Cocyclic Two Circulant Core HMs

Santiago Barrera Acevedo

Department of Mathematical and Physical Sciences
La Trobe University - Australia

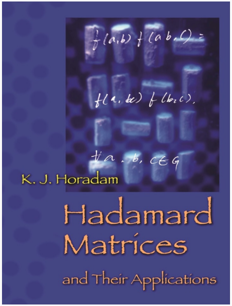
This is joint work with **Padraig Ó Catháin** and **Heiko Dietrich**
https://link.springer.com/article/10.1007/s10801-021-01033-x

Motivation

In her monography, *Hadamard matrices and their applications*, Kathy Horadam proposes the research question:

Research Problem 42 *Is the 'two circulant cores' construction (6.23) of Hadamard matrices cocyclic?*

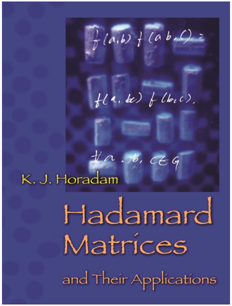
We studied this question by examining a permutation representation of the automorphism group of this combinatorial structure.



Motivation

In her monography, *Hadamard matrices and their applications*, Kathy Horadam proposes the research question:

Research Problem 42 *Is the 'two circulant cores' construction (6.23) of Hadamard matrices cocyclic?*



We studied this question by examining a permutation representation of the automorphism group of this combinatorial structure.

In the process, we classified transitive permutation groups of degree $2m+2$, with odd $m \geqslant 1$, containing an element of cycle type $1+1+m+m$.

Definitions

A $\{\pm 1\}$-matrix H of size $n \times n$ is a **Hadamard matrix** (HM) of order n, if there is a balanced number of matches and miss-matches between entries of distinct rows.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{-1} & \mathbf{-1} \\ \mathbf{1} & \mathbf{-1} & \mathbf{1} & \mathbf{-1} \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

[Two matches $(1, 1), (-1, -1)$ and two mismatches $(1, -1), (-1, 1)$].

Definitions

A $\{\pm 1\}$-matrix H of size $n \times n$ is a **Hadamard matrix** (HM) of order n, if there is a balanced number of matches and miss-matches between entries of distinct rows.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{-1} & \mathbf{-1} \\ \mathbf{1} & \mathbf{-1} & \mathbf{1} & \mathbf{-1} \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

[Two matches $(1,1), (-1,-1)$ and two mismatches $(1,-1), (-1,1)$].

Let $\mathbf{Mon}_n \leqslant \mathrm{GL}((n, \mathbb{C})$ be the group of $\{\pm 1\}$-monomial matrices of size $n \times n$.

The group $\mathbf{Mon}_n^2 = \mathbf{Mon}_n \times \mathbf{Mon}_n$ acts on the set of HMs of order n via

$$(R, S) \cdot H = RHS^{\intercal},$$

where H is a HM and $(R, S) \in \mathbf{Mon}_n^2$.

Definitions

The **automorphism group** of H is the stabiliser

$$\mathbf{Aut}(H) = \mathrm{Stab}_{\mathbf{Mon}_n^2}(H) = \{(R, S) \in \mathbf{Mon}_n^2 \colon RHS^\intercal = H\}.$$

[The element $(-I_n, -I_n)$ is an automorphism of H since $-I_n H(-I_n)^\intercal = H$].

Definitions

The **automorphism group** of H is the stabiliser

$$\mathbf{Aut}(H) = \mathrm{Stab}_{\mathbf{Mon}_n^2}(H) = \{(R, S) \in \mathbf{Mon}_n^2 \colon RHS^\intercal = H\}.$$

[The element $(-I_n, -I_n)$ is an automorphism of H since $-I_n H(-I_n)^\intercal = H$].

Observe $\mathbf{Mon}_n = \mathbf{Perm}_n \ltimes \mathbf{D}_n$ where $\mathbf{Perm}_n$ and $\mathbf{D}_n$ denote the subgroup of permutation matrices and diagonal matrices of order n, respectively.

Every element $R \in \mathbf{Mon}_n$ can be uniquely written as $P_R D_R$ with $P_R \in \mathbf{Perm}_n$ and $\mathbf{D}_R \in D_n$.

Definitions

The **automorphism group** of H is the stabiliser

$$\mathbf{Aut}(H) = \mathrm{Stab}_{\mathbf{Mon}_n^2}(H) = \{(R,S) \in \mathbf{Mon}_n^2 \colon RHS^\intercal = H\}.$$

[The element $(-I_n, -I_n)$ is an automorphism of H since $-I_n H(-I_n)^\intercal = H$].

Observe $\mathbf{Mon}_n = \mathbf{Perm}_n \ltimes \mathbf{D}_n$ where $\mathbf{Perm}_n$ and $\mathbf{D}_n$ denote the subgroup of permutation matrices and diagonal matrices of order n, respectively.

