

# On linear shift representations

D. L. Flannery and R. Egan \*

School of Mathematics, Statistics and Applied Mathematics  
National University of Ireland, Galway  
Ireland

December 10, 2014

## Abstract

We introduce and develop the concept of (linear) *shift representation*. This derives from a certain action on 2-cocycle groups that preserves both cohomological equivalence and orthogonality for cocyclic designs, discovered by K. J. Horadam. Detailed information about fixed point spaces and reducibility are given. We also discuss results of computational experiments, including the calculation of shift orbit structure and searching for orthogonal cocycles.

---

\*Corresponding author (r.egan3@nuigalway.ie)

2010 Mathematics Subject Classification: 20J06, 20H30, 20B25, 05B20

Keywords: cocycle, orthogonality, representation, shift action

# 1 Introduction

In [10], Horadam defines the *shift action* of a finite group  $G$  on the set of its 2-cocycles with trivial coefficients in an abelian group  $U$ . This action originates from equivalence of well-known objects in cocyclic design theory (see [2, Chapters 13, 15] and [9, Chapter 7]).

For example, let  $U = \langle -1 \rangle \cong C_2$ ; a cocycle  $\psi : G \times G \rightarrow U$  is *orthogonal* if  $H = [\psi(g, h)]_{g, h \in G}$  is a Hadamard matrix, i.e.,  $HH^\top = nI_n$  where  $n = |G|$ . Any such cocycle yields a relative difference set in the corresponding central extension of  $U$  by  $G$  with forbidden subgroup  $U$ , and vice versa [3]. These extensions, called *Hadamard groups*, were studied by Ito [11] using sophisticated algebraic techniques (see also [7]).

Orthogonal cocycles have diverse applications [9]. Moreover, de Launey and Horadam conjecture that there exists a cocyclic Hadamard matrix at every order  $n = 4t$  [9, p. 134]. It is unfortunate, then, that orthogonality and cohomological equivalence are incompatible: cocycles from the same cohomology class as an orthogonal cocycle need not themselves be orthogonal. A naive search for orthogonal cocycles would therefore run over the full cocycle space, whose size depends exponentially on  $|G|$ , rather than over the very much smaller space of cohomology classes. On the other hand, shift action respects both orthogonality and cohomological equivalence. That is, cocycles lying in the same shift orbit are cohomologous, and they are all orthogonal if any one of them is.

Shift action is consequently an important tool in the study of cocyclic pairwise combinatorial designs and their applications. We introduce and develop a representation-theoretic variant of this action, which allows us to treat it in a practical way: via matrix groups acting on an underlying vector space of reasonable dimension. To this end, we provide a comprehensive description of complete reducibility and fixed points for shift representations. Our paper extends the reach of previous work such as [12], and is a starting point for further investigation of shift action in a computationally tractable setting.

We now summarize the content of the paper. In Section 2 we prove elementary facts about shift representations. The main results of Section 3 are a determination of fixed points under shift action in the full cocycle space, and a bound on the dimension of the fixed coboundary space. We thereby solve most of Research Problem 55 (1) in [9]. Some relevant linear group theory is then given in Section 4. This serves as background for Section 5, where we establish that a shift represen-

tation is hardly ever completely reducible. In fact, we provide criteria for deciding irreducibility and complete reducibility. As an illustration of the practical nature of our approach, in the final section we describe new results obtained from our MAGMA [1] implementation of procedures to compute with shift representations. Open questions arising from the computational work are posed.

We remark that the machinery set up in this paper has been applied successfully in a recent classification of Butson Hadamard matrices of order  $n$  over  $p$ th roots of unity, for  $p$  prime and  $np \leq 100$  [5].

## 2 Preliminaries

Let  $G$  and  $U$  be finite non-trivial groups, with  $U$  abelian. A map  $\phi : G^n \rightarrow U$  is *normalized* if  $\phi(x) = 1$  whenever  $x$  has 1 in at least one component. We denote by  $F(G^n, U)$  the abelian group of normalized maps  $G^n \rightarrow U$  under pointwise multiplication. A *cocycle* is an element  $\psi$  of  $F(G^2, U)$  such that

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

The cocycles form a subgroup  $Z(G, U) \leq F(G^2, U)$ . If  $\phi \in F(G, U)$  then  $\partial\phi \in Z(G, U)$  defined by

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

is a *coboundary*. The map  $\partial : F(G, U) \rightarrow Z(G, U)$  is a homomorphism with kernel  $\text{Hom}(G, U) \cong \text{Hom}(G/G', U)$  where  $G' = [G, G]$ . Put  $\text{im } \partial = B(G, U)$ . The elements of  $H(G, U) = Z(G, U)/B(G, U)$  are *cohomology (equivalence) classes*; equivalent elements of  $Z(G, U)$  are *cohomologous*. If  $|G|, |U|$  are coprime (for example) then  $H(G, U) = 0$ .

For  $\psi \in Z(G, U)$  and  $a, g \in G$ , set  $\psi_a(g) = \psi(a, g)$ . Using (1) we verify that  $\psi_a\psi_b(\partial(\psi_a))_b = \psi_{ab}$ , so

$$\psi a = \psi \partial(\psi_a) \quad (2)$$

defines an action of  $G$  on  $Z(G, U)$  [10, Section 3]. This *shift action* obviously preserves cohomological equivalence.

Let  $\Gamma$  be the permutation representation  $G \rightarrow \text{Sym}(Z(G, U))$  associated to (2). If  $S \subseteq Z(G, U)$  is  $\Gamma(G)$ -invariant then  $\Gamma_S$  will denote the restricted representation of  $G$  in  $\text{Sym}(S)$ .

