$ is a prime power, or $m$ is odd and there is a Williamson matrix over $\mathbb{Z}_m$. Then there is a CRDS in $\mathbb{Q}_t$ for every $t$ of the form

$$t = 2^a \cdot 10^b \cdot 26^c \cdot m$$

with $a, b, c \geq 0$.

The orders 8.2.2 are connected to the known lengths of Golay sequences derived from Golay polynomials satisfying 8.2.1. In the next section, we show that Golay sequences constitute a special case of a broader range of sequence pairs that can be used to construct a CRDS in $\mathbb{Q}_t$.

8.3. Centrally relative difference sets via pairs of binary sequences

We now give another approach to searching for a CRDS in $\mathbb{Q}_t$. Much of this section is reminiscent of [51].

As in [4], we define the periodic autocorrelation of a $\{\pm 1\}$-sequence $r$ of period (or length) $n$ with shift $k$ to be

$$C_k(r) = \sum_{i=0}^{n-1} r_ir_{i+k}$$

where subscripts are taken modulo $n$. Sequences are indexed beginning with 0.
8. Cocyclic development via dihedral and dicyclic groups

unless stated otherwise. Any CRDS $R$ in $Q_{st}$ must contain $2t$ elements $a^i$, and $2t$ elements $a^j b$, where $a^j b \in R$ if and only if $a^{i+2t}b^j \notin R$ for all $0 \leq i \leq 2t$, $0 \leq j \leq 1$. The following draws on [51, Section 1].

8.3.1 Lemma. The set of $(4t, 2, 4t, 2t)$-CRDS in $Q_{st}$ is in one-to-one correspondence with the set of all pairs of sequences $r, s$ with entries in $\{\pm 1\}$ of length $4t$ satisfying

(P1) $r_i = -r_{2t+i}$ and $s_i = -s_{2t+i}$ for all $0 \leq i \leq 2t - 1$

(P2) $C_k(r) + C_k(s) = 0$ for all $1 \leq k \leq 2t - 1$.

Proof. Let $r$ and $s$ be sequences satisfying (P1), (P2). Further, let $R \subset Q_{st}$ be such that $a^i \in R$ if and only if $r_i = 1$ and $a^j b \in R$ if and only if $s_j = 1$. (P1) implies that $R$ has $2t$ elements of the form $a^i$, $2t$ elements of the form $a^j b$, and that $xy^{-1} \notin N$ for any $x, y \in R$. Choose $i$ such that $a^i \in R$. Then

$$\{a^i (a^j b)^{-1}\}_{a^j b \in R} = \{a^{2t+i+j} b\}_{a^j b \in R}$$

and

$$\{a^j b (a^i)^{-1}\}_{a^j b \in R} = \{a^{i+j} b\}_{a^j b \in R}.$$ 

Since $\{a^i+j b\} \cup \{a^{2t+i+j} b\}$ is a disjoint union, it is a set of order $4t$, i.e., each element of the form $a^k b$ where $0 \leq k \leq 4t - 1$ occurs exactly once. Thus, running over all $i$ such that $a^i \in R$ ensures that each element of the form $a^k b$ occurs exactly $2t$ times.

(P2) implies that for any $1 \leq k \leq 4t - 1, k \neq 2t$, in exactly $4t$ cases $r_i = r_{i+k}$ or $s_i = s_{i+k}$. (P1) implies that in $2t$ of these cases, $r_i = r_{i+k} = 1$ or $s_i = s_{i+k} = 1$. Thus for any $k$, we have $a^k = a^{i+k}(a^i)^{-1}$ or $a^k = a^{i+k} b(a^i b)^{-1}$, i.e., $a^k$ occurs exactly $2t$ times as $xy^{-1}$ for $x, y \in R$. This proves that $R$ is a central relative $(4t, 2, 4t, 2t)$-difference set in $Q_{st}$.