Every element $R \in \mathbf{Mon}_n$ can be uniquely written as $P_R D_R$ with $P_R \in \mathbf{Perm}_n$ and $\mathbf{D}_R \in D_n$.

The map

$$\begin{array}{rcccccc} \pi : & \mathbf{Aut}(H) & \to & \mathbf{Mon}_n & \to & \mathbf{Perm}_n \\ & (R,S) & \mapsto & R & \mapsto & P_R \end{array}$$

is a homomorphism (this gives us a representation of $\mathbf{Aut}(H)$).

Permutation Representation of **Aut**(H)

Denote the image of π by $\mathcal{A}(H) = \mathrm{Im}(\pi)$.

Under the identification $\mathbf{Perm}_n \equiv S_n$, the group $\mathcal{A}(H)$ is a permutation group, and thus π is a permutation representation of $\mathbf{Aut}(H)$.

The group $\mathcal{A}(H)$ acts on the rows of H via

$$P \cdot H = PH.$$

Permutation Representation of $\mathbf{Aut}(H)$

Denote the image of π by $\mathcal{A}(H) = \mathrm{Im}(\pi)$.

Under the identification $\mathbf{Perm}_n \equiv S_n$, the group $\mathcal{A}(H)$ is a permutation group, and thus π is a permutation representation of $\mathbf{Aut}(H)$.

The group $\mathcal{A}(H)$ acts on the rows of H via

$$P \cdot H = PH.$$

How much information is lost?

Since $\ker(\pi) = \langle(-I_n, -I_n)\rangle \cong C_2$ we have that $\mathrm{Aut}(H)$ is isomorphic to a central extension of C_2 by $\mathcal{A}(H)$.

Cocyclic Hadamard Matrices

A cocyclic HM is a HM with additional algebraic properties.

All we need to know today about CHMs is the following:

If a HM H is cocyclic then $\mathcal{A}(H)$ is transitive, acting on the rows of H[†].

[Given any two rows r_1, r_2 of H there exists $P \in \mathcal{A}(H)$ that maps r_1 to r_2].

† de Launey and Flannery, Algebraic Design Theory, 2010.

Cocyclic Hadamard Matrices

A cocyclic HM is a HM with additional algebraic properties.

All we need to know today about CHMs is the following:

If a HM H is cocyclic then $\mathcal{A}(H)$ is transitive, acting on the rows of H[†].

[Given any two rows r_1, r_2 of H there exists $P \in \mathcal{A}(H)$ that maps r_1 to r_2].

Given a transitive permutation group, one may ask:

Is the group primitive or imprimitive?

If it is primitive, is it n-transitive for some n?

[†] de Launey and Flannery, Algebraic Design Theory, 2010.

Two Circulant Cores Construction

A HM H of order $2m+2$ (with $m \geqslant 1$ odd) is **two circulant core** (TCC) if it has the form

$$H = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\intercal & \mathbf{1}^\intercal & A & B \\ \mathbf{1}^\intercal & -\mathbf{1}^\intercal & B^\intercal & -A^\intercal \end{bmatrix}$$

where

- $\mathbf{1} = [1 \ldots 1]$ denotes the all 1's row vector (whose length will be determined by the context),
- A and B are circulant $\{\pm 1\}$-matrices of order m.

[The matrix $\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$ is circulant of order 3].

A Distinguished Automorphism

Let P be the permutation matrix associated to the cycle $(1, 2, \ldots, m)$. The element (P, P) acts trivially on any circulant matrix.

[For example $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$].

A Distinguished Automorphism

Let P be the permutation matrix associated to the cycle $(1, 2, \ldots, m)$. The element (P, P) acts trivially on any circulant matrix.

[For example $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$].

Let R be the permutation matrix defined by the block matrix

$$R = \begin{bmatrix} 1 & 0 & \mathbf{0} & \mathbf{0} \\ 0 & 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0}^\intercal & \mathbf{0}^\intercal & P & \mathbf{0} \\ \mathbf{0}^\intercal & \mathbf{0}^\intercal & \mathbf{0} & P \end{bmatrix}.$$

If H is TCC HM then $(R, R) \in \mathrm{Aut}(H)$.

A Distinguished Automorphism

$$RHR^{\intercal} = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^{\intercal} & \mathbf{1}^{\intercal} & PAP^{\intercal} & PBP^{\intercal} \\ \mathbf{1}^{\intercal} & -\mathbf{1}^{\intercal} & PB^{\intercal}P^{\intercal} & -PA^{\intercal}P^{\intercal} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^{\intercal} & \mathbf{1}^{\intercal} & A & B \\ \mathbf{1}^{\intercal} & -\mathbf{1}^{\intercal} & B^{\intercal} & -A^{\intercal} \end{bmatrix}.$$

A Distinguished Automorphism

$$RHR^\intercal = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\intercal & \mathbf{1}^\intercal & PAP^\intercal & PBP^\intercal \\ \mathbf{1}^\intercal & -\mathbf{1}^\intercal & PB^\intercal P^\intercal & -PA^\intercal P^\intercal \end{bmatrix} = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\intercal & \mathbf{1}^\intercal & A & B \\ \mathbf{1}^\intercal & -\mathbf{1}^\intercal & B^\intercal & -A^\intercal \end{bmatrix}.$$

It follows that the element $\pi(R, R) = R \in \mathcal{A}(H)$ has cycle type $1 + 1 + m + m$.

