Shift Representations on 2-Cocycles

Ronan Egan*, Dane Flannery

School of Mathematics, Statistics and Applied Mathematics
Research Day 2015

*Supported by an NUI Galway Hardiman Scholarship and the Irish Research council

Overview

- Generalized Hadamard matrices
- Cocycles and orthogonality
- The shift action and linear shift representations
- Fixed points
- Reducibility
- Some computational results

Generalized Hadamard matrices

For n divisible by $|K|$, a *generalized Hadamard matrix* $\mathrm{GH}(n, K)$ *of order* n *over* K is an $n \times n$ matrix $H = [h_{ij}]$ whose entries h_{ij} lie in K and such that

$$HH^* = nI_n + \frac{n}{|K|}(\sum_{x \in K} x)(J_n - I_n)$$

where $H^* = [h_{ji}^{-1}]$, J_n is the all 1s matrix, and the matrix operations are performed over the group ring $\mathbb{Z}K$.

Generalized Hadamard matrices

For n divisible by $|K|$, a *generalized Hadamard matrix* $\mathrm{GH}(n, K)$ *of order* n *over* K is an $n \times n$ matrix $H = [h_{ij}]$ whose entries h_{ij} lie in K and such that

$$HH^* = nI_n + \frac{n}{|K|}(\textstyle\sum_{x \in K} x)(J_n - I_n)$$

where $H^* = [h_{ji}^{-1}]$, J_n is the all 1s matrix, and the matrix operations are performed over the group ring $\mathbb{Z}K$.

Example

Let $K = \mathrm{C}_3 = \langle a \rangle$, then H is a $\mathrm{GH}(3, K)$ where

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{pmatrix} \text{ and } H^* = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a^2 & a \\ 1 & a & a^2 \end{pmatrix}.$$

Cocycles and coboundaries

Let G and U be finite groups, U abelian. A map $\psi : G \times G \to U$ is a 2-*cocycle* (or cocycle) if

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

Cocycles and coboundaries

Let G and U be finite groups, U abelian. A map $\psi : G \times G \to U$ is a 2-*cocycle* (or cocycle) if

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

A $\mathrm{GH}(|G|, U)$, H is *cocyclic* if $H \approx [\psi(g,h)]_{g,h \in G}$.

Cocycles and coboundaries

Let G and U be finite groups, U abelian. A map $\psi : G \times G \to U$ is a 2-*cocycle* (or cocycle) if

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

A $\mathrm{GH}(|G|, U)$, H is *cocyclic* if $H \approx [\psi(g,h)]_{g,h \in G}$.

The cocycles form a subgroup $Z(G,U) \leq F^2(G,U)$. 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*.

Cohomology and Orthogonality

The coboundaries form a subgroup $B(G,U) \leq Z(G,U)$. The elements of $H(G,U) = Z(G,U)/B(G,U)$ are *cohomology (equivalence) classes*.

Cohomology and Orthogonality

The coboundaries form a subgroup $B(G,U) \leq Z(G,U)$. The elements of $H(G,U) = Z(G,U)/B(G,U)$ are *cohomology (equivalence) classes*.

Let $\psi_g : G \to U$ be given by $\psi_g(h) = \psi(g,h)$ for a cocycle ψ. Then ψ is *orthogonal* if $|\psi_g^{-1}(u)|$ is constant for all $g \in G \setminus \{1\}$ and $u \in U$. A cocycle of a Hadamard matrix is orthogonal.

Cohomology and Orthogonality

The coboundaries form a subgroup $B(G,U) \leq Z(G,U)$. The elements of $H(G,U) = Z(G,U)/B(G,U)$ are *cohomology (equivalence) classes*.

Let $\psi_g : G \to U$ be given by $\psi_g(h) = \psi(g,h)$ for a cocycle ψ. Then ψ is *orthogonal* if $|\psi_g^{-1}(u)|$ is constant for all $g \in G \setminus \{1\}$ and $u \in U$. A cocycle of a Hadamard matrix is orthogonal.

Cohomology does *NOT* preserve orthogonality!

The shift action

Let $a \in G$. Then

$$\psi \cdot a = \psi \partial \psi_a$$

defines the *shift action* of G on $Z(G, U)$.

The shift action

Let $a \in G$. Then

$$\psi \cdot a = \psi \partial \psi_a$$

defines the *shift action* of G on $Z(G, U)$.

The shift action preserves cohomology *and* orthogonality. That is, either all cocycles in an orbit under the shift action are orthogonal, or none are.

