Automorphisms of pairwise combinatorial designs

Padraig Ó Catháin
National University of Ireland, Galway

17 October 2011
Outline

1. Introduction: Designs and Hadamard matrices
2. Outline of thesis
3. Doubly transitive group actions on Hadamard matrices
Incidence Structures

Definition

An *incidence structure* $\Delta$ is a pair $(V, B)$ where $V$ is a finite set and $B \subseteq \mathcal{P}(V)$.

Definition

An *automorphism* of $\Delta$ is a permutation $\sigma \in \text{Sym}(V)$ which preserves $B$ setwise.

Definition

Define a function $\phi : V \times B \to \{0, 1\}$ given by $\phi(v, b) = 1$ if and only if $v \in b$. An *incidence matrix* for $\Delta$ is a matrix

$$M = [\phi(v, b)]_{v \in V, b \in B}.$$
**Designs**

**Definition**
Let \((V, B)\) be an incidence structure in which \(|V| = v\) and \(|b| = k\) for all \(b \in B\). Then \(\Delta = (V, B)\) is a \(t-(v, k, \lambda)\) **design** if and only if any \(t\)-subset of \(V\) occurs in exactly \(\lambda\) blocks.

**Definition**
The design \(\Delta\) is **symmetric** if \(|V| = |B|\).
Example

A symmetric 2-(7, 3, 1) design, $\Delta$ (the Fano plane). The point set is $V = \{1, \ldots, 7\}$, and the blocks are

$$\{1, 2, 3\} \quad \{1, 4, 5\} \quad \{1, 6, 7\} \quad \{2, 4, 6\} \quad \{2, 5, 7\} \quad \{3, 4, 7\} \quad \{3, 5, 6\}$$

A sample automorphism of $\mathcal{D}$ is $(2, 4, 6)(3, 5, 7)$. In fact, $\text{Aut}(\mathcal{D}) \cong \text{PGL}_3(2)$. 
Lemma

The $v \times v$ $(0, 1)$-matrix $M$ is the incidence matrix of a 2-$(v, k, \lambda)$ symmetric design if and only if

$$MM^\top = (k - \lambda)I + \lambda J$$

Proof.

The entry in position $(i, j)$ of $MM^\top$ counts the number of blocks containing both $v_i$ and $v_j$. 

\[\square\]
Let $G$ be a group of order $v$, and $\mathcal{D}$ a $k$-subset of $G$.
Suppose that every non-identity element of $G$ has $\lambda$ representations of the form $d_i d_j^{-1}$ where $d_i, d_j \in \mathcal{D}$.
Then $\mathcal{D}$ is a $(v, k, \lambda)$-difference set in $G$.

Example: take $G = (\mathbb{Z}_7, +)$ and $\mathcal{D} = \{1, 2, 4\}$.
Example: the Jordan ‘miracle’.
Definition

We say that $G < \text{Sym}(V)$ is regular (on $V$) if for any $v_i, v_j \in V$ there exists a unique $g \in G$ such that $v_i^g = v_j$.

Theorem

If $G$ contains a $(v, k, \lambda)$-difference set then there exists a symmetric 2-$(v, k, \lambda)$ design on which $G$ acts regularly. Conversely, a 2-$(v, k, \lambda)$ design on which $G$ acts regularly corresponds to a $(v, k, \lambda)$-difference set in $G$. 
Hadamard matrices

**Definition**

Let $H$ be a matrix of order $n$, with all entries in $\{1, -1\}$. Then $H$ is a **Hadamard matrix** if and only if $HH^\top = nl_n$.

\[
\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}
\]
Sylvester constructed Hadamard matrices of order $2^n$.

Hadamard showed that the determinant of a Hadamard matrix $H = [h_{i,j}]$ of order $n$ is maximal among all matrices of order $n$ over $\mathbb{C}$ whose entries satisfy $\|h_{i,j}\| \leq 1$ for all $1 \leq i, j \leq n$.

Hadamard also showed that the order of a Hadamard matrix is necessarily 1, 2 or $4t$ for some $t \in \mathbb{N}$. He also constructed Hadamard matrices of orders 12 and 20.

Paley constructed Hadamard matrices of order $n = p^t + 1$ for primes $p$, and conjectured that a Hadamard matrix of order $n$ exists whenever $4 \mid n$.