8.3.2 Remark. If $R$ is a CRDS in $Q_{st}$ then so too is $x R$ for all $x \in Q_{st}$.

Recall the requirement for the existence of an orthogonal cocycle in $D_{4t}$ given at the end of Section 8.1. Let $r$ and $s$ be as in Lemma 8.3.1 and let $r'$ and $s'$ be the subsequences of the first $2t$ entries in $r$ and $s$ respectively. Then for any
\[ 1 \leq i \leq 2t - 1, \]
\[ \sum_{k=0}^{2t-1} (r_k r_{k+i} + s_k s_{k+i}) - \sum_{k=0}^{2t-1-i} (r'_{k} r'_{k+i} + s'_{k} s'_{k+i}) = 0 \]

and so
\[ \sum_{k=0}^{2t-1-i} r'_{k} r'_{k+i} - \sum_{k=2t-i}^{2t-1} r'_{k} r'_{k+i} = - \sum_{k=0}^{2t-1-i} s_{k} s_{k+i} + \sum_{k=2t-i}^{2t-1} s'_{k} s'_{k+i}. \]

Hence \( r'(r'P^tW_i) = -s'(s'P^tW_i) \). This establishes once more the equivalence between cocyclic Hadamard matrices with extension group \( \mathbb{Q}_{8^t} \) and central relative \((4t, 2, 4t, 2t)\)-difference sets in \( \mathbb{Q}_{8^t} \).

We say that a pair of sequences \( r, s \) meeting the criteria of Lemma 8.3.1 is a suitable pair. Ito’s definition of an associated pair of sequences of length \( 2t \) in \([51]\) is similar. In fact, an associated pair is comprised of the first half of each sequence in a suitable pair; but as suitable pairs are sequences of length \( 4t \), we employ this term to avoid confusion. By constructing sequences that satisfy (P1), and testing pairs of sequences for (P2), a thorough computer search for suitable pairs is feasible when \( t \) is reasonably small. Table 8.3.1 displays the total number \( n(t) \) of pairs found for \( 1 \leq t \leq 9 \). So assume that \( r \) and \( s \) satisfy (P1). Then \( C_t(r) = C_t(s) = 0 \) and \( C_{t-i}(r) = -C_{t+i}(r) \) for all \( 1 \leq i \leq t - 1 \). Thus, to check (P2), we need only verify that \( C_k(r) + C_k(s) = 0 \) for \( 1 \leq k \leq t - 1 \).

<table>
<thead>
<tr>
<th>( t )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n(t) )</td>
<td>16</td>
<td>128</td>
<td>576</td>
<td>4096</td>
<td>11200</td>
<td>59904</td>
<td>90944</td>
<td>557056</td>
<td>1041984</td>
</tr>
</tbody>
</table>

Table 8.3.1. Number \( n(t) \) of suitable pairs

Note that we can construct new suitable pairs by performing certain operations on an existing suitable pair. We say that a sequence \( r' \) of length \( n \) is \( r \) shifted forward \( k \) places if \( r'_{i} = r_{i-k (\text{mod } n)} \). If \( r, s \) is a suitable pair, then so too is any pair \( r', s' \) obtained by a combination of the following operations on \( r, s \): shift either sequence forward \( k \) places for any \( 1 \leq k \leq 4t - 1 \); swapping sequences; reversing either sequence. There are \( 128t^2 \) different combinations of these operations which form a group isomorphic to \( E \cong (A \times B) \rtimes C_2 \), where
A \cong B \cong D_{4t} and A^c = B for C_2 = \langle c \rangle. Here A and B act on the first and second sequences respectively, by shifting forward and reversing the sequence, and the transposition c acts by swapping the sequences. Negating either sequence is the same as shifting it forward 2t places. The operation that negates both sequences is the lone non-trivial element in Z(E).

If any pair of sequences \( r', s' \) can be found via some combination of these operations on a pair \( r, s \), then these pairs will be called equivalent, and we say that equivalent pairs are in the same bundle. The operations will hereafter be known as equivalence operations. Bundles of equivalent sequences can be of any order dividing \( 128t^2 \). Table 8.3.2 gives the number \( b(t) \) of unique bundles of suitable pairs found for each \( 1 \leq t \leq 9 \).

<table>
<thead>
<tr>
<th>t</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>b(t)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>16</td>
<td>17</td>
<td>72</td>
<td>102</td>
</tr>
</tbody>
</table>

Table 8.3.2. Number \( b(t) \) of unique bundles

Tables 8.3.1 and 8.3.2 imply that for all \( t \neq 4 \) listed here, some bundles must be of order less than \( 128t^2 \). Thus, for some suitable pairs, performing a combination of equivalence operations fixes the pair. These cases are interesting, and will be discussed later.

8.3.3 Proposition. Let \( r, s \) be a pair of sequences meeting the criteria of Lemma 8.3.1. Let \( r', s' \) be the pair generated by negating \( r_i \) and \( s_i \) for odd \( i \), i.e., negating every second entry. Then \( r', s' \) is a suitable pair.