**Lemma 2.1.** *Suppose that  $S$  is a  $\Gamma(G)$ -invariant subgroup of  $Z(G, U)$ . Then  $\Gamma_S$  is a homomorphism  $G \rightarrow \text{Aut}(S)$ .*

*Proof.* For  $\psi, \mu \in S$  and  $a \in G$ ,

$$(\psi\mu)a = \psi\mu\partial((\psi\mu)_a) = \psi\mu\partial(\psi_a\mu_a) = \psi\partial(\psi_a)\mu\partial(\mu_a) = \psi_a\mu_a.$$

Since  $\Gamma_S(a)$  is bijective, it is therefore an automorphism of  $S$ .  $\square$

Now let  $S$  be a subgroup of  $Z(G, U)$  containing  $B(G, U)$ ; so  $S$  is  $\Gamma(G)$ -invariant. (Note that  $S$  could be  $B(G, U)$  itself.) By Lemma 2.1 we obtain a *shift representation*  $\Gamma_S$  of  $G$  in  $\text{Aut}(S)$ . We demonstrate that  $\Gamma_S$  is nearly always faithful, i.e., has trivial kernel.

**Lemma 2.2.** *Suppose that  $|G| \geq 5$ . For any  $\mu \in Z(G, U)$ ,  $\Gamma_{\mu B(G, U)}$  is faithful.*

*Proof.* If  $\Gamma_{\mu B(G, U)}(a) = 1$  then  $(\mu\psi)_a = \mu_a\psi_a$  is a homomorphism for all  $\psi \in B(G, U)$ . Thus  $\mu_a$  and so  $\psi_a$  are homomorphisms. It follows that

$$\phi(ag)\phi(ah)\phi(gh) = \phi(a)\phi(g)\phi(h)\phi(agh) \quad (3)$$

for all  $\phi \in F(G, U)$  and  $g, h \in G$ . Setting  $g = a^{-1}$  and then  $h = a^{-1}$  in (3), and combining, gives

$$\phi(g)\phi(ga^{-1}) = \phi(a^{-1}g)\phi(aga^{-1}). \quad (4)$$

Suppose  $\exists g \in G \setminus C_G(a)$ , and choose  $\phi$  so that  $\phi(g) = \phi(a^{-1}g) = \phi(aga^{-1}) = 1$ . If  $a \neq 1$  then  $ga^{-1} \notin \{1, g, a^{-1}g, aga^{-1}\}$ , so we can insist that  $\phi(ga^{-1}) \neq 1$ . Since this contradicts (4), we must have  $a \in Z(G)$ .

Let  $g \notin \{1, a^{-1}\}$ ,  $h \notin \{1, a, g, ag\}$ , and  $\phi(ag) \neq 1$ . If  $a \neq 1$  then  $ag \notin T := \{ah, gh, a, g, h, agh\}$ , leaving us free to choose  $\phi$  to be 1 on  $T$ . But then  $\phi(ag) = 1$  by (3).  $\square$

*Remark 2.3.* 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.

**Corollary 2.4.** *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  $\text{Aut}(S)$ .*

Usually, when discussing shift representations  $\Gamma$  or  $\Gamma_B = \Gamma_{B(G,U)}$ , it is implicit that they are faithful. Then we identify  $G$  with  $\Gamma(G)$  or  $\Gamma_B(G)$ .

We have

$$Z(G, U) \cong U^{|G|-1} \times \text{Hom}(H_2(G), U),$$

$H_2(G)$  denoting the Schur multiplier of  $G$  [2, 20.6.4, p. 246]. Suppose that  $U$  is an elementary abelian  $p$ -group. By additivity of  $Z(G, -)$ , it suffices to assume that  $U \cong C_p$  (we expand on this comment in Section 4). So  $Z(G, U)$  is a vector space of dimension  $n = |G| + r - 1$  over the field  $\mathbb{F}_p$  of size  $p$ , where  $r$  is the rank of the Sylow  $p$ -subgroup of  $H_2(G)$ . Hence  $\text{Aut}(Z(G, U)) \cong \text{GL}(n, p)$ , the general linear group of invertible  $n \times n$  matrices over  $\mathbb{F}_p$ . Also  $B(G, U) \cong F(G, U)/\text{Hom}(G/G', U)$  is an  $\mathbb{F}_p$ -vector space of dimension  $|G| - s - 1$ , where  $s$  is the rank of the Sylow  $p$ -subgroup of  $G/G'$ .

**Theorem 2.5.** *Suppose that  $|G| = m \geq 5$  and  $U$  has prime order  $p$ . Then  $\Gamma, \Gamma_B$  are faithful representations of  $G$  in  $\text{GL}(m + r - 1, p)$  and  $\text{GL}(m - s - 1, p)$  respectively.*

The explicit matrix representation of  $G$  depends on the choice of basis; varying this choice gives conjugate linear groups.

**Example 2.6.** Let  $AS(G, U) = \{\psi \in Z(G, U) \mid \psi(g, h) = \psi(h, g) \text{ if } gh = hg\}$ , the group of almost symmetric cocycles. Clearly  $B(G, U) \leq AS(G, U)$ . When  $G$  is abelian,  $AS(G, U)/B(G, U) \cong \text{Ext}(G/G', U)$  in the Universal Coefficient Theorem decomposition of  $H(G, U)$  [2, p. 255]. It is unknown whether this isomorphism holds for non-abelian  $G$  [6, Section 4]. The representation  $\Gamma_{AS(G, C_p)}$  has degree at least  $|G| - 1$ .

**Example 2.7.** Let  $M(G, U) = \text{Fix}(G) := \{\psi \in Z(G, U) \mid \psi a = \psi \forall a \in G\}$ , the group of cocycles multiplicative in one and hence both components [10, pp. 131–132]. The restricted representation  $\Gamma_M$  is trivial. One familiar instance of a multiplicative cocycle is a bilinear form.

We note the link to designs. As per [10, Section 5],  $\psi \in Z(G, U)$  is *orthogonal* if  $|\psi_g^{-1}(u)|$  is constant for all  $g \in G \setminus \{1\}$  and  $u \in U$ . Thus, for  $\psi$  to be orthogonal,  $|U|$  has to divide  $|G|$ .