[A permutation $g \in \mathcal{A}(H)$ has cycle type $m_1 + \cdots + m_k$ if the $\langle g \rangle$-orbits in the set of rows of H have sizes $m_1, \ldots, m_k$].

A Distinguished Automorphism

$$RHR^\intercal = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\intercal & \mathbf{1}^\intercal & PAP^\intercal & PBP^\intercal \\ \mathbf{1}^\intercal & -\mathbf{1}^\intercal & PB^\intercal P^\intercal & -PA^\intercal P^\intercal \end{bmatrix} = \begin{bmatrix} 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & -1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\intercal & \mathbf{1}^\intercal & A & B \\ \mathbf{1}^\intercal & -\mathbf{1}^\intercal & B^\intercal & -A^\intercal \end{bmatrix}.$$

It follows that the element $\pi(R, R) = R \in \mathcal{A}(H)$ has cycle type $1 + 1 + m + m$.

[A permutation $g \in \mathcal{A}(H)$ has cycle type $m_1 + \cdots + m_k$ if the $\langle g \rangle$-orbits in the set of rows of H have sizes $m_1, \ldots, m_k$].

Conclusion

If H is cocyclic and TCC then $\mathcal{A}(H)$ is a transitive permutation group of degree $2m + 2$, with $m \geqslant 1$ odd, and contains an element of cycle type $1 + 1 + m + m$.

We classified these groups.

Permutation Groups (Primer)

Let $G \leq \mathrm{Sym}(\Omega)$, the G-action on Ω is n-**transitive** if the induced action on n-tuples over Ω with *pairwise distinct* entries is transitive.

Permutation Groups (Primer)

Let $G \leq \mathrm{Sym}(\Omega)$, the G-action on Ω is n-**transitive** if the induced action on n-tuples over Ω with *pairwise distinct* entries is transitive.

A **block** of G (transitive) is a subset $B \subseteq \Omega$ such that for every $g \in G$ either $B = B^g$ or $B \cap B^g = \emptyset$. The *trivial blocks* are $B = \Omega$ and singletons $B = \{\omega\}$.

Permutation Groups (Primer)

Let $G \leq \mathrm{Sym}(\Omega)$, the G-action on Ω is n-**transitive** if the induced action on n-tuples over Ω with *pairwise distinct* entries is transitive.

A **block** of G (transitive) is a subset $B \subseteq \Omega$ such that for every $g \in G$ either $B = B^g$ or $B \cap B^g = \emptyset$. The *trivial blocks* are $B = \Omega$ and singletons $B = \{\omega\}$.

A transitive group is **imprimitive** if there is a nontrivial block, and **primitive** otherwise.

Permutation Groups (Primer)

Let $G \leq \mathrm{Sym}(\Omega)$, the G-action on Ω is *n*-**transitive** if the induced action on n-tuples over Ω with *pairwise distinct* entries is transitive.

A **block** of G (transitive) is a subset $B \subseteq \Omega$ such that for every $g \in G$ either $B = B^g$ or $B \cap B^g = \emptyset$. The *trivial blocks* are $B = \Omega$ and singletons $B = \{\omega\}$.

A transitive group is **imprimitive** if there is a nontrivial block, and **primitive** otherwise.

If B is a nontrivial block, then G acts transitively on $\{B^g \mid g \in G\}$ and the latter is a **system of imprimitivity** for G.

[$\langle(1,2,3,4)\rangle \leqslant S_4$ is imprimitive with system of imprimitivity $\{\{1,3\},\{2,4\}\}$].

Permutation Groups (Primer)

Let $G \leq \mathrm{Sym}(\Omega)$, the G-action on Ω is n-**transitive** if the induced action on n-tuples over Ω with *pairwise distinct* entries is transitive.

A **block** of G (transitive) is a subset $B \subseteq \Omega$ such that for every $g \in G$ either $B = B^g$ or $B \cap B^g = \emptyset$. The *trivial blocks* are $B = \Omega$ and singletons $B = \{\omega\}$.

A transitive group is **imprimitive** if there is a nontrivial block, and **primitive** otherwise.

If B is a nontrivial block, then G acts transitively on $\{B^g \mid g \in G\}$ and the latter is a **system of imprimitivity** for G.

[$\langle(1,2,3,4)\rangle \leqslant S_4$ is imprimitive with system of imprimitivity $\{\{1,3\},\{2,4\}\}$].

Given a block B, the set-wise stabiliser G_B acts on B transitively.

Permutation Groups (Primer)

Let $G \leq \mathrm{Sym}(\Omega)$, the G-action on Ω is *n*-**transitive** if the induced action on n-tuples over Ω with *pairwise distinct* entries is transitive.

