Classifying cocyclic Butson Hadamard matrices

Ronan Egan*

Joint work with Dane Flannery and Padraig Ó Catháin.

July 23, CoCoA 2015.

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



$$HH^* = nI_n$$

where * denotes Hermitian transpose,

$$HH^* = nI_n$$

where * denotes Hermitian transpose, i.e., $H = [h_{ij}] \Rightarrow H^* = [h_{ji}^{-1}]$.

B b d B b

$$HH^* = nI_n$$

where * denotes Hermitian transpose, i.e., $H = [h_{ij}] \Rightarrow H^* = [h_{ij}^{-1}]$.



.

$$HH^* = nI_n$$

where * denotes Hermitian transpose, i.e., $H = [h_{ij}] \Rightarrow H^* = [h_{ji}^{-1}]$.



If k is prime, then k must divide n. If k = 2, H is a real Hadamard matrix, and for n > 2 it is known that n is a multiple of 4.

• • = • • = •

Butson matrices play a crucial role in Quantum Information Theory. A library of known Complex Hadamard matrices is kept up to date at the URL below.

http://chaos.if.uj.edu.pl/~karol/hadamard/

Butson matrices play a crucial role in Quantum Information Theory. A library of known Complex Hadamard matrices is kept up to date at the URL below.

http://chaos.if.uj.edu.pl/~karol/hadamard/

Real Hadamard matrices have been extensively studied, but Butsons have not.

Butson matrices play a crucial role in Quantum Information Theory. A library of known Complex Hadamard matrices is kept up to date at the URL below.

http://chaos.if.uj.edu.pl/~karol/hadamard/

Real Hadamard matrices have been extensively studied, but Butsons have not. We classify up to equivalence, all cocyclic BH(n, p)s for odd prime p, and $np \leq 100$. This includes generating previously unknown Butson matrices.

Let X and Y be BH(n, k)s. We say $X \approx Y$ are equivalent if MXN = Y for monomial matrices M and N with non-zero entries in $\langle \zeta_k \rangle$.

Let X and Y be BH(n, k)s. We say $X \approx Y$ are equivalent if MXN = Y for monomial matrices M and N with non-zero entries in $\langle \zeta_k \rangle$. If $M, N \in \text{Perm}(n)$, then $X \sim Y$ are permutation equivalent.

Let X and Y be BH(n, k)s. We say $X \approx Y$ are equivalent if MXN = Y for monomial matrices M and N with non-zero entries in $\langle \zeta_k \rangle$. If $M, N \in \text{Perm}(n)$, then $X \sim Y$ are permutation equivalent.

The direct product $\operatorname{Mon}(n, \langle \zeta_k \rangle) \times \operatorname{Mon}(n, \langle \zeta_k \rangle)$ acts on $\operatorname{BH}(n, k)$ via $(M, N)X = MXN^*$.

- The orbit of X under this action is its equivalence class.
- The stabilizer of X is its full automorphism group Aut(X).

Let X and Y be BH(n, k)s. We say $X \approx Y$ are equivalent if MXN = Y for monomial matrices M and N with non-zero entries in $\langle \zeta_k \rangle$. If $M, N \in \text{Perm}(n)$, then $X \sim Y$ are permutation equivalent.

The direct product $\operatorname{Mon}(n, \langle \zeta_k \rangle) \times \operatorname{Mon}(n, \langle \zeta_k \rangle)$ acts on $\operatorname{BH}(n, k)$ via $(M, N)X = MXN^*$.

- The orbit of X under this action is its equivalence class.
- The stabilizer of X is its full automorphism group Aut(X).

The subgroup of Aut(X) comprised of pairs of permutation matrices, is denoted by PermAut(X).

B b d B b

э

 $\psi(g,h)\psi(gh,f) = \psi(g,hf)\psi(h,f), \ \forall \ g,h,f \in G.$

B N A B N

$$\psi(g,h)\psi(gh,f) = \psi(g,hf)\psi(h,f), \ \forall \ g,h,f \in G.$$

 ψ is normalized if $\psi(g,1) = \psi(1,h) = 1$, for all $g,h \in G$,

B b d B b

$$\psi(g,h)\psi(gh,f) = \psi(g,hf)\psi(h,f), \ \forall \ g,h,f \in G.$$

 ψ is normalized if $\psi(g, 1) = \psi(1, h) = 1$, for all $g, h \in G$, and we say M is row/column balanced if each element of $\langle \zeta_k \rangle$ appears equally often in every non-initial row/column of M.

$$\psi(g,h)\psi(gh,f) = \psi(g,hf)\psi(h,f), \ \forall \ g,h,f \in G.$$

 ψ is normalized if $\psi(g, 1) = \psi(1, h) = 1$, for all $g, h \in G$, and we say M is row/column balanced if each element of $\langle \zeta_k \rangle$ appears equally often in every non-initial row/column of M.