**Example 2.8.** Let  $U = \langle -1 \rangle$ ; then  $\psi$  is orthogonal precisely when  $[\psi(g, h)]_{g, h \in G}$  is a Hadamard matrix. Here  $|\psi_g^{-1}(u)| = |G|/2$ .

**Theorem 2.9.**  $\psi \in Z(G, U)$  is orthogonal if and only if  $\psi\partial(\psi_a)$  is orthogonal for all  $a \in G$ .

*Proof.* See [9, Lemma 8.4, p. 165]. □

The orthogonal elements of  $Z(G, U)$  form a  $\Gamma(G)$ -invariant subset, but not subgroup. When  $U$  is elementary abelian, this set is partitioned into shift orbits of 1-dimensional subspaces.

### 3 Fixed points

Before considering linear properties of shift representations, we look at fixed points under shift action. We construct the fixed point space of all cocycles, and prove a lower bound on the dimension of the fixed point coboundary space (which is achieved for abelian groups). This solves most of Research Problem 55 (1) in [9]; see Theorems 3.5 and 3.8 below.

Let  $\text{Fix}(K)$ ,  $\text{Fix}_B(K)$  denote the set of  $K$ -fixed points in  $Z(K, U)$ ,  $B(K, U)$  respectively.

**Lemma 3.1.** (i) Every 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.* Certainly  $\psi(g, -), \psi(-, g) \in \text{Hom}(G, U)$  for  $\psi \in \text{Fix}(G)$ , and both parts are consequences of this. □

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

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

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—however, see the paragraph before Lemma 3.6 below.

**Lemma 3.2.**  $\text{Fix}(G) \cong \text{Fix}(G/G')$ .

*Proof.* For each  $\psi \in \text{Fix}(G)$ , set  $\tilde{\psi}(gG', hG') = \psi(g, h)$ ; by Lemma 3.1 (i),  $\tilde{\psi} \in \text{Fix}(G/G')$ . It is readily checked that  $\psi \mapsto \tilde{\psi}$  defines an isomorphism with inverse  $\text{inf} : Z(G/G', U) \rightarrow Z(G, U)$  on  $\text{Fix}(G/G')$ . □

*Remark 3.3.* 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 3.2 need not map  $\text{Fix}_B(G)$  into  $B(G/G', U)$ .

**Proposition 3.4.** *Suppose that  $U$  is a cyclic  $p$ -group, and  $G$  a finite abelian  $p$ -group of rank  $r$ . Then  $\text{Fix}(G) \cong U^{r^2}$ .*

*Proof.* Let  $G = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle$  and  $|U| = p^s$ . Since  $\psi \in \text{Fix}(G)$  is multiplicative,  $\psi \mapsto (\psi(x_i, x_j))_{ij}$  defines an injective homomorphism between  $\text{Fix}(G)$  and the additive abelian group  $\text{Mat}(r, U)$ . In the opposite direction,  $\text{Mat}(r, U)$  embeds into  $\text{Fix}(C_p^r)$ : define  $\psi_M \in \text{Fix}(C_p^r)$  for  $M \in \text{Mat}(r, U)$  by  $\psi_M(x, y) = \epsilon(x)M\epsilon(y)^\top$ , where  $\epsilon(z)$  is the exponent vector  $(a_1, \dots, a_r)$  of  $z = x_1^{a_1} \cdots x_r^{a_r}$ ,  $0 \leq a_i \leq p-1$  ( $\psi_M$  is the bilinear form corresponding to  $M$  over  $\mathbb{Z}_{p^s}$ ). Thus  $\text{Fix}(C_p^r) \cong U^{r^2}$ . Finally, inflation embeds  $\text{Fix}(C_p^r)$  into  $\text{Fix}(G)$ , and the proof is complete.  $\square$

Let  $\mathcal{S}$  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  $U$ .

**Theorem 3.5.**  $\text{Fix}(G) \cong \prod_{p \in \mathcal{S}} U_p^{r_p^2}$ .

*Proof.* Additivity of  $Z(K, -)$  and Lemmas 3.1 (ii), 3.2 permit us to assume that  $G$  is abelian and replace  $U$  by  $\prod_{p \in \mathcal{S}} U_p$ . Also, restriction of  $\text{Fix}(X \times Y)$  to  $\text{Fix}(X)$  is an isomorphism if  $|Y|$  and  $|U|$  are coprime. Now use Proposition 3.4.  $\square$

Our analysis of  $\text{Fix}_B(G)$  uses the fact that inflation is an isomorphism of  $\text{Ext}(G/G', U) \leq H(G/G', U)$  onto a subgroup  $I(G, U)$  of  $H(G, U)$ .

**Lemma 3.6.** *Suppose that  $U$  is a cyclic  $p$ -group for an odd prime  $p$  dividing  $|G : G'|$  but not  $|G'|$ . Then  $[\psi] \cap \text{Fix}(G) = \emptyset$  for all non-trivial  $[\psi] \in I(G, U)$ .*

*Proof.* We first recap some material from [8, 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

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 & u \\ 1 & 1 & 1 & \cdots & 1 & u & u \\ \vdots & \vdots & & \ddots & & \vdots & \vdots \\ 1 & 1 & u & \cdots & u & u & u \\ 1 & u & u & \cdots & u & u & u \end{pmatrix}.$$

Then put

$$N_i = J_{p^{\epsilon_1+\dots+\epsilon_{i-1}}} \otimes M_i \otimes J_{p^{\epsilon_{i+1}+\dots+\epsilon_n}} \otimes J_{|K|},$$

$J_d$  denoting the  $d \times d$  all 1s matrix. The rows and columns of  $M_i$  are indexed  $1, g_i, \dots, g_i^{p^{\epsilon_i}-1}$ ; while  $N_i$  is indexed by the ‘Kronecker product’

$$\{1, g_1, \dots, g_1^{p^{\epsilon_1}-1}\} \otimes \dots \otimes \{1, g_n, \dots, g_n^{p^{\epsilon_n}-1}\} \otimes K$$