Proof. (P1) is trivially preserved. Clearly \( C_k(r) = C_k(r') \) and \( C_k(s) = C_k(s') \) for all even \( k \). It is readily checked that \( C_k(r) = -C_k(r') \) and \( C_k(s) = -C_k(s') \) for odd \( k \), and thus \( C_k(r) + C_k(s) = 0 = -(C_k(r') + C_k(s')) \).

As this is a construction of a new suitable pair from a known pair, it may seem appropriate to regard the new sequence pair as equivalent; Theorem 8.3.9 below indicates that the operation is natural in some sense. However, usually it changes the autocorrelation values of the individual sequences, and their run structure (runs are discussed in Subsection 8.3.2). Consequently, we omit it as an equivalence operation.
The proof of Proposition 8.3.3 leads to our first construction of a larger suitable pair from a smaller one.

8.3.4 Theorem. If there is a suitable pair of sequences of length $4t$, then there is a suitable pair of length $2^m4t$ for all positive integers $m$.

Proof. Let $r, s$ be a suitable pair of length $4t$. Define $x = r_0s_0r_1s_1\ldots r_{4t-1}s_{4t-1}$ of length $8t$. Then for all $1 \leq k \leq 2t - 1$, $C_{2k}(x) = C_k(r) + C_k(s) = 0$. Now let $y$ be the sequence obtained from $x$ by negating every second entry. Then $C_k(y) = \pm C_k(x)$ depending on whether $k$ is odd or even. Thus, for $1 \leq k \leq 2t - 1$, $C_k(x) + C_k(y) = 0$. ♦

8.3.5 Corollary. For any $t$ such that there is a CRDS in $Q_{8t}$, there is a CRDS in $Q_{2^m8t}$ for all $n \geq 1$.

8.3.6 Remark. Reversing the construction in Theorem 8.3.4 provides a way to generate a suitable pair of length $4t$ from any sequence $x$ of length $8t$ such that $x_i = -x_{i+4t}$, with $C_{2k}(x) = 0$ for $1 \leq k \leq 4t - 1$.

8.3.7 Remark. Corollary 8.3.5 is actually a special case of [67, Theorem 3.2], although the construction appears to be different. Schmidt builds larger central relative difference sets in $Q_{16mt}$ from known ones in $Q_{8t}$, and Golay sequences of length $2m$.

Proposition 8.3.3 also leads to a connection to the shift action, which we discuss next.

8.3.1. The shift action and CRDS in $Q_{8t}$

Let $R$ be a CRDS in $G = Q_{8t}$, and let $U = \langle u \rangle \cong C_2$. Define $\phi \in \text{Fun}(G, U)$ by

$$\phi(g) = u^{I_R(g)}$$

where $I_R(g) = 1$ if $g \in R$ and 0 otherwise. According to Lemma 6.3.5 $(\partial \phi)h = \partial \check{\phi}$ where $\check{\phi}(g) = \phi(h)^{-1}\phi(hg)$.

8.3.8 Theorem. Let $h \in G$ and let $R$, $\phi$ be as above. If $R_h = \check{\phi}^{-1}(u)$ then $R_h$ is a CRDS in $G$. 

91
8. Cocyclic development via dihedral and dicyclic groups

Proof. Suppose first that \( h \notin R \). Then \( \overline{\phi}(g) = \phi(hg) \) and thus \( \overline{\phi}^{-1}(u) = \{ h^{-1}x \mid x \in R \} \). Otherwise \( \overline{\phi}(g) = u\phi(hg) \), so \( \overline{\phi}^{-1}(u) = Q_{st} \setminus \{ h^{-1}x \mid x \in R \} \). Either way, by Remark 8.3.2 we get the result. ♦

So if we construct \( \phi \) from a known CRDS \( R \) as above, apply the shift action to get \( \overline{\phi} \), and then construct \( R_h \), we get another CRDS.

8.3.9 Theorem. Let \( R \) and \( \phi \) be as above. Let \( \mu \in \text{Hom}(G,U) \) and let \( R_{\mu} = \mu^{-1}(u) \). Then \( R' = (R \cup R_{\mu}) \setminus (R \cap R_{\mu}) \) is a CRDS.