In this case, ψ is orthogonal.

$$\psi(g,h)\psi(gh,f) = \psi(g,hf)\psi(h,f), \ \forall \ g,h,f \in G.$$

 ψ is normalized if $\psi(g, 1) = \psi(1, h) = 1$, for all $g, h \in G$, and we say M is row/column balanced if each element of $\langle \zeta_k \rangle$ appears equally often in every non-initial row/column of M.

In this case, ψ is *orthogonal*. The set of all cocycles form a group $Z(G, \langle \zeta_k \rangle) \cong Z(G, C_k)$.

• Develop theory of non-existence, i.e., determine the pairs (n, p) such that there are there no cocyclic BH(n, p)s.

きょうきょう

э

- Develop theory of non-existence, i.e., determine the pairs (n, p) such that there are there no cocyclic BH(n, p)s.
- Complete a thorough search for cocyclic BH(n, p) for any pair (n, p) such that $np \leq 100$, not ruled out by the above.

- Develop theory of non-existence, i.e., determine the pairs (n, p) such that there are there no cocyclic BH(n, p)s.
- Complete a thorough search for cocyclic BH(n, p) for any pair (n, p) such that $np \leq 100$, not ruled out by the above.
 - Search for orthogonal cocycles in Z(G, C_p) for all groups G of order n,

- Develop theory of non-existence, i.e., determine the pairs (n, p) such that there are there no cocyclic BH(n, p)s.
- Complete a thorough search for cocyclic BH(n, p) for any pair (n, p) such that $np \le 100$, not ruled out by the above.
 - Search for orthogonal cocycles in $Z(G, C_p)$ for all groups G of order n,
 - Search for (n, p, n, n/p)-central relative difference sets in a central extension E of C_p by a group G of order n.

- Develop theory of non-existence, i.e., determine the pairs (n, p) such that there are there no cocyclic BH(n, p)s.
- Complete a thorough search for cocyclic BH(n, p) for any pair (n, p) such that $np \le 100$, not ruled out by the above.
 - Search for orthogonal cocycles in $Z(G, C_p)$ for all groups G of order n,
 - Search for (n, p, n, n/p)-central relative difference sets in a central extension E of C_p by a group G of order n.
- Organize into equivalence classes.

A BH(n, k) matrix M is group developed over a group G if $M \sim [\phi(gh)]_{g,h\in G}$ for some $\phi: G \to \langle \zeta_k \rangle$.

A BH(n, k) matrix M is group developed over a group G if $M \sim [\phi(gh)]_{g,h\in G}$ for some $\phi : G \to \langle \zeta_k \rangle$.

Lemma

Set $r_j = \operatorname{Re}(\zeta_k^j)$ and $s_j = \operatorname{Im}(\zeta_k^j)$. A group-developed $\operatorname{BH}(n, k)$ exists only if there are non-negative integers $x_0, \ldots, x_{k-1} \in \{0, \ldots, n\}$ satisfying

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

and such that $\sum_{j=0}^{k-1} x_j = n$.

Non-existence of cocyclic BH(n, p)s

Let *p* be an odd prime.

э

Non-existence of cocyclic BH(n, p)s

Let p be an odd prime.

Lemma

A group-developed BH(n, p) exists only if there are non-negative integers $x_0, \ldots, x_{p-1} \in \{0, \ldots, n\}$ satisfying

•
$$\sum_{i=0}^{p-1} x_i^2 - x_i = \frac{n}{p}(n-1).$$

• • = • • = •

э

Let *p* be an odd prime.

Lemma

A group-developed BH(n, p) exists only if there are non-negative integers $x_0, \ldots, x_{p-1} \in \{0, \ldots, n\}$ satisfying

•
$$\sum_{i=0}^{p-1} x_i^2 - x_i = \frac{n}{p}(n-1).$$

•
$$\sum_{i=0}^{p-1} x_i x_{i+j} = \frac{n}{p}(n-1)$$
, for all $1 \le j \le p-1$

where subscripts are read modulo p.

Let *p* be an odd prime.

Lemma

A group-developed BH(n, p) exists only if there are non-negative integers $x_0, \ldots, x_{p-1} \in \{0, \ldots, n\}$ satisfying

•
$$\sum_{i=0}^{p-1} x_i^2 - x_i = \frac{n}{p}(n-1).$$

•
$$\sum_{i=0}^{p-1} x_i x_{i+j} = \frac{n}{p}(n-1)$$
, for all $1 \le j \le p-1$

where subscripts are read modulo p.