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  $\psi \partial \phi(g_k, g_k) = \psi_k^s \partial \phi(g_k, g_k) = u^m$  say, for some  $k$  and  $1 \leq s < \min\{p^{\epsilon_k}, |u|\}$ . Write  $g$  for  $g_k$  and  $e$  for  $\epsilon_k$ . 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  $\partial \phi(g, g^j) = u^{jm}$ . Hence

$$\prod_{j=1}^{p^e-1} \partial \phi(g, g^j) = u^{(\sum_{j=1}^{p^e-1} j)m-s}.$$

Furthermore  $\sum_{j=1}^{p^e-1} j \equiv 0 \pmod{p^e}$ . So

$$\begin{aligned} \prod_{j=1}^{p^e-1} \phi(g)^{-1} \cdot \prod_{j=1}^{p^e-1} \phi(g^j)^{-1} \cdot \prod_{j=1}^{p^e-1} \phi(g^{j+1}) &\in u^{-s} U^{p^e} \\ \implies \phi(g^{p^e}) &\in u^{-s} U^{p^e}. \end{aligned}$$

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

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

Since  $r$  is coprime to  $p$ , this implies that  $u^s \in U^{p^e}$ : a contradiction, proving the lemma.  $\square$

*Remark 3.7.* As further preparation for the next theorem, we note that when  $G$  is an abelian 2-group, and  $\psi_i, s$  are as in the above proof,  $[\psi_i^s] \cap \text{Fix}(G) = \emptyset$  if and only if  $e_i > 1$  or  $|U| > 2$ .

**Theorem 3.8.** *Let  $G$  be abelian. In the notation defined just before Theorem 3.5,  $\text{Fix}_B(G) \cong \prod_{p \in \mathcal{S}} U_p^{s_p}$  where*

- (i)  $s_p = \binom{r_p+1}{2}$  if  $p$  is odd or  $|U_p| > 2$ ,
- (ii)  $s_2 = \binom{r_2+1}{2} - k$  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 3.5 and its proof.) Since

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

where  $G_p$  is the Sylow  $p$ -subgroup of  $G$ , we assume that  $G, U$  are  $p$ -groups with  $U$  cyclic. Next,  $I(G, U) = AS(G, U)/B(G, U)$  and  $\text{Fix}_B(G) \leq F := \text{Fix}(G) \cap AS(G, U)$ . As the proof of Proposition 3.4 shows,  $F$  is bijective with the set of symmetric elements of  $\text{Mat}(r, U)$ . Now everything follows from Lemma 3.6 and Remark 3.7.  $\square$

It remains to determine  $s_p$  precisely for non-abelian  $G$ . We return to the problem of calculating  $\text{Fix}_B(G)$  in Section 6.

## 4 Shift representations via linear groups

Our purpose in this section is to outline some basic linear group theory (as in, e.g., [4, Chapters 1 and 2]) relevant to the study of shift representations.

Let  $H \leq \text{GL}(n, \mathbb{F})$  for any field  $\mathbb{F}$ , and let  $V$  be the underlying  $n$ -dimensional  $\mathbb{F}$ -vector space. An  $H$ -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  $H$  *ir/reducible* when  $V$  is *ir/reducible*. Note that  $H$  is conjugate to a group of block triangular matrices with irreducible diagonal blocks. A *completely reducible*  $H$ -module is a direct sum of irreducible submodules; if  $V$  is completely reducible then we say that  $H$  is too. In that event  $H$  has a block diagonal conjugate in  $\text{GL}(n, \mathbb{F})$  with irreducible diagonal blocks.

**Theorem 4.1** (Clifford). *A normal subgroup of a completely reducible group is completely reducible.*

**Theorem 4.2** (Maschke). *A finite subgroup of  $\mathrm{GL}(n, \mathbb{F})$  of order coprime to  $\mathrm{char} \mathbb{F}$  is completely reducible.*

We obtain a reduction to completely reducible groups in many cases. To elucidate, suppose that  $H \leq \mathrm{GL}(n, \mathbb{F})$  is block triangular with irreducible diagonal blocks. The kernel of projection onto the block diagonal is the unipotent radical  $U(H)$  of  $H$ , i.e., its largest unipotent normal subgroup (a unipotent subgroup of  $\mathrm{GL}(n, \mathbb{F})$  consists of unipotent matrices, so may be conjugated to a unitriangular group.) If  $H$  is completely reducible then  $U(H) = 1$ ; if  $U(H) = 1$  then  $H$  is isomorphic to a completely reducible subgroup of  $\mathrm{GL}(n, \mathbb{F})$ .

Let  $\mathrm{char} \mathbb{F} = p$ .

**Lemma 4.3.** *A  $p$ -subgroup  $P \neq 1$  of  $\mathrm{GL}(n, \mathbb{F})$  is unipotent, so has non-trivial fixed points in  $V$ , and every irreducible  $P$ -module is 1-dimensional.*

**Corollary 4.4.** *If  $H$  has a non-trivial normal  $p$ -subgroup then  $H$  is not completely reducible.*

**Corollary 4.5.** *A nilpotent subgroup  $H$  of  $\mathrm{GL}(n, \mathbb{F})$  is completely reducible if and only if  $p$  does not divide  $|H|$ .*

**Lemma 4.6.** *Let  $|\mathbb{F}| = q$ . An abelian subgroup of  $\mathrm{GL}(n, \mathbb{F})$  is irreducible if and only if it is cyclic of order dividing  $q^n - 1$  but not  $q^k - 1$  for  $k < n$ . At each order, the irreducible abelian subgroups of  $\mathrm{GL}(n, \mathbb{F})$  form a single conjugacy class.*

We now focus on (faithful) shift representations.