Proof. Let \( r,s \) be the suitable pair associated with \( R \). We need only check two generators \( \mu_1, \mu_2 \) of \( \text{Hom}(G,U) \), where \( \mu_1(a) = u \), \( \mu_1(b) = 1 \) and \( \mu_2(b) = u \), \( \mu_2(a) = 1 \). First, \( \mu_1(a^i) = \mu_1(a^ib) = u \) if and only if \( i \) is even. Then \( R' \) has a suitable pair \( r',s' \) which can be derived from \( r,s \) by negating every second entry in each. By Proposition 8.3.3, \( R' \) will be a CRDS.

Now \( \mu_2(a^ib) = u \) for all \( i \) and \( \mu_2(a^j) = 1 \) for all \( j \). In this case \( r' = s \) and \( s' = r \), and hence \( R' \) is a CRDS. ♦

8.3.2. Some criteria for suitable pairs

We now study some properties of suitable pairs \( r,s \). A run is a subsequence of a sequence \( r \) where all elements have the same value. Since our interest is in periodic autocorrelation of sequences, we will say that if the entries in the first and last positions match then they are part of the same run; e.g., the sequence \( 1 \ldots \ldots \ldots \ldots \ldots \cdot \cdot \cdot 11 \) has two runs of length 4. Hereafter \( r,s \) is a suitable pair.

8.3.10 Lemma. The number of runs in the sequences \( r \) and \( s \) must sum to \( 4t \).

Proof. Deny; then \( C_1(r) + C_1(s) \neq 0 \). ♦

8.3.11 Remark. Ito refers to runs as blocks. Lemma \( 8.3.10 \) is similar to [51, Proposition 4], regarding blocks in an associated pair. Lemmas \( 8.3.12 \) and \( 8.3.13 \) are also similar to [51, Proposition 6].

8.3.12 Lemma. The number of runs in either sequence \( r \) or \( s \) is bounded below by \( t \) and above by \( 3t \).

Proof. Suppose we have \( m \) runs in \( r \). By Lemma \( 8.3.10 \) we have \( 4t - m \) runs in the second. This implies that there are at most \( 2m \) positions \( r_i \) such that \( r_i \neq r_{i+2} \), and similarly for \( s \). If \( 4m < 4t \) then \( C_2(r) + C_2(s) > 0 \); thus \( m \geq t \). ♦
8.3.13 Lemma. The number of runs in either sequence must be even, but not divisible by 4.

Proof. Without loss of generality, suppose that \( r_0 = 1 \) and thus \( r_{2t} = -1 \). Either \( r_{2t-1} = 1 \) or \(-1\). In the first case, a run ends at positions \( 2t - 1 \) and \( 4t - 1 \). Since the \( m \)th run ending at \( r_{2t-1} \) is a run of 1s, \( m \) is odd and there are \( 2m \) runs in total. In the second case, because shifting the sequence forward does not affect the run structure, we shift forward until we can revert to the first case. ♦

8.3.14 Example. If \( t = 3 \) then Lemma 8.3.12 and Lemma 8.3.13 restrict our search to pairs of sequences that each have precisely 6 runs.

8.3.15 Remark. Because we may shift the sequence forward until \( r_0 = r_{2t-1} = 1 \), we can restrict our search for bundles to sequences with an odd number of runs in the first \( 2t \) entries.

8.3.16 Lemma. If \( r \) is a sequence of length \( 4t \) in a suitable pair, then \(|C_k(r)| < 4t\) for all \( k \neq 0 \).

Proof. Suppose that \( C_k(r) = 4t \) for some \( 1 \leq k \leq t - 1 \). For \( r, s \) to satisfy the properties of Lemma 8.3.1, we must have \( C_k(s) = -4t \). But this would imply that \( C_{2k}(s) = C_{2k}(r) = 4t \). ♦

8.3.3. The aperiodic approach

Since the first \( 2t \) entries in the sequence determine the rest, we now study the first half of each sequence in a suitable pair. These sequences of length \( 2t \) are more closely related to Ito’s associated pairs.