A **block** of G (transitive) is a subset $B \subseteq \Omega$ such that for every $g \in G$ either $B = B^g$ or $B \cap B^g = \emptyset$. The *trivial blocks* are $B = \Omega$ and singletons $B = \{\omega\}$.

A transitive group is **imprimitive** if there is a nontrivial block, and **primitive** otherwise.

If B is a nontrivial block, then G acts transitively on $\{B^g \mid g \in G\}$ and the latter is a **system of imprimitivity** for G.

[$\langle(1,2,3,4)\rangle \leqslant S_4$ is imprimitive with system of imprimitivity $\{\{1,3\},\{2,4\}\}$].

Given a block B, the set-wise stabiliser G_B acts on B transitively.

Thus, G can be identified with a subgroup of $G_B^B \wr G^{\mathcal{P}}$.

Main Ingredient of our Classification

Theorem 1 (Jones 2011, Theorem 1.2 and Remark 1.5)

If T is a transitive permutation group of degree $k > 2$, and contains a cycle fixing exactly one point, then it is 2-transitive and satisfies (up to isomorphism) one of the following:

Main Ingredient of our Classification

Theorem 1 (Jones 2011, Theorem 1.2 and Remark 1.5)

If T is a transitive permutation group of degree $k > 2$, and contains a cycle fixing exactly one point, then it is 2-transitive and satisfies (up to isomorphism) one of the following:

a) $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ with $k = q^d$ for some prime power q,

$[\mathrm{AGL}_d(q) = \mathbb{F}_q \rtimes \mathrm{GL}_d(q), \mathrm{A\Gamma L}_d(q) = \mathbb{F}_q \rtimes (\mathrm{GL}_d(q) \rtimes \mathrm{Aut}(\mathbb{F}_q))]$.

Main Ingredient of our Classification

Theorem 1 (Jones 2011, Theorem 1.2 and Remark 1.5)

If T is a transitive permutation group of degree $k > 2$, and contains a cycle fixing exactly one point, then it is 2-transitive and satisfies (up to isomorphism) one of the following:

a) $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ with $k = q^d$ for some prime power q,

$[\mathrm{AGL}_d(q) = \mathbb{F}_q \rtimes \mathrm{GL}_d(q), \mathrm{A\Gamma L}_d(q) = \mathbb{F}_q \rtimes (\mathrm{GL}_d(q) \rtimes \mathrm{Aut}(\mathbb{F}_q))]$.

b) $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p)\}$ with $k = p + 1$ for some prime $p > 3$,

Main Ingredient of our Classification

Theorem 1 (Jones 2011, Theorem 1.2 and Remark 1.5)

If T is a transitive permutation group of degree $k > 2$, and contains a cycle fixing exactly one point, then it is 2-transitive and satisfies (up to isomorphism) one of the following:

a) $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ with $k = q^d$ for some prime power q,

$[\mathrm{AGL}_d(q) = \mathbb{F}_q \rtimes \mathrm{GL}_d(q), \mathrm{A\Gamma L}_d(q) = \mathbb{F}_q \rtimes (\mathrm{GL}_d(q) \rtimes \mathsf{Aut}(\mathbb{F}_q))]$.

b) $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p)\}$ with $k = p + 1$ for some prime $p > 3$,

c) $T \in \{M_{11}, M_{12}, M_{24}\}$ with $k = 12, 12, 24$, respectively,

Main Ingredient of our Classification

Theorem 1 (Jones 2011, Theorem 1.2 and Remark 1.5)

If T is a transitive permutation group of degree $k > 2$, and contains a cycle fixing exactly one point, then it is 2-transitive and satisfies (up to isomorphism) one of the following:

a) $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ with $k = q^d$ for some prime power q,

$[\mathrm{AGL}_d(q) = \mathbb{F}_q \rtimes \mathrm{GL}_d(q), \mathrm{A\Gamma L}_d(q) = \mathbb{F}_q \rtimes (\mathrm{GL}_d(q) \rtimes \mathsf{Aut}(\mathbb{F}_q))]$.

b) $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p)\}$ with $k = p + 1$ for some prime $p > 3$,

c) $T \in \{M_{11}, M_{12}, M_{24}\}$ with $k = 12, 12, 24$, respectively,

d) $A_k \leq T$.

Main Ingredient of our Classification

Theorem 1 (Jones 2011, Theorem 1.2 and Remark 1.5)

If T is a transitive permutation group of degree $k > 2$, and contains a cycle fixing exactly one point, then it is 2-transitive and satisfies (up to isomorphism) one of the following:

a) $\mathrm{AGL}_d(q) \leq T \leq \mathrm{A\Gamma L}_d(q)$ with $k = q^d$ for some prime power q,

$[\mathrm{AGL}_d(q) = \mathbb{F}_q \rtimes \mathrm{GL}_d(q), \mathrm{A\Gamma L}_d(q) = \mathbb{F}_q \rtimes (\mathrm{GL}_d(q) \rtimes \mathrm{Aut}(\mathbb{F}_q))]$.

b) $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p)\}$ with $k = p + 1$ for some prime $p > 3$,

c) $T \in \{M_{11}, M_{12}, M_{24}\}$ with $k = 12, 12, 24$, respectively,

d) $A_k \leq T$.