**Lemma 4.7.** *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.* For each direct factor  $U_i \cong C_p$  of  $U$ , the subgroup  $Z(G, U_i)$  of  $Z(G, U)$  is a  $G$ -module, because its elements are the cocycles that map into  $U_i$ .  $\square$

In the situation of Lemma 4.7,  $G \leq \mathrm{GL}(d, p)$  is conjugate to a block diagonal group  $\{(\alpha(g), \dots, \alpha(g)) \mid g \in G\}$  where  $d = \dim_{\mathbb{F}_p}(Z(G, U))$  and  $\alpha$  is a homomorphism  $G \rightarrow \mathrm{GL}(d/r, p)$ . So the shift representation theory of  $Z(G, U)$

reduces to that of  $Z(G, C_p)$ . If  $U$  is not elementary abelian then we may encounter shift representations over the ring  $\mathbb{Z}_{p^a}$ ,  $a > 1$ .

Remember that orthogonal cocycles in  $Z(G, U)$  can exist only if  $|U|$  divides  $|G|$ ; which is frequently our working assumption. Observe also 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.

**Lemma 4.8.** *Suppose that  $Z(G, C_p)$  is completely reducible. Then  $Z(G, C_p) = B(G, C_p) \oplus W$  for some  $W \leq \text{Fix}(G)$  isomorphic to  $H(G, C_p)$ . Hence each non-trivial element of  $H(G, C_p)$  contains a fixed point that is not a coboundary.*

*Proof.* Since  $Z(G, C_p)$  is completely reducible,  $Z(G, C_p) = B(G, C_p) \oplus W$  for some  $G$ -submodule  $W$ . By definition  $\psi a \in W$  is cohomologous to  $\psi$  for all  $\psi \in W$  and  $a \in G$ : thus  $\psi a = \psi$ .  $\square$

**Corollary 4.9.** *If  $p$  is an odd prime dividing  $|G : G'|$  but not  $|G'|$  then  $Z(G, C_p)$  is not completely reducible.*

*Proof.* Apply Lemmas 3.6 and 4.8.  $\square$

Complete reducibility of  $\Gamma$  and  $\Gamma_B$  (i.e., of  $\Gamma(G)$ ,  $\Gamma_B(G)$ ) is explored fully in the next section.

## 5 Completely reducible shift representations

We first settle the question of when  $\Gamma_B(G)$  can be irreducible. Theorems 5.10, 5.11, and 5.17 then cover the harder problem of deciding complete reducibility.

**Lemma 5.1.** *Inflation  $Z(G/N, U) \rightarrow Z(G, U)$  maps each  $G/N$ -invariant subgroup of  $Z(G/N, U)$  isomorphically onto a  $G$ -invariant subgroup of  $Z(G, U)$ .*

*Proof.* A routine calculation shows that  $\inf(\psi)a = \inf(\psi aN)$ , from which the claim is immediate.  $\square$

For the rest of this section,  $U = \langle u \rangle \cong C_p$ .

**Corollary 5.2.** *If  $Z(G, U)$  (resp.  $B(G, U)$ ) is completely reducible then each  $G/N$ -submodule of  $Z(G/N, U)$  (resp.  $B(G/N, U)$ ) is completely reducible.*

We proceed to determine the irreducible  $\Gamma_B(G)$ .

**Proposition 5.3.** *Suppose that  $B(G, U)$  is irreducible. Then  $G$  is simple and  $p \nmid |G|$ .*

*Proof.* The first assertion is another consequence of Lemma 5.1.

Suppose that  $p$  divides  $|G|$ . By Corollary 4.5 and Lemma 4.3,  $G$  is not abelian, and 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

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

However,  $p^{s-1}(p-1) \geq s+1$  for all valid  $p, s$ . □

Order the non-identity elements  $g_1, \dots, g_n$  of  $G$ , and define  $\phi_i \in F(G, U)$  by  $\phi_i(g_j) = u^{\delta_{ij}}$ . The  $\phi_i$ s comprise an  $\mathbb{F}_p$ -basis of  $F(G, U)$ . Let  $\{\phi_1^{\epsilon_{1,1}} \cdots \phi_n^{\epsilon_{1,n}}, \dots, \phi_1^{\epsilon_{s,1}} \cdots \phi_n^{\epsilon_{s,n}}\}$  be a basis of  $\text{Hom}(G, U)$ , where  $0 \leq \epsilon_{i,j} \leq p-1$ . If  $\varphi_i = \partial\phi_i$  then

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

is a presentation of  $B(G, U)$ . From this we extract a basis  $\mathcal{B}(G, U) = \{\partial\mu_1, \dots, \partial\mu_m\}$  of  $B(G, U)$ .

**Lemma 5.4.** *For any  $a, g \in G$  and  $\phi \in F(G, U)$ ,  $(\partial\phi)a = \partial\bar{\phi}$  where  $\bar{\phi}(g) = \phi(ag)\phi(a)^{-1}$ .*

We find  $\Gamma_B(a)$  with respect to  $\mathcal{B}(G, U)$  as follows. Write  $\bar{\mu}_i \in F(G, U)$  in terms of the  $\phi_i$ . The relations in  $\text{Hom}(G, U)$  may be used to rewrite this expression in terms of the  $\mu_i$ , say  $\mu_1^{\eta_{i,1}} \cdots \mu_m^{\eta_{i,m}}$ . Then the  $i$ th row of the matrix in  $\text{GL}(m, p)$  representing  $\Gamma_B(a)$  is the exponent vector  $\eta_{i,1} \eta_{i,2} \cdots \eta_{i,m}$ .

**Lemma 5.5.** *Suppose that  $\text{Hom}(G, U) = 1$ . Then 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 5.4,  $\overline{\phi_i}(g) = \phi_i(g_j g)$  if  $i \neq j$ , whereas  $\overline{\phi_i}(g) = u^{-1}$  if  $i = j$ . That is,  $\overline{\phi_i} = \phi_l$  where  $g_i = g_j g_l$  in the former cases, and  $\overline{\phi_i} = \phi_1^{-1} \cdots \phi_n^{-1}$  in the latter.  $\square$

Now we can pinpoint when the coboundary module is irreducible. The large (compared to  $|G|$ ) degree of such a representation again exerts a strong influence.