Denote by \( A_k(r) \) the aperiodic autocorrelation of a sequence \( r \) of length \( n \) with shift \( k \):

\[
A_k(r) = \sum_{i=0}^{n-1-k} r_i r_{i+k}.
\]

8.3.17 Lemma. Let \( r \) be a sequence of length \( 2t \) and \( r' \) be the sequence of length \( 4t \) where \( r'_i = -r'_{i+2t} = r_i \) for all \( 1 \leq i \leq 2t \). Then \( C_k(r') = 2A_k(r) - 2A_{2t-k}(r) \).
8. Cocyclic development via dihedral and dicyclic groups

Proof. Observe that

\[ C_k(r') = \sum_{i=0}^{4t-1} (-1)^{r'_i + r'_{i+k}} \]

\[ = 2A_k(r) + \sum_{i=2t-k}^{2t-1} (-1)^{r'_i + r'_{i+k}} + \sum_{i=4t-k}^{4t-1} (-1)^{r'_i + r'_{i+k}} \]

\[ = 2A_k(r) - 2A_{2t-k}(r). \]

Thus, if we wish to search for suitable pairs \( r, s \) of length \( 4t \) satisfying the criteria of Lemma 8.3.1, we may instead search for a pair of sequences \( r', s' \) of length \( 2t \) such that

\[ A_k(r') - A_{2t-k}(r') = -A_k(s') + A_{2t-k}(s'), \]

i.e.,

\[ A_k(r') + A_k(s') = A_{2t-k}(r') + A_{2t-k}(s'), \quad (8.3.1) \]

for \( 1 \leq k \leq t - 1 \). A pair of sequences \( a \) and \( b \) of length \( l \) are called Golay sequences if \( A_k(a) + A_k(b) = 0 \) for \( 1 \leq k \leq l - 1 \). Such pairs of sequences satisfy the condition above, and so a pair of Golay sequences of length \( 2t \) can be used to construct a CRDS in \( Q_{8t} \). First introduced by Golay [38], these sequences have been studied extensively by Golay himself [39], and many others. Turyn [70] proved that the sequences exist at all lengths \( l = 2^a10^b26^c \) where \( a, b, c \) are non-negative integers; they are not currently known to exist at other lengths. Golay sequences have been used to construct Hadamard matrices and other orthogonal designs; see, e.g., [13, 16, 17]. The condition for sequence pairs above is less restrictive than for Golay sequences, and by virtue of our computer searches, is satisfied by pairs of sequences of lengths \( 2t \) for \( 1 \leq t \leq 9 \). This includes sequences of length 6, 12, 14, 18, which are not Golay numbers. Of course Schmidt’s proof that a CRDS exists in \( Q_{8t} \) for all \( 1 \leq t \leq 46 \) implies an even greater extension. There are constructions of larger Golay sequences using known smaller ones. For example, see [17, Lemma 1], which ultimately leads to infinite families of Golay sequences, and, in turn, cocyclic Hadamard matrices. So we should investigate constructions for larger suitable pairs from smaller ones. We pose the following questions.
Given pairs of sequences \( r_1, s_1 \) and \( r_2, s_2 \) of length \( n \) and \( m \) respectively, satisfying (8.3.1), can we construct a larger pair of length \( nm \)?

If \( r_1, s_1 \) and \( r_2, s_2 \) are pairs of length \( 2n \) and \( 2m \) respectively, can we construct a larger pair of length \( 2nm \)?

8.3.4. Aperiodic autocorrelation properties

In this section we focus on properties of sequences of length \( 2t \) satisfying (8.3.1). We start by looking at the aperiodic autocorrelation properties of any binary sequence. The following theorem first appeared in a similar form in [30].

8.3.18 Theorem. There are precisely \( 2^k \binom{n-k}{z} \) binary sequences \( r \) of length \( n \) such that \( A_k(r) = n - k - 2z \).

Proof. Fix \( k \). The maximum possible value of \( A_k(r) \) is \( n - k \) for any sequence \( r \). Thus, for \( z = 0 \) we have \( 2^k \) possible ways to pick the first \( k \) elements of the sequence. The sequence is then completed by letting \( r_{i+k} = r_i \) for all \( 1 \leq i \leq n - k \). Suppose then that \( z > 0 \). We can construct a sequence \( r \) such that \( A_k(r) = n - k - 2z \) by applying the following simple algorithm to one of the \( 2^k \) sequences with maximal autocorrelation:

1. Let \( s \) be a sequence such that \( A_k(s) = n - k \), constructed as above.
2. Choose \( z \) of the last \( n - k \) entries of \( s \).
3. Let \( r = s \).
4. For each \( s_i \) chosen in (ii), negate \( r_{i+mk} \) for all \( 0 \leq m \leq \lfloor (n - i)/k \rfloor \).

