Hadamard matrices, difference sets and doubly transitive permutation groups

Padraig Ó Catháin

University of Queensland

13 November 2012
Outline

1. Hadamard matrices
2. Symmetric designs
3. Hadamard matrices and difference sets
4. Two-transitivity conditions
Overview

Difference set $\leftrightarrow$ Relative difference set

Symmetric Design $\leftrightarrow$ Hadamard matrix
Hadamard’s Determinant Bound

Theorem (Hadamard, 1893)

Let $M$ be an $n 	imes n$ matrix with complex entries. Denote by $r_i$ the $i^{th}$ row vector of $M$. Then

$$\det(M) \leq \prod_{i=1}^{n} \|r_i\|,$$

with equality precisely when the $r_i$ are mutually orthogonal.

Corollary

Let $M$ be as above. Suppose that $\|m_{ij}\| \leq 1$ holds for all $1 \leq i, j \leq n$. Then $\det(M) \leq \sqrt{n^n} = n^{n/2}$. 
Hadamard matrices

Matrices meeting Hadamard’s bound exist trivially. The character tables of abelian groups give examples for every order $n$. The problem for real matrices is more interesting.

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 $\det(H) = n^{\frac{n}{2}}$.

$H$ is Hadamard if and only if $HH^\top = nl_n$.

Equivalently, distinct rows of $H$ are orthogonal.

\[
\begin{pmatrix}
1 \\
1 \\
1
\end{pmatrix}
\begin{pmatrix}
1 & 1 \\
1 & -1 \\
1 & -1
\end{pmatrix}
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix}
\]
1867: Sylvester constructed Hadamard matrices of order $2^n$.

1893: Hadamard gave the maximal determinant characterisation and showed 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, and proposed investigation of when Hadamard matrices exist.

1934: 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.
Equivalence, automorphisms of Hadamard matrices

Definition

A signed permutation matrix is a matrix containing precisely one non-zero entry in each row and column. The non-zero entries are all 1 or $-1$. Denote by $\mathcal{W}$ the group of all signed permutation matrices, and let $H$ be a Hadamard matrix. Let $\mathcal{W} \times \mathcal{W}$ act on $H$ by

$$(P, Q) \cdot H = PHQ^\top.$$

- The equivalence class of $H$ is the orbit of $H$ under this action.
- The automorphism group of $H$, $\text{Aut}(H)$ is the stabiliser.
- $\text{Aut}(H)$ has an induced permutation action on the set $\{r\} \cup \{-r\}$.
- The 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 $A_H$. 

Padraig Ó Catháin

Hadamard matrices and difference sets

13 November 2012
Numerics at small orders

The total number of Hadamard matrices of order 32 is
63263484717718549429422548505408010969755998084039927770862019356599724585340056371200000000000000!

<table>
<thead>
<tr>
<th>Order</th>
<th>Hadamard matrices</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>0.25</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>$7 \times 10^{-4}$</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>$1.3 \times 10^{-13}$</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>$2.5 \times 10^{-30}$</td>
</tr>
<tr>
<td>16</td>
<td>5</td>
<td>$1.1 \times 10^{-53}$</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>$1.0 \times 10^{-85}$</td>
</tr>
<tr>
<td>24</td>
<td>60</td>
<td>$1.2 \times 10^{-124}$</td>
</tr>
<tr>
<td>28</td>
<td>487</td>
<td>$1.3 \times 10^{-173}$</td>
</tr>
<tr>
<td>32</td>
<td>13,710,027</td>
<td>$3.5 \times 10^{-212}$</td>
</tr>
<tr>
<td>36</td>
<td>$\geq 3 \times 10^6$</td>
<td>?</td>
</tr>
</tbody>
</table>
Applications of Hadamard matrices

- Design of experiments: Hadamard matrices provide constructions of Orthogonal Arrays of strengths 2 and 3.
- Signal Processing: sequences with low autocorrelation are provided by designs with circulant incidence matrices.
- Coding Theory: Walsh-Hadamard codes are linear and optimal with respect to the Plotkin bound. Such codes enjoy simple (and extremely fast) encryption and decryption algorithms. The code of length $2^5$ was used in the Mariner 9 mission.
- Quantum Computing: Hadamard matrices arise as unitary operators used for entanglement.
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 \((v, k, \lambda)\)-design if and only if any pair of elements of \(V\) occurs in exactly \(\lambda\) blocks.