**Theorem 5.6.**  *$B(G, U)$  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 any  $k \leq n - 1$ .*

*Proof.* Let  $B(G, U)$  be irreducible, and suppose that  $G$  is non-abelian. So there exists  $g \in G$  such that  $|g| = t > 2$ . Say that our ordering of the elements of  $G$  begins with  $g, g^2, \dots, g^{t-1}$ , and let  $\alpha$  be the unimodular vector with 1 in position  $t - 1$ . By Lemma 5.5, if  $t < |G|$  then  $\beta = \alpha + \alpha g + \cdots + \alpha g^{t-1} \neq 0$ ; indeed  $\beta = (0, \dots, 0, -1, \dots, -1)$  where the initial  $-1$  appears in position  $t$ . Clearly  $\langle g \rangle$  fixes  $\beta$ . Thus  $|\beta G| \leq |G|/3$ , implying that  $\beta G$  spans a proper non-zero  $G$ -submodule of  $B(G, U)$ . Hence  $G$  must be abelian. Proposition 5.3 and Lemma 4.6 complete the proof.  $\square$

Our next task is to prove that  $\Gamma(G)$  and  $\Gamma_B(G)$  are almost never completely reducible.

Let  $H$  be a subgroup of  $\mathrm{GL}(d, \mathbb{F})$  with underlying space  $V$ . The *dual module*  $V^*$  of  $V$  is the  $d$ -dimensional  $\mathbb{F}$ -space  $\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ , where the action of  $H$  on  $V^*$  is defined by  $fx(v) = f(vx^{-1})$ . This action gives rise to a (‘contragredient’) representation  $\Lambda : H \rightarrow \mathrm{GL}(d, \mathbb{F})$ . For a suitable basis of  $V^*$ ,  $\Lambda(x) = (x^{-1})^\top$ .

**Lemma 5.7.** *If  $\mathrm{Hom}(G, U) = 1$  and  $p$  divides  $|G|$  then  $B(G, U)^*$  has non-trivial fixed points.*

*Proof.* By Lemma 5.5,  $\Lambda(G) = \Gamma_B(G)^\top$  fixes every element in the subspace spanned by the all 1s vector.  $\square$

**Lemma 5.8.** *Let  $V$  be a completely reducible  $H$ -module. Then  $V$  has non-trivial  $H$ -fixed points if and only if  $V^*$  does.*

*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  $f : aw + x \mapsto a$  for  $a \in \mathbb{F}$ ,  $x \in X$  then defines a non-trivial fixed point  $f$  in  $V^*$ . Since  $V^*$  is completely reducible and  $V \cong V^{**}$ , this proves the lemma.  $\square$

Henceforth  $p$  divides  $|G|$ .

**Proposition 5.9.** *If  $\text{Hom}(G, U) = 1$  then  $B(G, U)$  is not completely reducible.*

*Proof.* This follows from Lemmas 3.1 (ii), 5.7, and 5.8.  $\square$

**Theorem 5.10.** *Suppose that  $|G : G'| \geq 5$ , or  $G/G' \cong C_4$ , or  $G/G' \cong C_3$  and  $p \neq 3$ . Then  $\Gamma_B(G)$  is not completely reducible.*

*Proof.* With the aid of Lemma 5.4 it may be seen that  $|\Gamma_B(C_4)| \geq 2$  and  $\Gamma_B(C_3) = 1$  if and only if  $p = 3$ . Therefore, by Lemma 2.2,  $G$  (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 5.9. Otherwise Corollaries 4.5 and 5.2 give the result.  $\square$

The next theorem extends Corollary 4.9 significantly.

**Theorem 5.11.** *Suppose that 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 5.10 carries over, mutatis mutandis (heeding Remark 2.3).  $\square$

*Remark 5.12.*  $\Gamma(G)$  completely reducible implies  $\Gamma_B(G)$  completely reducible, so most of this theorem follows from the previous one anyway.

To round out the section, we provide a family of completely reducible shift representations as a partial converse of Theorems 5.10 and 5.11.

**Lemma 5.13.** *If  $\text{Hom}(K, U) = 1$  then the kernel  $W = \{\partial\lambda \mid \lambda_K = 1\}$  of the restriction map  $B(G, U) \rightarrow B(K, U)$  is a  $K$ -submodule of  $B(G, U)$ .*

Now suppose that  $U \cong C_2$ , and  $G = K \rtimes \langle h \rangle$  where  $|K| > 1$  is odd,  $|h| = 2$ , and  $h$  acts invertingly on  $K$ .

**Lemma 5.14.** *Let  $W$  be the  $K$ -submodule of  $V = B(G, U)$  as in Lemma 5.13. Then  $V = W \oplus Wh$ .*

*Proof.* First,  $\dim_{\mathbb{F}_2}(W) = \dim_{\mathbb{F}_2}(Wh) = \frac{1}{2}\dim_{\mathbb{F}_2}(V)$ . By Lemma 5.4, if  $\partial\lambda \in W \cap Wh$  then  $\partial\lambda = \partial\mu$  where  $\mu(hK)$  is constant and  $\mu_K = 1$ . For any such  $\mu$ ,  $\partial\mu = 1$ .  $\square$

**Corollary 5.15.**  $V$  is a direct sum  $\sum_{i=1}^r (W_i \oplus W_i h)$  of  $G$ -modules  $W_i \oplus W_i h$  where  $W_1, \dots, W_r$  are irreducible  $K$ -submodules of  $W$ .