The resulting sequence will be such that \( A_k(r) = n - k - 2z \). Thus there are \( 2^k \binom{n-k}{z} \) sequences generated in this way. Finally, since \( 2^m = \sum_{i=0}^{m} \binom{m}{i} \), we know that we have accounted for all sequences. ♦

The construction of sequences with a desired value for \( A_k(r) \) described above can be useful computationally. For convenience we adhere to Ito’s notation and write a sequence in terms of the length of runs in the sequence. In this instance the first and last entries of the sequence are not considered part of the same run, even if they are equal. So, for example, we may write \((2, 1, 5)\) in place of \(11 - 11111\). Table 8.3.3 gives examples of suitable pairs \( r, s \) in this format.

95
8. Cocyclic development via dihedral and dicyclic groups

<table>
<thead>
<tr>
<th>$t$</th>
<th>$r$</th>
<th>$s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(2)</td>
<td>(2)</td>
</tr>
<tr>
<td>2</td>
<td>(4)</td>
<td>(1,1,2)</td>
</tr>
<tr>
<td>3</td>
<td>(1,1,4)</td>
<td>(2,1,3)</td>
</tr>
<tr>
<td>4</td>
<td>(2,1,5)</td>
<td>(2,1,1,1,3)</td>
</tr>
<tr>
<td>5</td>
<td>(2,2,6)</td>
<td>(1,1,2,1,1,3)</td>
</tr>
<tr>
<td>6</td>
<td>(3,2,7)</td>
<td>(2,1,1,1,1,2,1,2)</td>
</tr>
<tr>
<td>7</td>
<td>(2,1,1,1,1,1,7)</td>
<td>(3,2,1,2,1,2,3)</td>
</tr>
<tr>
<td>8</td>
<td>(2,1,1,1,1,2,8)</td>
<td>(1,1,2,2,3,2,1,1,3)</td>
</tr>
<tr>
<td>9</td>
<td>(3,1,1,2,2,1,8)</td>
<td>(3,2,2,1,1,1,2,1,1,3)</td>
</tr>
</tbody>
</table>

Table 8.3.3. Suitable pairs

By Remark 8.3.15, we can restrict searches to cases where $m$ is odd and where the sequence begins and ends with 1. There are $2^{t-2}$ such sequences $r$ of length $2t$, all of which have $A_{2t-1}(r) = 1$.

**8.3.19 Lemma.** In a pair of sequences $r$, $s$ of length $2t > 2$ satisfying (8.3.1), with each sequence beginning and ending with 1, there are exactly $t$ runs of length 1 in the combined sequences.

**Proof.** Suppose that there are $x$ runs of length 1. Let $y$ be the number of runs of length greater than 2 in the sequences combined and let $l_i$ be the length of one of these for $1 \leq i \leq y$. By Lemma 8.3.10, there are $2t$ runs in total between $r$ and $s$, and thus $\sum_{i=1}^{y} (l_i - 2) = x$. Suppose that there are $z$ runs of length 1 at either end of either sequence, so $0 \leq z \leq 4$. Then $A_2(r) + A_2(s) = (-4t + 4) + 2(2x - z)$ and $A_{2t-2}(r) + A_{2t-2}(s) = 4 - 2z$. Hence $x = t$ by (8.3.1). \[\Box\]

**8.3.5. Bundles not of maximal order**

We noted previously that for $1 \leq t \leq 9$ there is at least one bundle of suitable pairs of order less than $128t^2$. This can only occur if some combination of equivalence operations fixes the suitable pair $r, s$. By Lemma 8.3.16, we eliminate the possibility that shifting a sequence forward fixes the sequence. Swapping the sequences only fixes the pair if $r = s$, and is highly unlikely for large $t$; it does not occur for $2 \leq t \leq 9$. Thus we consider the situation that reversing one of the sequences in a suitable pair fixes it. We will say that such a sequence is symmetric. Since this occurs at least once for all $t \neq 4$ where we have completed a search for suitable pairs, we study the properties such a sequence may have.
Let $r$ be a symmetric sequence of length $4t$ where $r_i = -r_{i+2t}$ for $0 \leq i \leq 2t - 1$. Then we also have that $r_i = -r_{2t-1-i}$ for $0 \leq i \leq t - 1$.

**8.3.20 Lemma.** For $1 \leq k \leq t - 1$, the value of $C_k(r)$ has the following properties.

- Odd $t$, odd $k$: $C_k(r) \equiv 0 \mod 8$.
- Odd $t$, even $k$: $C_k(r) \equiv 4 \mod 8$.
- Even $t$, odd $k$: $C_k(r) \equiv 4 \mod 8$.
- Even $t$, even $k$: $C_k(r) \equiv 0 \mod 8$.