Every 2-transitive group is primitive; 2-transitive groups form a strict class of primitive groups and are classified (affine or almost-simple).

Groups under a) are affine, and groups under b-d) are almost simple.

Classification

Theorem 2 (BA-OC-D)

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree $n = 2m + 2$ with $m \geq 1$ odd. If G has an element of cycle type $1 + 1 + m + m$, then there exists a 2-transitive group T (as in the theorem of Jones) with $k = m + 1$ such that

Classification

Theorem 2 (BA-OC-D)

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree $n = 2m + 2$ with $m \geq 1$ odd. If G has an element of cycle type $1 + 1 + m + m$, then there exists a 2-transitive group T (as in the theorem of Jones) with $k = m + 1$ such that

a) G is 2-transitive (and thus primitive), or

Classification

Theorem 2 (BA-OC-D)

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree $n = 2m + 2$ with $m \geq 1$ odd. If G has an element of cycle type $1 + 1 + m + m$, then there exists a 2-transitive group T (as in the theorem of Jones) with $k = m + 1$ such that

a) G is 2-transitive (and thus primitive), or

b) G is imprimitive with $m + 1$ blocks of size 2, and the induced action of G on the system of imprimitivity is T, that is, $G \leq C_2 \wr T = C_2^k \rtimes T$, or

Classification

Theorem 2 (BA-OC-D)

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree $n = 2m + 2$ with $m \geq 1$ odd. If G has an element of cycle type $1 + 1 + m + m$, then there exists a 2-transitive group T (as in the theorem of Jones) with $k = m + 1$ such that

a) G is 2-transitive (and thus primitive), or

b) G is imprimitive with $m + 1$ blocks of size 2, and the induced action of G on the system of imprimitivity is T, that is, $G \leq C_2 \wr T = C_2^k \rtimes T$, or

c) G is imprimitive with 2 blocks of size $m+1$, and the induced action on each block is T, that is $G \leq T \wr C_2 = T^2 \rtimes C_2$.

Sketch of Classification

Let $\sigma \in G$ be the element with cycle type $1 + 1 + m + m$.

Sketch of Classification

Let $\sigma \in G$ be the element with cycle type $1 + 1 + m + m$.

Let $\alpha \in \Omega$ be a fixed point of σ and note that $\langle \sigma \rangle \leq G_\alpha$ has four orbits of size $1, 1, m, m$.

Sketch of Classification

Let $\sigma \in G$ be the element with cycle type $1 + 1 + m + m$.

Let $\alpha \in \Omega$ be a fixed point of σ and note that $\langle \sigma \rangle \leq G_\alpha$ has four orbits of size $1, 1, m, m$.

[The rank of G is the number of orbits of the point stabiliser G_α; the subdegrees of G are the sizes of the orbits of the point stabiliser G_α].

Sketch of Classification

Let $\sigma \in G$ be the element with cycle type $1 + 1 + m + m$.

Let $\alpha \in \Omega$ be a fixed point of σ and note that $\langle \sigma \rangle \leq G_\alpha$ has four orbits of size $1, 1, m, m$.

[The rank of G is the number of orbits of the point stabiliser G_α; the subdegrees of G are the sizes of the orbits of the point stabiliser G_α].

Thus, G has rank $r \in \{2, 3, 4\}$, and we make a case distinction.

Sketch of Classification

Let $\sigma \in G$ be the element with cycle type $1 + 1 + m + m$.

Let $\alpha \in \Omega$ be a fixed point of σ and note that $\langle \sigma \rangle \leq G_\alpha$ has four orbits of size $1, 1, m, m$.

[The rank of G is the number of orbits of the point stabiliser G_α; the subdegrees of G are the sizes of the orbits of the point stabiliser G_α].

Thus, G has rank $r \in \{2, 3, 4\}$, and we make a case distinction.

Suppose G has rank 2 with subdegrees $1, 2m + 1$:

G_α-orbits on Ω : $\Omega_1 = \{\alpha\}$ and $\Omega_2 = \{\beta_2, \ldots, \beta_{2m+2}\}$.

Sketch of Classification

Let $\sigma \in G$ be the element with cycle type $1+1+m+m$.

Let $\alpha \in \Omega$ be a fixed point of σ and note that $\langle \sigma \rangle \leq G_\alpha$ has four orbits of size $1, 1, m, m$.

[The rank of G is the number of orbits of the point stabiliser G_α; the subdegrees of G are the sizes of the orbits of the point stabiliser G_α].

Thus, G has rank $r \in \{2, 3, 4\}$, and we make a case distinction.