This is the Hadamard conjecture, and has been verified for all $n \leq 667$. Asymptotic results.
Automorphisms of Hadamard matrices

- A pair of \( \{\pm 1\} \) monomial matrices \((P, Q)\) is an **automorphism** of \( H \) if \( PHQ^\top = H \).
- Aut\((H)\) has an induced permutation action on the set \( \{r\} \cup \{-r\} \).
- Quotient by diagonal matrices is a permutation group with an induced action on the set of pairs \( \{r, -r\} \), which we identify with the rows of \( H \), denoted \( A_H \).
Hadamard matrices and 2-designs

Lemma

There exists a Hadamard matrix $H$ of order $4n$ if and only there exists a $2-(4n - 1, 2n - 1, n - 1)$ design $\mathcal{D}$. Furthermore $\text{Aut}(\mathcal{D}) < A_H$.

Proof.

Let $M$ be an incidence matrix for $\mathcal{D}$. Then $M$ satisfies $MM^\top = nl + (n - 1)J$. So $(2M - J)(2M - J)^\top = 4nl - J$. Adding a row and column of 1s gives a Hadamard matrix, $H$. Every automorphism of $M$ is a permutation automorphism of $H$ fixing the first row. $\square$
Example: the Paley construction

The existence of a \((4n - 1, 2n - 1, n - 1)\)-difference set implies the existence of a Hadamard matrix \(H\) of order \(4n\). Difference sets with these parameters are called \textit{Paley-Hadamard}.

- Let \(\mathbb{F}_q\) be the finite field of size \(q\), \(q = 4n - 1\).
- The quadratic residues in \(\mathbb{F}_q\) form a difference set in \((\mathbb{F}_q, +)\) with parameters \((4n - 1, 2n - 1, n - 1)\) (Paley).
- Let \(\chi\) be the quadratic character of \(\mathbb{F}_q^*\), given by \(\chi : x \mapsto x^{\frac{q-1}{2}}\), and let \(Q = [\chi(x - y)]_{x,y \in \mathbb{F}_q}\).
- Then

\[
H = \begin{pmatrix}
1 & 1 \\
1^\top & Q - I
\end{pmatrix}
\]

is a Hadamard matrix.
Outline of Thesis

Chapters:

- Preliminary material
- Classification of cocyclic Hadamard matrices of order $\leq 40$
- Doubly transitive group actions on Hadamard matrices
- Classification of cocyclic Hadamard matrices from difference sets (non-affine case)
- Non-cocyclic Hadamard matrices from difference sets (two families)
- Skew Hadamard difference sets (a new 3-parameter infinite family)
Cocyclic development

**Definition**
Let $G$ be a group and $C$ an abelian group. We say that $\psi : G \times G \to C$ is a cocycle if

$$\psi(g, h)\psi(gh, k) = \psi(h, k)\psi(g, hk)$$

for all $g, h, k \in G$.

**Definition (de Launey & Horadam)**
Let $H$ be an $n \times n$ Hadamard matrix. Let $G$ be a group of order $n$. We say that $H$ is cocyclic if there exists a cocycle $\psi : G \times G \to \langle -1 \rangle$ such that

$$H \cong [\psi(g, h)]_{g, h \in G}.$$ 

In particular, if $H$ is cocyclic, then $A_H$ is transitive.
Classification of cocyclic Hadamard matrices

Theorem (De Launey, Flannery & Horadam)

The following statements are equivalent.

- There is a cocyclic Hadamard matrix over $G$.
- There is a normal $(4t, 2, 4t, 2t)$-relative difference set in a central extension of $N \cong C_2$ by $G$, relative to $N$.
- There is a divisible $(4t, 2, 4t, 2t)$ design, class regular with respect to $C_2 \cong \langle -1 \rangle$, and with a central extension of $\langle -1 \rangle$ by $G$ as a regular group of automorphisms.