Definition

The design \(\Delta\) is **symmetric** if \(|V| = |B|\).
Incidence matrices

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

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

Lemma
Denote the all 1s matrix of order $v$ by $J_v$. The $v \times v$ $(0, 1)$-matrix $M$ is the incidence matrix of a $2-(v, k, \lambda)$ symmetric design if and only if

$$MM^\top = (k - \lambda)I_v + \lambda J_v.$$

Proof.
Entry $(i, j)$ in $MM^\top$ is the inner product of the $i^{th}$ and $j^{th}$ rows of $M$. This is $|b_i \cap b_j|$.  

Padraig Ó Catháin
Hadamard matrices and difference sets
13 November 2012
A projective plane is an example of a symmetric design with $\lambda = 1$.

Example
Let $\mathbb{F}$ be any field. Then there exists a projective plane over $\mathbb{F}$ derived from a 3-dimensional $\mathbb{F}$-vector space. In the case that $\mathbb{F}$ is a finite field of order $q$ we obtain a geometry with

- $q^2 + q + 1$ points and $q^2 + q + 1$ lines.
- $q + 1$ points on every line and $q + 1$ lines through every point.
- Every pair of points lying on a unique line.
- Every pair of lines intersecting in a unique point.
Automorphisms of 2-designs

Definition

An **automorphism** of a symmetric 2-design $\Delta$ is a permutation $\sigma \in \text{Sym}(V)$ which preserves $B$ set-wise. Let $M$ be an incidence matrix for $\Delta$. Then $\sigma$ corresponds to a pair of permutation matrices such that $P\sigma M Q^\top = M$.

The automorphisms of $\Delta$ form a **group**, $\text{Aut}(\Delta)$.

Example

Let $\Delta$ be a projective plane of order $q + 1$. Then $\text{PSL}_2(q) \leq \text{Aut}(\Delta)$. 
Suppose that $G$ acts regularly on $V$, the set of points of a symmetric $2-(v, k, \lambda)$ design.

Labelling one point with $1_G$ induces a labelling of the remaining points in $V$ with elements of $G$.

Blocks of $\Delta$ are now subsets of $G$. The induced action of $G$ on blocks is also regular. It follows that every block is of the form $bg$ relative to some fixed base block $b$.

Identify $b$ with the $\mathbb{Z}G$ element $\hat{b} = \sum_{g \in b} g$, and denote by $\hat{b}(-1) = \sum_{g \in b} g^{-1}$.

Then $\hat{b} \hat{b}(-1) = \sum_{g \in b} \hat{b}g^{-1} = (k - \lambda)1_G + \lambda G$. 
Difference sets

Definition

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 $G$.

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 $G$. 
Example

Theorem (Singer)

The group $\text{PSL}_n(q)$ contains a cyclic subgroup acting regularly on the points of projective $n$-space.

Corollary

Every desarguesian projective plane is described by a difference set.

- Difference sets in abelian groups are studied using character theory and number theory.
- Many necessary and sufficient conditions for (non-)existence are known.
- Most known constructions for infinite families of Hadamard matrices come from difference sets.
Let $H$ be a normalised Hadamard matrix of order $4t$. 

$$H = \begin{pmatrix} 1 & \bar{1} \\ 1 & M \end{pmatrix}.$$ 

Denote by $J$ the all ones matrix of order $4t - 1$. Then $\frac{1}{2}(M + J)$ is a $(0, 1)$-matrix.

$$MM^\top = (4t)l_{4t-1} - J$$

$$\frac{1}{4}(M + J)(M + J)^\top = tl_{4t-1} + (t - 1)J$$

So $\frac{1}{2}(M + J)$ is the incidence matrix of a symmetric $(4t - 1, 2t - 1, t - 1)$ design.
Example: the Paley construction

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

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

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

is a Hadamard matrix.
Other sporadic Hadamard difference sets are known at these parameters.