Suppose G has rank 2 with subdegrees $1, 2m+1$:

G_α-orbits on Ω : $\Omega_1 = \{\alpha\}$ and $\Omega_2 = \{\beta_2, \ldots, \beta_{2m+2}\}$.

G_α acts transitively on Ω_2; this is equivalent to G being 2-transitive on Ω.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, 1, 2m$, or 4 with subdegrees $1, 1, m, m$:

G_α-orbits on Ω :

$$\Omega_1 = \{\alpha\}, \quad \Omega_2 = \{\beta\} \quad \text{and} \quad \Omega_3 = \{\beta_3, \ldots, \beta_{2m+2}\}, \text{ or}$$

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta\},\ \Omega_3 = \{\beta_3, \ldots, \beta_{m+2}\} \ \text{ and } \ \Omega_4 = \{\beta_{m+3}, \ldots, \beta_{2m+2}\}.$$

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, 1, 2m$, or 4 with subdegrees $1, 1, m, m$:

G_α-orbits on Ω :

$$\Omega_1 = \{\alpha\}, \quad \Omega_2 = \{\beta\} \quad \text{and} \quad \Omega_3 = \{\beta_3, \ldots, \beta_{2m+2}\}, \text{ or}$$

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta\},\ \Omega_3 = \{\beta_3, \ldots, \beta_{m+2}\} \ \text{ and } \ \Omega_4 = \{\beta_{m+3}, \ldots, \beta_{2m+2}\}.$$

G_α has exactly two fixed points, namely α, β, which form a block of G.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, 1, 2m$, or 4 with subdegrees $1, 1, m, m$:

G_α-orbits on Ω :

$$\Omega_1 = \{\alpha\}, \quad \Omega_2 = \{\beta\} \quad \text{and} \quad \Omega_3 = \{\beta_3, \ldots, \beta_{2m+2}\}, \text{ or}$$

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta\},\ \Omega_3 = \{\beta_3, \ldots, \beta_{m+2}\}\ \text{ and }\ \Omega_4 = \{\beta_{m+3}, \ldots, \beta_{2m+2}\}.$$

G_α has exactly two fixed points, namely α, β, which form a block of G.

The element σ fixes the block $\{\alpha, \beta\}$ and acts not only transitively but as a cycle on the remaining m blocks.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, 1, 2m$, or 4 with subdegrees $1, 1, m, m$:

G_α-orbits on Ω :

$$\Omega_1 = \{\alpha\}, \quad \Omega_2 = \{\beta\} \quad \text{and} \quad \Omega_3 = \{\beta_3, \ldots, \beta_{2m+2}\}, \text{ or}$$

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta\},\ \Omega_3 = \{\beta_3, \ldots, \beta_{m+2}\} \ \text{ and } \ \Omega_4 = \{\beta_{m+3}, \ldots, \beta_{2m+2}\}.$$

G_α has exactly two fixed points, namely α, β, which form a block of G.

The element σ fixes the block $\{\alpha, \beta\}$ and acts not only transitively but as a cycle on the remaining m blocks.

The induced action of G on the system of imprimitivity $\{\{\alpha, \beta\}^g \mid g \in G\}$ is 2-transitive and one of the theorem of Jones. This gives the groups $G \leqslant C_2 \wr T$.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, m, m+1$:

$G_\alpha -$ orbits on Ω :

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta_2, \ldots, \beta_{m+1}\} \text{ and } \Omega_3 = \{\beta_{m+2}, \ldots, \beta_{2m+2}\}.$$

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, m, m+1$:

G_α – orbits on Ω :

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta_2, \ldots, \beta_{m+1}\} \text{ and } \Omega_3 = \{\beta_{m+2}, \ldots, \beta_{2m+2}\}.$$

G is not primitive as violates a condition on the subdegrees for primitive groups, ($\gcd(m, m+1) \neq 1$).

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, m, m+1$:

$G_\alpha -$ orbits on Ω :

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta_2, \ldots, \beta_{m+1}\} \text{ and } \Omega_3 = \{\beta_{m+2}, \ldots, \beta_{2m+2}\}.$$

G is not primitive as violates a condition on the subdegrees for primitive groups, $(\gcd(m, m+1) \neq 1)$.

Let B a block containing α and $g \in G_\alpha$. Then $B^g = B$ implies Ω_2 or Ω_3 is contained in B. But only $\Omega_2 \subset B$ is possible. Thus $|B| = m+1$.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, m, m+1$:

G_α – orbits on Ω :

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta_2, \ldots, \beta_{m+1}\} \text{ and } \Omega_3 = \{\beta_{m+2}, \ldots, \beta_{2m+2}\}.$$

G is not primitive as violates a condition on the subdegrees for primitive groups, ($\gcd(m, m+1) \neq 1$).

Let B a block containing α and $g \in G_\alpha$. Then $B^g = B$ implies Ω_2 or Ω_3 is contained in B. But only $\Omega_2 \subset B$ is possible. Thus $|B| = m+1$.