### Table of results

<table>
<thead>
<tr>
<th>Order</th>
<th>Cocyclic</th>
<th>Indexing Groups</th>
<th>Extension Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2</td>
<td>3 / 5</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>3 / 5</td>
<td>9 / 14</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>3 / 5</td>
<td>3 / 15</td>
</tr>
<tr>
<td>16</td>
<td>5</td>
<td>13 / 14</td>
<td>45 / 51</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>2 / 5</td>
<td>3 / 14</td>
</tr>
<tr>
<td>24</td>
<td>16 / 60</td>
<td>8 / 15</td>
<td>14 / 52</td>
</tr>
<tr>
<td>28</td>
<td>6 / 487</td>
<td>2 / 4</td>
<td>2 / 13</td>
</tr>
<tr>
<td>32</td>
<td>100/ ≥ 3 × 10^6</td>
<td>49/51</td>
<td>261/267</td>
</tr>
<tr>
<td>36</td>
<td>35 / ≥ 3 × 10^6</td>
<td>12 /14</td>
<td>21 / 50</td>
</tr>
</tbody>
</table>

**Comprehensive data available at:** [www.maths.nuigalway.ie/~padraig](http://www.maths.nuigalway.ie/~padraig)
We can compare the proportion of cocyclic Hadamard matrices (of order $n$) among all $\{\pm 1\}$-cocyclic matrices to the proportion of Hadamard matrices among $\{\pm 1\}$-matrices:

<table>
<thead>
<tr>
<th>$n$</th>
<th>Hadamard matrices</th>
<th>Cocyclic Hadamard matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>4</td>
<td>$7 \times 10^{-4}$</td>
<td>0.125</td>
</tr>
<tr>
<td>8</td>
<td>$1.3 \times 10^{-13}$</td>
<td>7.8 $\times 10^{-3}$</td>
</tr>
<tr>
<td>12</td>
<td>$2.5 \times 10^{-30}$</td>
<td>1.4 $\times 10^{-4}$</td>
</tr>
<tr>
<td>16</td>
<td>$1.1 \times 10^{-53}$</td>
<td>1.7 $\times 10^{-4}$</td>
</tr>
<tr>
<td>20</td>
<td>$1.0 \times 10^{-85}$</td>
<td>1.1 $\times 10^{-6}$</td>
</tr>
<tr>
<td>24</td>
<td>$1.2 \times 10^{-124}$</td>
<td>1.8 $\times 10^{-7}$</td>
</tr>
<tr>
<td>28</td>
<td>$1.3 \times 10^{-173}$</td>
<td>1.0 $\times 10^{-8}$</td>
</tr>
</tbody>
</table>
Two constructions of Hadamard matrices: from \((4n - 1, 2n - 1, n - 1)\) difference sets, and from \((4n, 2, 4n, 2n)\)-RDSs.

Problem

- *How do these constructions interact?*
- *Can a Hadamard matrix support both structures?*
- *If so, can we classify such matrices?*
Motivation

- Horadam: Are the Hadamard matrices developed from twin prime power difference sets cocyclic? (Problem 39 of *Hadamard matrices and their applications*).
- Jungnickel: Classify the skew Hadamard difference sets. (Open Problem 13 of the survey *Difference sets*).
- Ito and Leon: There exists a Hadamard matrix of order 36 on which $Sp_6(2)$ acts. Are there others?
We show that a cocyclic Hadamard matrix which is also developed from a difference set has $A_H$ doubly transitive.

The doubly transitive groups which can act on a Hadamard matrix have been classified by Ito.

From this list a classification of Hadamard matrices with doubly transitive automorphism groups is easily deduced.

This list may be exploited to:

- Solve Horadam’s problem.
- Solve Ito and Leon’s problem.
- Construct a new family of skew Hadamard difference sets.
Lemma

Let $H$ be a Hadamard matrix developed from a $(4n - 1, 2n - 1, n - 1)$-difference set, $\mathcal{D}$ in the group $G$. Then the stabiliser of the first row of $H$ in $A_H$ contains a regular subgroup isomorphic to $G$.

Lemma

Suppose that $H$ is a cocyclic Hadamard matrix with cocycle $\psi : G \times G \to \langle -1 \rangle$. Then $A_H$ contains a regular subgroup isomorphic to $G$.

Corollary

If $H$ is a cocyclic Hadamard matrix which is also developed from a difference set, then $A_H$ is a doubly transitive permutation group.
The groups

Theorem (Ito, 1979)

Let $\Gamma \leq A_H$ be a non-affine doubly transitive permutation group acting on the set of rows of a Hadamard matrix $H$. Then the action of $\Gamma$ is one of the following.

- $\Gamma \cong M_{12}$ acting on 12 points.
- $\text{PSL}_2(p^k) \leq \Gamma$ acting naturally on $p^k + 1$ points, for $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.
- $\Gamma \cong \text{Sp}_6(2)$, and $H$ is of order 36.
The matrices

Theorem

Each of Ito’s doubly transitive groups is the automorphism group of exactly one equivalence class of Hadamard matrices.