Linear shift representations

We know that

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

where $H_2(G)$ denotes the Schur multiplier of G.

Linear shift representations

We know that

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

where $H_2(G)$ denotes the Schur multiplier of G. Assume for now that $U \cong \mathrm{C}_p$ for a prime p. Then $Z(G,U)$ is a vector space of dimension $|G|+r-1$ over $\mathbb{F}_p$ where r is the rank of the Sylow p-subgroup of $H_2(G)$.

Linear shift representations

We know that

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

where $H_2(G)$ denotes the Schur multiplier of G. Assume for now that $U \cong \mathrm{C}_p$ for a prime p. Then $Z(G,U)$ is a vector space of dimension $|G|+r-1$ over $\mathbb{F}_p$ where r is the rank of the Sylow p-subgroup of $H_2(G)$.

Also $B(G,U) \cong F(G,U)/\mathrm{Hom}(G/G',U)$ is an $\mathbb{F}_p$-vector space of dimension $|G|-s-1$ where s is the rank of of the Sylow p-subgroup of G/G'.

Linear shift representations

Let Γ be the permutation representation $G \to \mathrm{Sym}(Z(G,U))$ associated to the shift action. If $S \leq Z(G,U)$ is $\Gamma(G)$-invariant then Γ_S will denote the restricted representation of G in $\mathrm{Sym}(S)$. We write $\Gamma = \Gamma_{Z(G,U)}$ and $\Gamma_B = \Gamma_{B(G,U)}$.

Linear shift representations

Let Γ be the permutation representation $G \to \mathrm{Sym}(Z(G,U))$ associated to the shift action. If $S \leq Z(G,U)$ is $\Gamma(G)$-invariant then Γ_S will denote the restricted representation of G in $\mathrm{Sym}(S)$. We write $\Gamma = \Gamma_{Z(G,U)}$ and $\Gamma_B = \Gamma_{B(G,U)}$.

Theorem

For $|G| = n \geq 5$, Γ and Γ_B are faithful representations of G in $\mathrm{GL}(n+r-1,p)$ and $\mathrm{GL}(n-s-1,p)$ respectively.

Fixed points

A cocycle ψ is *multiplicative* if $\psi(g,h)\psi(g,k) = \psi(g,hk)$ for all $g,h,k \in G$. The set of all multiplicative cocycles is a subgroup $M(G,U) \leq Z(G,U)$.

Fixed points

A cocycle ψ is *multiplicative* if $\psi(g,h)\psi(g,k) = \psi(g,hk)$ for all $g,h,k \in G$. The set of all multiplicative cocycles is a subgroup $M(G,U) \leq Z(G,U)$.

$$M(G,U) = \mathrm{Fix}(G) := \{\psi \in Z(G,U) \mid \psi \cdot a = \psi \ \forall\, a \in G\}.$$

Fixed points

A cocycle ψ is *multiplicative* if $\psi(g,h)\psi(g,k) = \psi(g,hk)$ for all $g,h,k \in G$. The set of all multiplicative cocycles is a subgroup $M(G,U) \leq Z(G,U)$.

$$M(G,U) = \mathrm{Fix}(G) := \{\psi \in Z(G,U) \mid \psi \cdot a = \psi \ \forall\, a \in G\}.$$

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

Fixed points

A cocycle ψ is *multiplicative* if $\psi(g,h)\psi(g,k) = \psi(g,hk)$ for all $g,h,k \in G$. The set of all multiplicative cocycles is a subgroup $M(G,U) \leq Z(G,U)$.

$$M(G,U) = \mathrm{Fix}(G) := \{\psi \in Z(G,U) \mid \psi \cdot a = \psi \ \forall\, a \in G\}.$$

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

Lemma

$\mathrm{Fix}(G) \cong \mathrm{Fix}(G/G')$.

Fixed points

A cocycle ψ is *multiplicative* if $\psi(g,h)\psi(g,k) = \psi(g,hk)$ for all $g,h,k \in G$. The set of all multiplicative cocycles is a subgroup $M(G,U) \leq Z(G,U)$.

$$M(G,U) = \mathrm{Fix}(G) := \{\psi \in Z(G,U) \mid \psi \cdot a = \psi \ \forall\, a \in G\}.$$

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

Lemma

$\mathrm{Fix}(G) \cong \mathrm{Fix}(G/G')$.

Proposition

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

Fixed points

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.

Fixed points

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

$\mathrm{Fix}(G) \cong \prod_{p \in \mathcal{S}} U_p^{r_p^2}$.