Suppose that  $X$  is a proper non-zero  $G$ -submodule of  $W_i \oplus W_i h$ . Select  $v \in W_i$  and  $g \in K$  such that  $vg \neq v$  (we can do this because the only  $K$ -fixed point in  $W$  is the zero vector). Since projection of  $W_i \oplus W_i h$  onto  $W_i h$  restricted to  $X$  is surjective, there exists  $u \in W_i$  such that  $u + vh \in X$ . Let  $Y$  be the span of  $aK$  where  $a := ug + vgh$ . Notice that  $a \notin X$ . Thus  $Y$  is a non-zero  $K$ -submodule of  $W_i \oplus W_i h$  not contained in  $X$ .

**Lemma 5.16.** If  $K$  is abelian then  $Y$  is a  $G$ -module.

*Proof.* We have  $v = \sum_{c \in K} e_c u c$  for some  $e_c \in \mathbb{F}_2$ . Hence  $v + \sum_{c \in K} e_c v c^{-1} h = \sum_c e_c (u + vh) c \in X$ . Since  $uh + v \in X$ , this forces  $u = \sum_c e_c v c^{-1}$ . Therefore

$$ah = ugh + vg = \left( \sum_{c \in K} e_c v g h c \right) + \sum_{c \in K} e_c u g c = \sum_c e_c a c \in Y$$

as desired. □

It is easy to see that  $X, Y, W_i$  are of the same dimension. Also  $X \cap Y = 0$ : thus  $W_i \oplus W_i h = X \oplus Y$ . We conclude that  $B(G, C_2)$  is a completely reducible  $G$ -module. Since  $Z(G, C_2)$  splits over  $B(G, C_2)$  by a 1-dimensional fixed point space, this proves

**Theorem 5.17.** Suppose that  $G = K \rtimes \langle h \rangle$ , where  $K \neq 1$  is odd order abelian and the involution  $h$  inverts  $K$  elementwise. Then  $\Gamma(G)$  is completely reducible.

## 6 Computing with shift representations

Building on work by E. A. O'Brien and the first author, we have implemented a suite of MAGMA procedures for computing with the shift representation of  $G$  in  $\text{GL}(Z(G, U))$  and  $\text{GL}(B(G, U))$  for an elementary abelian group  $U$ . In this section we discuss the output of several computational experiments dealing with fixed points, complete reducibility, the orbit structure of  $Z(G, U)$ , and orthogonal cocycles.

We explained after Lemma 5.4 how to compute  $\Gamma_B(G)$ . Suppose that  $\{\partial\mu_1, \dots, \partial\mu_m\}$  is a basis of  $B(G, U)$ . We extend this to a basis  $\{\psi_1, \dots, \psi_n, \partial\mu_1, \dots,$

$\partial\mu_m\}$  of  $Z(G, U)$  by the method in [8, Section 2]. If  $\psi_i a = \psi_i \partial\phi$  for  $\partial\phi = \mu_1^{\eta_{i,1}} \cdots \mu_m^{\eta_{i,m}}$  then

$$\Gamma(a) = \begin{pmatrix} 1_n & M \\ 0_{m \times n} & \Gamma_B(a) \end{pmatrix},$$

where the  $i$ th row of  $M$  is  $\eta_{i,1} \cdots \eta_{i,m}$ .

## 6.1 Fixed points

Let  $U \cong C_p$  and let  $r$  be the rank of the Sylow  $p$ -subgroup of  $G/G'$ . Remark 3.3 implies a lower bound  $l_s$  for  $s = \dim_{\mathbb{F}_p}(\text{Fix}_B(G))$ :  $l_s = \binom{r+1}{2}$  and  $l_s = \binom{r+1}{2} - k$  in parts (i), (ii) respectively of Theorem 3.8. There are certainly groups  $G$  with  $s > l_s$ . Some examples, drawn from the MAGMA SmallGroups library, are given in Table 1 ( $D_m$  is the dihedral group of order  $2m$ ;  $Q_m$  is the generalized quaternion group of order  $2^m$ ).

$G$	SmallGroups label	$p$	$l_s$	$s$
$D_8$	(16,7)	2	1	2
$C_3 \rtimes Q_3$	(24,4)	2	1	2
$C_2^4 \rtimes C_2$	(32,27)	2	3	5
$(C_3 \times C_3) \rtimes C_3$	(27,3)	3	3	4
$(C_9 \times C_3) \rtimes C_3$	(81,3)	3	3	4
$C_5 \rtimes (C_5 \times C_5)$	(125,3)	5	3	4

Table 1: Dimensions of fixed coboundary spaces

We seek to characterize those  $G$  for which  $s = l_s$ .

## 6.2 Completely reducible representations

By Theorem 5.11,  $G$  seldom has a completely reducible shift representation  $\Gamma$  in characteristic  $p$  dividing  $|G|$ ; Theorem 5.17 demonstrates sufficient conditions for their existence. Computational searches suggest that these conditions are necessary too.

*Conjecture 6.1.* *Let  $U \cong C_p$ . Then  $\Gamma(G) \neq 1$  is completely reducible if and only if  $|G : G'| = p = 2$  and  $G'$  is abelian of odd order.*

The other possibility  $G/G' \cong U \cong C_3$  unaccounted for by Theorem 5.10 prompted more searches. The evidence points to

*Conjecture 6.2.* *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.*

At this stage it is worthwhile reviewing the interplay between existence of fixed points and complete reducibility. In the uninteresting case that  $p$  does not divide  $|G|$ , there are no fixed points at all by Lemma 3.1 (ii) (cf. the comment before [9, Corollary 8.44, p. 188]). Suppose that  $p$  divides  $|G : G'|$ . Fixed coboundaries exist for odd  $p$ , but  $B(G, U)$  can be completely reducible only if  $p = 3$  and  $\text{Fix}_B(G)$  is 1-dimensional. For  $p = 2$ , Theorem 5.17 furnishes completely reducible  $G$  with  $\text{Fix}(G)$  of dimension 1 and intersecting  $B(G, U)$  trivially.