Proof.

- If $H$ is of order 12 then $A_H \cong M_{12}$. (Hall)
- If $PSL_2(q) \triangleleft A_H$, then $H$ is the Paley matrix of order $q + 1$.
- $Sp_6(2)$ acts on a unique matrix of order 36. (Computation)

Corollary

Twin prime power Hadamard matrices are not cocyclic.

Skew difference sets

Definition

Let $D$ be a difference set in $G$. Then $D$ is skew if $G = D \cup D^{-1} \cup \{1_G\}$.

- The Paley difference sets are skew.
- Conjecture (1930’s): $D$ is skew if and only if $D$ is a Paley difference set.
- Proved in the cyclic case (1950s - Kelly).
- Exponent bounds obtained in the general abelian case.
- Disproved using permutation polynomials, examples in $\mathbb{F}_3^5$ and $\mathbb{F}_3^7$ (2005 - Ding, Yuan).
- Infinite families found in groups of order $q^3$ and $3^n$. (2008-2011 - Muzychuk, Weng, Qiu, Wang, ...).
Suppose that $H$ is developed from a difference set $\mathcal{D}$ and that $\mathcal{A}_H$ is non-affine doubly transitive. Then:

- $H$ is a Paley matrix.
- A result of Kantor: $\mathcal{A}_H \cong P\Sigma L_2(q)$.
- A point stabiliser is of index 2 in $A\Gamma L_1(q)$.
- Difference sets correspond to regular subgroups of the stabiliser of a point in $\mathcal{A}_H$.

Lemma

Let $\mathcal{D} \subseteq G$ be a difference set such that the associated Hadamard matrix $H$ has $\mathcal{A}_H$ non-affine doubly transitive. Then $G$ is a regular subgroup of $A\Gamma L_1(q)$ in its natural action.
Suppose that $q = p^{kp^\alpha}$. A Sylow $p$-subgroup of $A\Gamma L_1(q)$ is

$$G_{p,k,\alpha} = \left\langle a_1, \ldots, a_n, b \mid a_i^p = 1, [a_i, a_j] = 1, b^{p^\alpha} = 1, a_i^b = a_{i+k} \right\rangle.$$ 

Lemma (Ó C., 2011)

There are $\alpha + 1$ conjugacy classes of regular subgroups of $A\Gamma L_1(q)$. The subgroups

$$R_e = \left\langle a_1 b^{p^e}, a_2 b^{p^e}, \ldots, a_n b^{p^e} \right\rangle$$

for $0 \leq e \leq \alpha$ are a complete and irredundant list of representatives.
Lemma

Let $G$ be a group containing a difference set $\mathcal{D}$, and let $M$ be an incidence matrix of the underlying 2-design. Set $M^* = 2M - J$. That is,

$$M^* = [\chi(g_i g_j^{-1})]_{g_i, g_j \in G}$$

where the ordering of the elements of $G$ used to index rows and columns is the same, and where $\chi(g) = 1$ if $g \in \mathcal{D}$ and $-1$ otherwise. Then $M^* + I$ is skew-symmetric if and only if $\mathcal{D}$ is skew Hadamard.

- The Paley difference sets are skew.
- So the underlying 2-design $\mathcal{D}$ is skew.
- So any difference set associated $\mathcal{D}$ is skew.
Theorem (Ó C., 2011)

Let \( p \) be a prime, and \( n = kp^\alpha \in \mathbb{N} \).

- Define

\[
G_{p,k,\alpha} = \left\langle a_1, \ldots, a_n, b \mid a_i^p = 1, [a_i, a_j] = 1, b^{p^\alpha} = 1, a_i^b = a_{i+k} \right\rangle.
\]

- The subgroups

\[
R_e = \left\langle a_1 b^{p^e}, a_2 b^{p^e}, \ldots, a_n b^{p^e} \right\rangle
\]

for \( 0 \leq e \leq \alpha \) contain skew Hadamard difference sets.

- Each difference set gives rise to a Paley Hadamard matrix.

- These are the only non-affine difference sets which give rise to Hadamard matrices in which \( A_H \) is transitive.

- These are the only skew difference sets which give rise to Hadamard matrices in which \( A_H \) is transitive.