But every known Hadamard difference set has the same parameters as one of those in the series above.

The first two families are infinite, the other two presumably so.
Difference set $\leftrightarrow$ Relative difference set

$\downarrow$

Symmetric Design $\leftrightarrow$ 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

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

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.
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?
Recall that any normalised Hadamard matrix has the form

\[ H = \begin{pmatrix} 1 & \bar{1} \\ \bar{1} & M \end{pmatrix}. \]

where \( M \) is a \( \pm 1 \) version of the incidence matrix of a \((4t - 1, 2t - 1, t - 1)\)-design, \( \Delta \).

Any automorphism of \( \Delta \) gives rise to a pair of permutation matrices such that \( PMQ^\top = M \). These extend to an automorphism of \( H \):

\[
\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix} \begin{pmatrix} 1 & \bar{1} \\ \bar{1} & M \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}^\top = H.
\]

So we obtain an injection \( \iota : \text{Aut}(\Delta) \hookrightarrow A_H \). Furthermore, \( \iota(P, Q) \) fixes the first row of \( H \) for any \( (P, Q) \in \text{Aut}(\Delta) \).
Doubly transitive group actions on Hadamard matrices

Lemma
Let \( H \) be a Hadamard matrix developed from a \((4n - 1, 2n - 1, n - 1)\)-difference set, \( D \) 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.
Theorem (Burnside, 1897)

Let $G$ be a doubly transitive permutation group. Then $G$ contains a unique minimal normal self-centralising subgroup, $N$. Either $N$ is elementary abelian, or $N$ is simple.

- In the first case, $G$ is affine, and $G = N \rtimes H$ where $H$ is quasi-cyclic or one of a list of classical groups acting naturally.
- In the second case, $G = N \rtimes H$ is almost simple and both $N$ and $H \leq \text{Aut}(N)$ are known.
The groups

Theorem (Kantor, Moorhouse)

If $\mathcal{A}_H$ is affine doubly transitive then $\mathcal{A}_H$ contains $\text{PSL}_n(2)$ and $H$ is a Sylvester matrix.

Theorem (Ito, 1979)

Let $\Gamma \leq \mathcal{A}_H$ 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 $\text{PSL}_2(q) \trianglelefteq A_H$, then $H$ is the Paley matrix of order $q + 1$.
- $\text{Sp}_6(2)$ acts on a unique matrix of order 36. (Computation)
The difference sets, I

We classify the \((4t - 1, 2t - 1, t - 1)\) difference sets \(\mathcal{D}\) for which the associated Hadamard matrix \(H\) is cocyclic.

**Theorem (Affine case, Ó C.)**

Suppose that \(H\) is cocyclic and that \(A_H\) is affine doubly transitive.

- Then \(A_H\) contains a sharply doubly transitive permutation group.
- These have been classified by Zassenhaus. All such groups are contained in \(A\Gamma L_1(2^n)\).
- So difference sets are in bijective correspondence with conjugacy classes of regular subgroups of \(A\Gamma L_1(2^n)\).
- Every difference set obtained in this way is contained in a metacyclic group and gives rise to a Sylvester matrix.
The difference sets, II

Theorem (Non-affine case, Ó C., 2012, JCTA)

Let $p$ be a prime, $k, \alpha \in \mathbb{N}$, and set $n = kp^\alpha$.

Define

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

The subgroups $R_e = \langle a_1 b^{p^e}, a_2 b^{p^e}, \ldots, a_n b^{p^e} \rangle$ 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 skew difference sets which give rise to Hadamard matrices in which $A_H$ is transitive.