G is imprimitive with 2 blocks of size $m+1$.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, m, m+1$:

$G_\alpha -$ orbits on Ω :

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta_2, \ldots, \beta_{m+1}\} \text{ and } \ \Omega_3 = \{\beta_{m+2}, \ldots, \beta_{2m+2}\}.$$

G is not primitive as violates a condition on the subdegrees for primitive groups, $(\gcd(m, m+1) \neq 1)$.

Let B a block containing α and $g \in G_\alpha$. Then $B^g = B$ implies Ω_2 or Ω_3 is contained in B. But only $\Omega_2 \subset B$ is possible. Thus $|B| = m+1$.

G is imprimitive with 2 blocks of size $m+1$.

σ stabilises B and acts on the elements of B as a cycle that fixes exactly one point.

Sketch of Classification

Suppose that the rank of G is 3 with subdegrees $1, m, m+1$:

G_α – orbits on Ω :

$$\Omega_1 = \{\alpha\},\ \Omega_2 = \{\beta_2, \ldots, \beta_{m+1}\} \text{ and } \ \Omega_3 = \{\beta_{m+2}, \ldots, \beta_{2m+2}\}.$$

G is not primitive as violates a condition on the subdegrees for primitive groups, $(\gcd(m, m+1) \neq 1)$.

Let B a block containing α and $g \in G_\alpha$. Then $B^g = B$ implies Ω_2 or Ω_3 is contained in B. But only $\Omega_2 \subset B$ is possible. Thus $|B| = m+1$.

G is imprimitive with 2 blocks of size $m+1$.

σ stabilises B and acts on the elements of B as a cycle that fixes exactly one point. The induced action on blocks is 2-transitive and thus one of the theorem of Jones. This gives the groups $G \leqslant T \wr C_2$.

Classification – $\mathcal{A}(H)$ for cocyclic TCC HMs

Results of Ito[†], and Moorehouse[‡] in combination with Theorem 2 yield:

[†] Hadamard matrices with "doubly transitive" automorphism groups.

[‡] The 2–transitive complex Hadamard matrices.

Classification – $\mathcal{A}(H)$ for cocyclic TCC HMs

Results of Ito†, and Moorehouse‡ in combination with Theorem 2 yield:

Theorem 3 (BA-OC-D)

Let H be a cocyclic TCC HM of order $n = 2m + 2$ with m odd. Then one of the following holds, where p denotes a prime and q denotes a prime-power:

† Hadamard matrices with "doubly transitive" automorphism groups.

‡ The 2–transitive complex Hadamard matrices.

Classification – $\mathcal{A}(H)$ for cocyclic TCC HMs

Results of Ito[†], and Moorehouse[‡] in combination with Theorem 2 yield:

Theorem 3 (BA-OC-D)

Let H be a cocyclic TCC HM of order $n = 2m + 2$ with m odd. Then one of the following holds, where p denotes a prime and q denotes a prime-power:

a) $\mathcal{A}(H)$ is affine 2-transitive and contains $\mathrm{AGL}_n(2)$ as subgroup, or

[†] Hadamard matrices with "doubly transitive" automorphism groups.

[‡] The 2–transitive complex Hadamard matrices.

Classification – $\mathcal{A}(H)$ for cocyclic TCC HMs

Results of Ito[†], and Moorehouse[‡] in combination with Theorem 2 yield:

Theorem 3 (BA-OC-D)

Let H be a cocyclic TCC HM of order $n = 2m + 2$ with m odd. Then one of the following holds, where p denotes a prime and q denotes a prime-power:

a) $\mathcal{A}(H)$ is affine 2-transitive and contains $\mathrm{AGL}_n(2)$ as subgroup, or

b) $\mathcal{A}(H)$ is almost-simple 2-transitive, and contains M_{12} or $\mathrm{PSL}_2(q)$ as a normal subgroup, or

[†] Hadamard matrices with "doubly transitive" automorphism groups.

[‡] The 2–transitive complex Hadamard matrices.

Classification – $\mathcal{A}(H)$ for cocyclic TCC HMs

Results of Ito[†], and Moorehouse[‡] in combination with Theorem 2 yield:

Theorem 3 (BA-OC-D)

Let H be a cocyclic TCC HM of order $n = 2m + 2$ with m odd. Then one of the following holds, where p denotes a prime and q denotes a prime-power:

a) $\mathcal{A}(H)$ is affine 2-transitive and contains $\mathrm{AGL}_n(2)$ as subgroup, or

b) $\mathcal{A}(H)$ is almost-simple 2-transitive, and contains M_{12} or $\mathrm{PSL}_2(q)$ as a normal subgroup, or

c) $\mathcal{A}(H) \leq C_2 \wr T$ and $\mathrm{AGL}_1(q) \leq T \leq \mathrm{A\Gamma L}_1(q)$.

[†] Hadamard matrices with "doubly transitive" automorphism groups.

