Doubly transitive group actions on designs and Hadamard matrices

Padraig Ó Catháin

National University of Ireland, Galway

16 November 2011
Outline

1. Introduction: Designs and Hadamard matrices
2. Cocyclic development
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 $\phi : V \times B \rightarrow \{0, 1\}$ given by $\phi(v, b) = 1$ if and only if $v \in b$. An *incidence matrix* for $\Delta$ is a matrix

$$M = [\phi(v, b)]_{v \in V, b \in B}.$$
Incidence structure $\leftrightarrow \{0, 1\}$-matrix (without repeated columns)

$\Delta \leftrightarrow M$

$\sigma \in \text{Aut}(\Delta) \leftrightarrow (P, Q) \text{ s.t. } PMQ^\top = M$
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 3-(8, 4, 1) design $\Delta$ with $V = \{1, \ldots, 7, \infty\}$ and blocks

\[
\begin{align*}
\{\infty, 1, 2, 3\} & \quad \{4, 5, 6, 7\} & \quad \{\infty, 1, 4, 5\} & \quad \{2, 3, 6, 7\} \\
\{\infty, 1, 6, 7\} & \quad \{2, 3, 4, 5\} & \quad \{\infty, 2, 4, 6\} & \quad \{1, 3, 5, 7\} \\
\{\infty, 2, 5, 7\} & \quad \{1, 3, 4, 6\} & \quad \{\infty, 3, 4, 7\} & \quad \{1, 2, 5, 6\} \\
\{\infty, 3, 5, 6\} & \quad \{1, 2, 4, 7\} & & \\
\end{align*}
\]

- Every 3-subset occurs in precisely 1 block.
- Every 2-subset occurs in 3 blocks: $\Delta$ is also a 2-(8, 4, 3) design.
- Finally, $\Delta$ is a 1-(8, 4, 7) design.
Example

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

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

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

\[ \begin{array}{c}
  7 \\
  \downarrow \\
  2 \\
  \downarrow \\
  1 \\
  \downarrow \\
  4 \\
  \downarrow \\
  3 \\
  \downarrow \\
  6 \\
  \downarrow \\
  5 \\
\end{array} \]
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 \( v_j \).
Theorem (Ryser)

Suppose the $(0, 1)$-matrix $M$ satisfies

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

Then $M^\top M = MM^\top$.

Corollary

The incidence structure $\mathcal{D}$ is a symmetric 2-design if and only if $D^*$ is.

Every pair of points lies on $\lambda$ blocks $\iff$ Every pair of blocks intersect in $\lambda$ points.
Difference sets

- 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 $d_id_j^{-1}$ 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’ in $C_4^2$. 

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 $G$. 
Proof.

- Denote by $\mathcal{D}$ the difference set in $G$ (written multiplicatively).
- Define an incidence structure, $\Delta$, by $V = \{g \mid g \in G\}$ and $B = \{g\mathcal{D} \mid g \in G\}$.
- Let $g \in V$ be incident with $h\mathcal{D} \in B$ if (and only if) $g \in h\mathcal{D}$.
- Furthermore $|g\mathcal{D} \cap h\mathcal{D}| = \lambda$: consider the equation $gd_i = hd_j$ with $d_i, d_j \in \mathcal{D}, g \neq h$. Rewrite as $d_id_j^{-1} = g^{-1}h$.
- There are precisely $\lambda$ solutions, since $\mathcal{D}$ is a difference set.
- So every pair of blocks meet in $\lambda$ points.
- Thus $\Delta^*$ is a $2- (v, k, \lambda)$ design as required.

The other direction requires careful labelling of points and blocks, but is similar.
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 $HH^\top = nl_n$.

\[
\begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix}
\begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix}
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix}
\]
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 \( PHQ^\top = H \).
- \( \text{Aut}(H) \) 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 $D$. Furthermore $\text{Aut}(D) < \mathcal{A}_H$.

Proof.

Let $M$ be an incidence matrix for $D$. 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.
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.
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 for all $g, h, k \in G$

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

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

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

Corollary
Suppose that $H$ is a cocyclic Hadamard matrix. Then $A_H$ contains a regular subgroup.
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 / $\geq 3 \times 10^6$</td>
<td>49 / 51</td>
<td>261 / 267</td>
</tr>
<tr>
<td>36</td>
<td>35 / $\geq 3 \times 10^6$</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?
Strategy

- 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.
Doubly transitive groups

Definition
A permutation group $G$ on $\Omega$ is doubly transitive if the induced action of $G$ on ordered pairs of $\Omega$ is transitive.

Lemma
A transitive group $G$ is doubly transitive if and only if $G_\alpha$ is transitive on $\Omega - \alpha$.

Theorem
The finite doubly transitive permutation groups are known.

Proof: Burnside, Hering, CFSG.
Lemma

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

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 $G$.

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 $\text{PSL}_2(q) \leq A_H$, then $H$ is the Paley matrix of order $q + 1$.
- $\text{Sp}_6(2)$ 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 $A_H$ is non-affine doubly transitive. Then:

- $H$ is a Paley matrix.
- A result of Kantor: $A_H \cong P\Sigma L_2(q)$, $q > 11$.
- 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 $A_H$.

**Lemma**

*Let $\mathcal{D} \subseteq G$ be a difference set such that the associated Hadamard matrix $H$ has $A_H$ 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 $\text{AGL}_1(q)$ 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 $\text{AGL}_1(q)$. 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,

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

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.