**Proof.** First let $t$ and $k$ be odd. Then

$$r_i r_{i+k} = r_{2t-1-i} r_{2t-1-i-k} = r_{2t+i} r_{2t+i+k} = r_{4t-1-i} r_{4t-1-i-k}$$

(8.3.2)

for all $i$. This implies that every product of two elements in the sequence is repeated in four different positions, except when $2t - 1 - i = i + k$, i.e., $i = \frac{(2t-1-k)}{2}$. In that case,

$$r_{\frac{(2t-1-k)}{2}} r_{\frac{(2t-1+k)}{2}} + k = r_{4t-1-\frac{(2t-1-k)}{2}} r_{4t-1-\frac{(2t-1+k)}{2}} = -1$$

and

$$r_{\frac{2t-(k+1)}{2}} r_{\frac{2t+(k-1)}{2}} = r_{4t-\frac{(k+1)}{2}} r_{\frac{(k-1)}{2}} = 1.$$

These four products sum to zero. The remaining $4t - 4$ products are split into $t - 1$ products that each appear 4 times as per (8.3.2), and since $t - 1$ is even, the total sums to a multiple of 8; thus $C_k(r) \equiv 0 \mod 8$.

If $k$ is even then it is impossible that $i = (2t - 1 - k)/2$. So there are $4t$ products split into $t$ products that appear four times as per (8.3.2), giving $C_k(r) \equiv 4 \mod 8$.

The proof for even $t$ is similar. ♦

It may appear that a likely complement to a symmetric sequence is another symmetric sequence. However, we have found no examples of a suitable pair comprised of two symmetric sequences when $t \geq 3$. This means that since only one sequence is fixed by reversing it, the bundle of pairs has order $64t^2$. Table
8. Cocyclic development via dihedral and dicyclic groups

8.3.4 adds a row $m(t)$ to Table 8.3.2 to indicate how many of the unique bundles of suitable pairs found contain a symmetric sequence.

<table>
<thead>
<tr>
<th>$t$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b(t)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>16</td>
<td>17</td>
<td>72</td>
<td>102</td>
</tr>
<tr>
<td>$m(t)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>8</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 8.3.4. Unique bundles not of maximal order

While $m(t)$ is small here, we should consider the relative search spaces, where the first property of Lemma 8.3.1 is assumed. With no restriction on symmetry, there are at least $2^t/128t^2$ unique bundles in the search space. If we insist on symmetry in one sequence then there are no less than $2^t/64t^2$ unique bundles. Thus the search space with one symmetric sequence is approximately $1/2^{t-1}$ times the size of the original. Bearing this in mind, with the exception of $t = 4$ above, the success rate in this search space is higher. When $t = 9$, we find just 3 of the 102 bundles were in this search space; but the space is approximately $1/256$ times the size of the larger space.
9. Conclusions and open problems

In this final chapter, we formulate some open problems arising out of the research undertaken for the thesis. We also suggest some possibilities for future work.

9.1. Cocyclic development of the generalized Sylvester matrix

In Chapter 3 we proved that an indexing group of the generalized Sylvester matrix $D_{(p,m,k)}$ is isomorphic to a regular subgroup of $\text{AGL}(k, p^m)$. It remains to determine precisely when a regular subgroup of $\text{AGL}(k, \text{GF}(p^m))$ is an indexing group of $D_{(p,m,k)}$.

**Research Problem 1.** Give a full characterization of the regular subgroups of $\text{AGL}(k, \text{GF}(p^m))$ that are isomorphic to indexing groups of $D_{(p,m,k)}$.

**Research Problem 2.** Completely classify the groups over which Kantor’s design $K_{2n}$ is developed for all $n$.

9.2. Shift actions

Theorems 5.2.5 and 5.2.9 solve the problem of enumerating fixed points in $Z(G, U)$, and of enumerating fixed points in $B(G, U)$ when $G$ is abelian. We saw that $s_p$ as in Theorem 5.2.9 is always a lower bound on the dimension of $\text{Fix}_B(G)$. For some non-abelian $G$, the dimension bound is met exactly. But this does not always happen (as Example 5.2.12 shows). So we pose the following.

**Research Problem 3.** For any $G$ and abelian $U$ such that $|G|$ and $|U|$ are not coprime, enumerate the fixed points of $B(G, U)$ under the shift action.