Theorem

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

No cocyclic BH(n, p)s exist for any $(n, p) \in \{(6, 3), (15, 3), (24, 3), (30, 3), (33, 3), (10, 5), (15, 5)\}.$

э

No cocyclic BH(n, p)s exist for any $(n, p) \in \{(6, 3), (15, 3), (24, 3), (30, 3), (33, 3), (10, 5), (15, 5)\}.$

For all odd primes $p \leq 17$, there is a unique BH(p, p) up to equivalence. This is the Fourier matrix of order p, which is group developed.

No cocyclic BH(n, p)s exist for any $(n, p) \in \{(6, 3), (15, 3), (24, 3), (30, 3), (33, 3), (10, 5), (15, 5)\}.$

For all odd primes $p \leq 17$, there is a unique BH(p, p) up to equivalence. This is the Fourier matrix of order p, which is group developed.

It remains to check for BH(n, p)s for all $(n, p) \in \{(9, 3), (12, 3), (18, 3), (21, 3), (27, 3), (20, 5), (14, 7)\}.$

The shift action, and orthogonal cocycles in $Z(G, \mathbb{C}_p)$

 $|Z(G, \mathcal{C}_p)| pprox p^{|G|-1}$, so a naive search is out of the question.

ヨト イヨト

The shift action, and orthogonal cocycles in $Z(G, \mathbb{C}_p)$

 $|Z(G, C_p)| \approx p^{|G|-1}$, so a naive search is out of the question. We define the *shift action* of G on $Z(G, C_p)$ by $\psi \cdot a = \psi \partial \psi_a$,

The shift action, and orthogonal cocycles in $Z(G, \mathbb{C}_p)$

 $|Z(G, C_p)| \approx p^{|G|-1}$, so a naive search is out of the question. We define the *shift action* of G on $Z(G, C_p)$ by $\psi \cdot a = \psi \partial \psi_a$, where

 $\psi_{\mathsf{a}}(g) = \psi(\mathsf{a},g) \text{ and } \partial \psi_{\mathsf{a}}(g,h) = \psi_{\mathsf{a}}(g)^{-1}\psi_{\mathsf{a}}(h)^{-1}\psi_{\mathsf{a}}(gh).$

 $|Z(G,\mathrm{C}_p)|pprox p^{|G|-1}$, so a naive search is out of the question.

We define the *shift action* of G on $Z(G, C_p)$ by $\psi \cdot a = \psi \partial \psi_a$, where $\psi_a(g) = \psi(a, g)$ and $\partial \psi_a(g, h) = \psi_a(g)^{-1} \psi_a(h)^{-1} \psi_a(gh)$.

The shift action preserves orthogonality, i.e., elements in an orbit under the shift action are either all orthogonal, or none are. $|Z(G,\mathrm{C}_p)|pprox p^{|G|-1}$, so a naive search is out of the question.

We define the *shift action* of G on $Z(G, C_p)$ by $\psi \cdot a = \psi \partial \psi_a$, where $\psi_a(g) = \psi(a, g)$ and $\partial \psi_a(g, h) = \psi_a(g)^{-1} \psi_a(h)^{-1} \psi_a(gh)$.

The shift action preserves orthogonality, i.e., elements in an orbit under the shift action are either all orthogonal, or none are.

Let Γ be the permutation representation $G \to \text{Sym}(Z(G, \mathbb{C}_p))$ associated to the shift action.

 $|Z(G,\mathrm{C}_p)|pprox p^{|G|-1}$, so a naive search is out of the question.

We define the *shift action* of G on $Z(G, C_p)$ by $\psi \cdot a = \psi \partial \psi_a$, where $\psi_a(g) = \psi(a, g)$ and $\partial \psi_a(g, h) = \psi_a(g)^{-1} \psi_a(h)^{-1} \psi_a(gh)$.

The shift action preserves orthogonality, i.e., elements in an orbit under the shift action are either all orthogonal, or none are.

Let Γ be the permutation representation $G \to \text{Sym}(Z(G, C_p))$ associated to the shift action.

Theorem

Suppose that $|G| = n \ge 5$. Then Γ is a faithful representation of G in GL(n + r - 1, p) where r is the rank of the Sylow p-subgroup of $Hom(H_2(G), C_p)$.

4 冊 ト 4 三 ト 4 三 ト

The matrix group setting enables fast calculation of orbits under the shift action. While the search space is still quite large ($\approx p^{n-1}/n$), it is feasible to calculate the orbits and test representatives for orthogonality for reasonably small p and n.

The matrix group setting enables fast calculation of orbits under the shift action. While the search space is still quite large ($\approx p^{n-1}/n$), it is feasible to calculate the orbits and test representatives for orthogonality for reasonably small p and n.