Fixed points

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

$\mathrm{Fix}(G) \cong \prod_{p \in \mathcal{S}} U_p^{r_p^2}$.

Theorem

Let G be abelian. Then $\mathrm{Fix}_B(G) \cong \prod_{p \in \mathcal{S}} U_p^{s_p}$ 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.*

Reducibility

Let $H \leq \mathrm{GL}(n, \mathbb{F})$ for any field $\mathbb{F}$, and let V be the underlying n-dimensional $\mathbb{F}$-vector space.

Reducibility

Let $H \leq \mathrm{GL}(n, \mathbb{F})$ 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*).

Reducibility

Let $H \leq \mathrm{GL}(n, \mathbb{F})$ 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*.

Reducibility

Let $H \leq \mathrm{GL}(n, \mathbb{F})$ 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*.
- A *completely reducible* H-module is a direct sum of irreducible submodules; if V is completely reducible then we say that H is too.

Irreducible shift representations

Lemma

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

Irreducible shift representations

Lemma

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

Hereafter let $U \cong \mathrm{C}_p$, and $|G| = n$.

Lemma

Suppose that $B(G, U)$ is irreducible. Then G is simple and $p \nmid n$.

Irreducible shift representations

Lemma

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

Hereafter let $U \cong \mathrm{C}_p$, and $|G| = n$.

Lemma

Suppose that $B(G, U)$ is irreducible. Then G is simple and $p \nmid n$.

Theorem

$B(G, U)$ 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 $k \leq n - 1$.

Complete reducibility

It turns out that that $\Gamma(G)$ and $\Gamma_B(G)$ are almost never completely reducible (when $n = mp$).

Complete reducibility

It turns out that that $\Gamma(G)$ and $\Gamma_B(G)$ are almost never completely reducible (when $n = mp$).

Theorem

Suppose that $|G : G'| \geq 5$, *or* $G/G' \cong \mathrm{C}_4$, *or* $G/G' \cong \mathrm{C}_3$ *and* $p \neq 3$. *Then* $\Gamma_B(G)$ *is not completely reducible.*

Complete reducibility

It turns out that that $\Gamma(G)$ and $\Gamma_B(G)$ are almost never completely reducible (when $n = mp$).

Theorem

Suppose that $|G : G'| \geq 5$, or $G/G' \cong \mathrm{C}_4$, or $G/G' \cong \mathrm{C}_3$ and $p \neq 3$. Then $\Gamma_B(G)$ is not completely reducible.

Theorem

Suppose that either $p > 2$ or $G/G' \ncong \mathrm{C}_2, \mathrm{C}_2^2$. Then $\Gamma(G)$ is not completely reducible.

The exceptional case

Let $U = \mathrm{C}_2$.

The exceptional case

Let $U = \mathrm{C}_2$.

Theorem

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.

The exceptional case

Let $U = \mathrm{C}_2$.

Theorem

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.

In particular, this includes dihedral groups of order $n \equiv 2 \mod 4$.

Some computational results

In the tables below add some new examples of the orbit structure 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

Some computational results

The tables below 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

G abelian, $|U| = 2$

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

G non-abelian, $|U| = 2$

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

$|U| = 3$

An application

An $n \times n$ matrix H with entries in the kth roots of unity is a $\mathrm{BH}(n, k)$ (*Butson Hadamard matrix*) if

$$HH^* = nI_n$$

where H^* is the conjugate transpose of H.

An application

An $n \times n$ matrix H with entries in the kth roots of unity is a $\mathrm{BH}(n, k)$ (*Butson Hadamard matrix*) if

$$HH^* = nI_n$$

where H^* is the conjugate transpose of H.

We classify up to equivalence all cocyclic Butson Hadamard matrices over pth roots of unity for an odd prime p, and $np \leq 100$.

References

- Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24**, 235-265, 1997.
- Warwick de Launey and Dane Flannery, *Algebraic design theory*, Mathematical Surveys and Monographs, vol. 175, American Mathematical Society, Providence, RI, 2011.
- R. Egan, D. L. Flannery, and P. Ó Catháin, Classifying cocyclic Butson Hadamard matrices, Springer Proceedings in Mathematics and Statistics: Algebraic Design Theory and Hadamard Matrices, to appear 2015.
- D. L. Flannery, *Calculation of cocyclic matrices*, J. Pure Appl. Algebra **112** (1996), no. 2, 181–190.
- D. L. Flannery and R. Egan, On linear shift representations, J. Pure Appl. Algebra **219**, Issue 8, (2015), 3482–3494.
- K.J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, 2007.