In Chapter 6 we almost fully settle the problem of complete reducibility of shift representations. A couple of questions remain, which we have already discussed in Section 6.6.2, so merely state the problem formally here.
9. Conclusions and open problems

**Research Problem 4.** Resolve Conjectures 6.6.1 and 6.6.2.

We developed algorithms to calculate \( \Gamma \) and \( \Gamma_B \) for the case \( U \cong C_p \). The insights and experimental data obtained using these algorithms have been invaluable, both for the theory in Chapters 5 and 6, and the classification of cocyclic Butson Hadamard matrices in Chapter 7. With an eye on classification problems for other kinds of cocyclic generalized Hadamard matrices, we therefore propose

**Research Problem 5.** Develop and implement algorithms to compute with shift representations for any abelian coefficient group \( U \).

The most attractive feature of the shift action is that it preserves orthogonality of cocycles. Computation of shift orbits in \( Z(G,U) \) is hampered by the fact that orbits have maximal length \( |G| \). In order to push the computation further we need to improve our search methods. It is certainly not the case that a submodule of \( Z(G,U) \) generated by orthogonal cocycles contains only orthogonal cocycles. However, some empirical evidence gained from the orthogonal cocycles that we did find provides encouragement. For example, the majority of orthogonal cocycles found were in maximal orbits. For \( G \cong C_2^2 \times C_p \), \( p = 3, 5, 7 \), all orthogonal cocycles are in orbits of maximal length \( |G| \). Furthermore, all orthogonal cocycles for \( p = 3, 5 \) are in the same cohomology class, \( [\psi_1 \psi_2 \psi_3] \) where \( \{\psi_1, \psi_2, \psi_3\} \) generates \( H(G,U) \) as per [36]. In fact it is conjectured that this must always be the case when \( G \cong C_t \times C_2^2 \) for odd \( t \); see [43, Research Problem 37] or [3, Section 2.2]. Baliga and Horadam first investigated this problem and found that Williamson matrices correspond to orthogonal cocycles of this form [5]. In these cases we also observed that two orbits containing orthogonal cocycles differed by the single non-trivial element \( \partial \phi \) of \( \text{Fix}_B(G) \). That is, if \( \psi \) is orthogonal then so too is \( \psi \partial \phi \).

**9.3. Cocyclic Butson Hadamard matrices**

Although the investigation of Chapter 7 was completed for the proposed values of \( n \) and \( p \), there is great scope for further work. Of course we could attempt to extend the classification to larger \( n \) and \( p \)—but we would inevitably hit a computational wall before too long. The next step may be to generalize to \( BH(n,k) \) for composite \( k \); see e.g., Section 7.4.2. Research is ongoing toward...
this end. This introduces a number of problems that do not arise for BH\((n, p)\)s. Firstly, \(k\) need not divide \(n\); it must only satisfy the conditions of Theorem 2.2.4. Secondly, the BH\((n, k)\) are not necessarily row or column balanced, which makes orthogonality testing a slower process. The coincidence between Butson Hadamard matrices and generalized Hadamard matrices is also restricted to prime phase. Two research problems born from these issues are as follows.

**Research Problem 6.** For composite \(k\) dividing \(n\), when is a cocyclic BH\((n, k)\) row/column balanced?

**Research Problem 7.** When is the transpose of a GH\((n, G)\) also a GH\((n, G)\), for non-abelian \(G\)?

### 9.4. Final comments

The study of pairwise combinatorial designs is by no means limited to the various kinds of Hadamard matrices which have predominated in this thesis. The many different families of PCDs described in [21, Chapter 2] are all studied in their own right. These designs are closely related to other mathematical objects such as difference sets, Steiner systems, and projective planes. Problems in design theory are thereby often somehow equivalent to problems in finite geometry or combinatorics. For instance, we may be able to answer the existence question for projective planes of non-prime-power order by studying generalized Hadamard matrices. Conversely it may be that the solutions to large problems in design theory, such as the Hadamard conjecture, will come from other areas of mathematics.

Of course, it is not just intellectual curiosity that propels the study of pairwise combinatorial designs; the huge range of applications is a constantly motivating force. As an attempt to systematize approaches to all these problems, algebraic design theory will surely continue to develop. It is hoped that this thesis will be a useful contribution to the field.
Bibliography


Bibliography


Bibliography


Bibliography