The table below gives the number t of orthogonal cocycles found for the given group isotypes, when p = 3. Note than none were found for groups of order 18.

G	C ₉	C_3^2	C ₁₂	$\mathrm{C}_3\rtimes\mathrm{C}_4$	Alt(4)	D_6	$\mathrm{C}_2^2 imes \mathrm{C}_3$
t	18	144	0	288	48	0	96

A relative (v, w, k, λ) -difference set in a finite group E of order vw relative to a normal subgroup N of order w, is a k-subset R of E such that the multiset of quotients $r_i r_j^{-1}$, $(r_i, r_j \in R, i \neq j)$, contains each element of $E \setminus N$ exactly λ times, and no element of the forbidden subgroup N. If $N \leq Z(E)$, then R is central.

A relative (v, w, k, λ) -difference set in a finite group E of order vwrelative to a normal subgroup N of order w, is a k-subset R of E such that the multiset of quotients $r_i r_j^{-1}$, $(r_i, r_j \in R, i \neq j)$, contains each element of $E \setminus N$ exactly λ times, and no element of the forbidden subgroup N. If $N \leq Z(E)$, then R is central.

Let *E* be a central extension of C_p by *G*.

A relative (v, w, k, λ) -difference set in a finite group E of order vwrelative to a normal subgroup N of order w, is a k-subset R of E such that the multiset of quotients $r_i r_j^{-1}$, $(r_i, r_j \in R, i \neq j)$, contains each element of $E \setminus N$ exactly λ times, and no element of the forbidden subgroup N. If $N \leq Z(E)$, then R is central.

Let *E* be a central extension of C_p by *G*.

Theorem

There exists a cocyclic BH(n, p) if and only if there is a relative (n, p, n, n/p)-difference set in E with central forbidden subgroup C_p .

The table below summarizes existence of matrices in our classification.

$p \setminus \frac{n}{p}$	1	2	3	4	5	6	7	8	9	10	11
3	F	N	E	E	Ν	S2	S1	N	E	Ν	Ν
5	F	N	N	S1							
7	F	S1									

N: no cocyclic Butson Hadamard matrices by non-existence theores.

E: cocyclic Butson Hadamard matrices exist.

S1: no cocyclic Butson Hadamard matrices according to an relative difference set search.

S2: no cocyclic Butson Hadamard matrices according to an orthogonal cocycle search.

F: the Fourier matrix is the only Butson Hadamard matrix.

There are only 3 interesting cases remaining, all with entries in $\langle \zeta_3 \rangle$.

э

There are only 3 interesting cases remaining, all with entries in $\langle \zeta_3 \rangle$.

• BH(9,3) : 3 unique equivalence classes.

There are only 3 interesting cases remaining, all with entries in $\langle \zeta_3 \rangle$.

- BH(9,3) : 3 unique equivalence classes.
- BH(12,3) : 2 unique equivalence classes.

There are only 3 interesting cases remaining, all with entries in $\langle \zeta_3 \rangle$.

- BH(9,3) : 3 unique equivalence classes.
- BH(12,3) : 2 unique equivalence classes.
- BH(27,3) : 16 unique equivalence classes.

There are only 3 interesting cases remaining, all with entries in $\langle \zeta_3 \rangle$.

- BH(9,3) : 3 unique equivalence classes.
- BH(12,3) : 2 unique equivalence classes.
- BH(27,3) : 16 unique equivalence classes.

The full classification is available at

http://www.maths.nuigalway.ie/~dane/BHIndex.html.

There are only 3 interesting cases remaining, all with entries in $\langle \zeta_3 \rangle$.

- BH(9,3) : 3 unique equivalence classes.
- BH(12,3) : 2 unique equivalence classes.
- BH(27,3) : 16 unique equivalence classes.

The full classification is available at

http://www.maths.nuigalway.ie/~dane/BHIndex.html.

Concluding comments

- All matrices found were equivalent to group developed matrices.
- Many of the classes found were previously unknown.
- Various composition techniques may be used to generate higher order Butson matrices from these ones.

References

- W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24, no. 3-4, 235–265,(1997).
- R. Egan, D. L. Flannery, P. Ó Catháin, Classifying cocyclic Butson Hadamard matrices, *Algebraic Design Theory and Hadamard Matrices*, Springer Proc. Math. Stat., 133, in press, 2015.
- D. L. Flannery, R. Egan, On linear shift representations, J. Pure Appl. Algebra, 219, no. 8, 3482–3494, 2015.
- P. Ó Catháin and M. Röder, The cocyclic Hadamard matrices of order less than 40, Des. Codes Cryptogr., 58, no. 1, 73–88, 2011.
- M. Röder, The GAP package RDS, http://www.gap-system.org/Packages/rds.html

A I > A I > A