### 6.3 Orbit structure

Although shift representations enable us to compute  $G$ -orbits in moderate degree, the number of orbits grows exponentially with  $|G|$ . Shift orbits in  $B(G, U)$  have been enumerated previously for cyclic and elementary abelian  $G$  [12, Section 4]. (Our  $G$ -module  $B(G, U)$  is isomorphic to a quotient of the group ring  $RG$  in [12].) We confirmed those listings, and in the tables below add some new examples in the full cocycle space  $Z(G, U)$ . The first row states orbit length and the second row gives the number of orbits of each length.

$B(C_3^2, C_3)$		
1	3	9
27	0	78

$Z(C_3^2, C_3)$		
1	3	9
81	216	2106

$Z(C_9, C_3)$		
1	3	9
3	8	726

$B(C_2^2 \times C_3, C_3)$					
1	2	3	4	6	12
3	15	24	12	360	4728

$B(D_4, C_2)$			
1	2	4	8
4	4	1	2

$Z(D_4, C_2)$			
1	2	4	8
16	16	36	8

$Z(D_8, C_2)$				
1	2	4	8	16
16	16	100	968	3584

## 6.4 Orthogonal cocycles

We often stipulate that  $U \cong C_p$  when handling shift representations algebraically. However, this may complicate a search for orthogonal cocycles. If  $U = \times_{j=1}^r U_j$  and  $\psi \in Z(G, U)$  is orthogonal then so too is each projection  $\psi_j \in Z(G, U_j)$ . (For a converse statement see [13, Theorem 3.4].) Suppose that  $Z(G, U_k)$  contains exactly  $t_k$  orthogonal cocycles; by testing a space of size  $t_1 \cdots t_r$  we will locate all orthogonal elements of  $Z(G, U)$ . The problem is most amenable when the  $U_k$  are isomorphic. For instance, much is known about orthogonal cocycles when  $G$  and  $U$  are both elementary abelian  $p$ -groups (see, e.g., [2, Chapter 21]).

As just a sample of the data that can be generated, Tables 2, 3, and 4 display the total number  $n$  of orthogonal cocycles found using shift orbits in  $Z(G, U)$  for various small  $G$  and  $|U| = 2$  or 3.

$G$	$C_2 \times C_4$	$C_2^2 \times C_3$	$C_2^2 \times C_4$	$C_4 \times C_4$	$C_2^2 \times C_5$	$C_2 \times C_8$
$n$	16	24	1984	192	120	96

Table 2:  $G$  abelian,  $|U| = 2$

$G$	$D_4$	$Q_3$	$D_6$	$\text{Alt}(4)$	$D_8$	$Q_4$	$D_{10}$
$n$	32	0	72	96	768	128	2200

Table 3:  $G$  non-abelian,  $|U| = 2$

$G$	$C_6$	$D_3$	$C_9$	$C_3^2$	$C_{12}$	$C_3 \times C_4$	$\text{Alt}(4)$	$D_6$	$C_2^2 \times C_3$	$C_{15}$
$n$	0	0	18	144	0	288	48	0	96	0

Table 4:  $|U| = 3$

Many cocycles in Tables 2 and 3 correspond to Hadamard equivalent matrices. Note that cocyclic Hadamard matrices of orders less than 40 were classified by Ó Catháin and Röder [14]. Tables 2 and 3 agree with results of that paper.

The majority of orthogonal cocycles tend to lie in orbits of maximal length. When  $U \cong C_2$  and  $G \cong C_2^2 \times C_m$  for  $m \in \{3, 5\}$ , orthogonal cocycles are in orbits of length  $|G|$ , and are of the form  $\psi_1 \cdots \psi_m \partial \phi$  where  $\{[\psi_1], \dots, [\psi_m]\}$  is a basis of  $H(G, U)$ . The orthogonal cocycles for  $G \cong D_6$  or  $D_{10}$  also lie in maximal orbits. This is consistent with [12, Theorem 12].

## Acknowledgments

R. Egan received support from the Irish Research Council (Government of Ireland Postgraduate Scholarship) and National University of Ireland, Galway (Hardiman Fellowship).

## References

- [1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265.
- [2] W. de Launey and D. L. Flannery, *Algebraic design theory*, Mathematical Surveys and Monographs vol. 175, American Mathematical Society, Providence, RI, 2011.
- [3] W. de Launey, D. L. Flannery, and K. J. Horadam, Cocyclic Hadamard matrices and difference sets, *Discrete Appl. Math.* **102** (2000), no.s 1-2, 47–61.
- [4] J. D. Dixon, *The structure of linear groups*, Van Nostrand Reinhold, New York, 1971.
- [5] R. Egan, D. L. Flannery, and P. Ó Catháin, Classifying cocyclic Butson Hadamard matrices, submitted (2014).
- [6] D. L. Flannery, Calculation of cocyclic matrices, *J. Pure Appl. Algebra* **112** (1996), no. 2, 181–190.
- [7] D. L. Flannery, Cocyclic Hadamard matrices and Hadamard groups are equivalent, *J. Algebra* **192** (1997), 749–779.
- [8] D. L. Flannery and E.A. O’Brien, Computing 2-cocycles for central extensions and relative difference sets, *Comm. Algebra* **28** (2000), 1939–1955.
- [9] K. J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, 2007.
- [10] K. J. Horadam, The shift action on 2-cocycles, *J. Pure Appl. Algebra* **188** (2004), no. 1-3, 127–143.

- [11] N. Ito, On Hadamard groups, *J. Algebra* **168** (1994), no. 3, 981–987.
- [12] A. LeBel, D. L. Flannery, and K. J. Horadam, Group algebra series and coboundary modules, *J. Pure Appl. Algebra* **214** (2010), no. 7, 1291-1300.
- [13] A. LeBel and K. J. Horadam, Direct sums of balanced functions, perfect nonlinear functions, and orthogonal cocycles, *J. Combin. Des.*, **16** (2008), no. 3, 173–181.
- [14] P. Ó Catháin and M. Röder, The cocyclic Hadamard matrices of order less than 40, *Des. Codes Cryptogr.* **58** (2011), no. 1, 73-88.