[‡] The 2–transitive complex Hadamard matrices.

Classification – $\mathcal{A}(H)$ for cocyclic TCC HMs

Results of Ito†, and Moorehouse‡ in combination with Theorem 2 yield:

Theorem 3 (BA-OC-D)

Let H be a cocyclic TCC HM of order $n = 2m + 2$ with m odd. Then one of the following holds, where p denotes a prime and q denotes a prime-power:

a) $\mathcal{A}(H)$ is affine 2-transitive and contains $\mathrm{AGL}_n(2)$ as subgroup, or

b) $\mathcal{A}(H)$ is almost-simple 2-transitive, and contains M_{12} or $\mathrm{PSL}_2(q)$ as a normal subgroup, or

c) $\mathcal{A}(H) \leq C_2 \wr T$ and $\mathrm{AGL}_1(q) \leq T \leq \mathrm{A\Gamma L}_1(q)$.

d) $\mathcal{A}(H) \leq C_2 \wr T$ where $T \in \{\mathrm{PSL}_2(p), \mathrm{PGL}_2(p)\}$ with $m = p$ a prime, or $T \in \{M_{11}, M_{12}, M_{24}\}$ with $m + 1 = 12, 12, 24$, respectively, or,

---

†Hadamard matrices with "doubly transitive" automorphism groups.

‡The 2–transitive complex Hadamard matrices.

Order of cocyclic TCC HMs

The order of a cocyclic TCC HM has the form

(A) $q + 1$, where $q \equiv 3 \bmod 4$ is a prime power, or

(B) $2p + 2$, where $p \geq 3$ is a prime, or

(C) 2^t, where $t \geq 2$ is an integer.

Order of cocyclic TCC HMs

The order of a cocyclic TCC HM has the form

(A) $q + 1$, where $q \equiv 3 \bmod 4$ is a prime power, or

(B) $2p + 2$, where $p \geq 3$ is a prime, or

(C) 2^t, where $t \geq 2$ is an integer.

Existence of cocyclic TCC HMs

There exist cocyclic TCC HMs

(i) for all orders as in (A): Paley I,

(ii) for all orders as in (B) for which $p \equiv 1 \bmod 4$: Paley II,

(iii) for all orders as in (B) for which $p < 1000$: Generalised Legendre pairs,

(iv) for all orders as in (C) with $t \leq 8$: since $2^t - 1$ is a prime for $t = 3, 5, 7$, the first power of two not covered by (i) or (ii) is 512.

Order of cocyclic TCC HMs

The order of a cocyclic TCC HM has the form

(A) $q+1$, where $q \equiv 3 \bmod 4$ is a prime power, or

(B) $2p+2$, where $p \geq 3$ is a prime, or

(C) 2^t, where $t \geq 2$ is an integer.

Existence of cocyclic TCC HMs

There exist cocyclic TCC HMs

(i) for all orders as in (A): Paley I,

(ii) for all orders as in (B) for which $p \equiv 1 \bmod 4$: Paley II,

(iii) for all orders as in (B) for which $p < 1000$: Generalised Legendre pairs,

(iv) for all orders as in (C) with $t \leq 8$: since $2^t - 1$ is a prime for $t = 3, 5, 7$, the first power of two not covered by (i) or (ii) is 512.

The TCC HMs Stanton-Sprott cyclic difference sets are not cocyclic.

Questions

- What are the automorphism groups of the aforementioned families of cocyclic TCC HMs?

  This requires solving the extension problem

  $$1 \to C_2 \to \mathrm{Aut}(H) \to \mathcal{A}(H) \to 1$$

  and constructing certain monomial action based on a permutation action.

- A Kimura HM is a HM of order $n = 4 + 4m$ of the form

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 1 & 1 & -1 & -1 & \mathbf{1} & \mathbf{1} & -\mathbf{1} & -\mathbf{1} \\ 1 & -1 & 1 & -1 & \mathbf{1} & -\mathbf{1} & \mathbf{1} & -\mathbf{1} \\ 1 & -1 & -1 & 1 & -\mathbf{1} & \mathbf{1} & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\top & \mathbf{1}^\top & \mathbf{1}^\top & -\mathbf{1}^\top & A & B & C & D \\ \mathbf{1}^\top & \mathbf{1}^\top & -\mathbf{1}^\top & \mathbf{1}^\top & -B & A & D & -C \\ \mathbf{1}^\top & -\mathbf{1}^\top & \mathbf{1}^\top & \mathbf{1}^\top & -C & -D & A & B \\ \mathbf{1}^\top & -\mathbf{1}^\top & -\mathbf{1}^\top & -\mathbf{1}^\top & D & -C & B & -A \end{bmatrix}$$

where A, B, C, D are certain $\{\pm 1\}$-matrices of order m, and $\mathbf{1}$ denotes the all 1's row vector (whose length is determined by the context).

Research Problem 41 *Is the Kimura construction (6.22) of Hadamard matrices cocyclic?*

Thank you