Outline

1. (Finite) Projective planes
2. Symmetric Designs
3. Difference sets
4. Doubly transitive group actions on Hadamard matrices
Definition

Let \( V \) be a set whose elements are points, and let \( B \) be a set of subsets of \( V \) whose elements are called lines. Then \( (V, B) \) is a projective plane if the following axioms hold:

1. Any two distinct points are incident with a unique line.
2. Any two distinct lines are incident with a unique point.
3. There exist four points no three of which are co-linear.

Bijections are easily established between:

1. The lines containing \( x \) and the points on a line not containing \( x \).
2. The points of two distinct lines.
3. The number of lines and the number of points, etc.
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 lines intersecting in a unique point.

Symmetric designs are a generalization of finite projective planes, and give a unified approach to many combinatorial objects.
Definition

Let $V$ be a set of size $v$ and let $B$ be a set of $k$ subsets of $V$ (now called blocks). Then $\Delta = (V, B)$ is a symmetric $(v, k, \lambda)$-design if every pair of blocks intersect in a fixed number $\lambda$ of points.

A projective plane is a symmetric design with $(v, k, \lambda) = (q^2 + q + 1, q + 1, 1)$.

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 matrices**

**Lemma**

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

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

**Lemma (Ryser)**

Suppose that $M$ is a square $(0,1)$ matrix satisfying $MM^\top = \alpha I + \beta J$. Then

$$M^\top M = \alpha I + \beta J.$$  

The matrix $M^\top$ is incidence matrix of the dual of $\Delta$. Thus a little linear algebra and combinatorics recovers the classical duality of projective spaces (in this finite setting).
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 $HH^T = nI_n$.

\[
\begin{pmatrix}
1 \\
1 \\
1 \\
1
\end{pmatrix}
\begin{pmatrix}
1 & 1 \\
1 & -1 \\
1 & 1 \\
1 & -1
\end{pmatrix}
\begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix}
\]
Hadamard matrices

- 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 $4n$ for some $n \in \mathbb{N}$. 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.
Lemma

There exists a Hadamard matrix $H$ of order $4n$ if and only there exists a $2-(4n - 1, 2n - 1, n - 1)$ design $D$.

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, $H$.

For this reason, a symmetric $2-(4n - 1, 2n - 1, n - 1)$ design is called a Hadamard design.
Automorphisms of 2-designs

Definition
Let $\Delta = (V, B)$ be a symmetric design, and let $S_V$ be the full symmetric group on $V$. Then $S_V$ has an induced action on $B$. The stabiliser of $B$ under this action is the **automorphism group** of $\Delta$, $\text{Aut}(\Delta)$.

Definition
A subgroup $G$ of $S_V$ is called **regular** if for any $v_i, v_j \in V$, there exists a unique $g \in G$ such that $v_i^g = v_j$.

In the remainder of this talk we will be interested in regular subgroups of $\text{Aut}(\Delta)$. 
Suppose that $G$ acts regularly on $V$.
Labelling one point with $1_G$ induces a labelling of the remaining points in $V$ with elements of $G$.
So blocks of $\Delta$ are subsets of $G$.
$G$ also acts regularly on the blocks (linear algebra again).
Denote by $D$ one block of $G$. Then every other block of $\Delta$ is of the form $Dg$. 
Difference sets

Let $G$ be a group of order $v$, and $D$ a $k$-subset of $G$. Suppose that every non-identity element of $G$ has $\lambda$ representations of the form $d_id_j^{-1}$ where $d_i, d_j \in D$. Then $D$ 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 $G$.***
Recall that the automorphism group of $\text{PG}_2(q)$ is $\text{PGL}_3(q)$.

**Theorem (Singer)**

The group $\text{PGL}_3(q)$ contains a cyclic subgroup of order $q^2 + q + 1$ which acts regularly on the points of $\text{PG}_2(q)$ and regularly on the lines of $\text{PG}_2(q)$.

**Corollary**

So there exists a $(q^2 + q + 1, q + 1, 1)$ difference set in the cyclic group of order $q^2 + q + 1$.

Example: Consider the set $\{0, 1, 3\}$ in $\mathbb{Z}/7\mathbb{Z}$, or the set $\{0, 1, 3, 9\}$ in $\mathbb{Z}/13\mathbb{Z}$, which generate the projective planes of orders 2 and 3.
Hadamard difference sets

- From a \((v, k, \lambda)\)-difference set, we can construct a symmetric 2-(\(v, k, \lambda\)) design.
- From a symmetric 2-(\(4t - 1, 2t - 1, t - 1\)) design, we can construct a Hadamard matrix.
- So from a \((4t - 1, 2t - 1, t - 1)\) difference set, we can construct a Hadamard matrix.
- There are four classical families of difference sets with these parameters.
Example: the Paley construction

- 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
  \[
  H = \begin{pmatrix}
  1 & \bar{1} \\
  \bar{1}^T & Q - I
  \end{pmatrix}
  \]
  is a Hadamard matrix.
### Families of Hadamard difference sets

<table>
<thead>
<tr>
<th>Difference set</th>
<th>Matrix</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singer</td>
<td>Sylvester</td>
<td>$2^n$</td>
</tr>
<tr>
<td>Paley</td>
<td>Paley Type I</td>
<td>$p^\alpha + 1$</td>
</tr>
<tr>
<td>Stanton-Sprott</td>
<td>TPP</td>
<td>$p^\alpha q^\beta + 1$</td>
</tr>
<tr>
<td>Sextic residue</td>
<td>HSR</td>
<td>$p + 1 = x^2 + 28$</td>
</tr>
</tbody>
</table>

- 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.
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 \(A_H\).
Induced automorphisms

Let $\Delta$ be a symmetric 2-$(4t - 1, 2t - 1, t - 1)$ design with incidence matrix $M$, and let $\sigma$ be an automorphism of $\Delta$. Then there exist permutation matrices $P, Q$ such that

$$M = PMQ^\top$$

**Lemma**

Let $\Delta$ be a symmetric 2-$(4t - 1, 2t - 1, t - 1)$ design with associated Hadamard matrix $H$. Then

$$\begin{pmatrix} 1 & \bar{0} \\ \bar{0}^\top & P \end{pmatrix} \begin{pmatrix} 1 & \bar{1} \\ \bar{1}^\top & 2M - J \end{pmatrix} \begin{pmatrix} 1 & \bar{0} \\ \bar{0}^\top & Q \end{pmatrix}^\top = H$$

So every automorphism of $\Delta$ induces an automorphism of $H$.

$$\text{Aut}(\Delta) \hookrightarrow \mathcal{A}_H$$
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

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

- Let $\langle -, - \rangle$ be the usual dot product on $k = \mathbb{F}_2^n$.
- This is a 2-cocycle.
- The matrix $H = \left[ -1^{\langle u, v \rangle} \right]_{u,v \in k}$ is Hadamard and equivalent to the Sylvester matrix.
- So the Sylvester matrices are cocyclic.
- Likewise the Paley matrices are cocyclic, though this is not as easily seen.

Conjecture (Horadam): The TPP-Hadamard matrices are cocyclic. We answer this, and the corresponding question for HSR-matrices also.
Doubly transitive group actions on Hadamard matrices

Doubly transitive groups

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 $G$.

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.
Classification of doubly transitive groups

- Burnside: Either a doubly transitive group contains a regular elementary abelian subgroup (and so is of degree $p^k$), or is almost simple.
- Following the CFSG, all (finite) doubly transitive permutation groups have been classified.
- The classification provides detailed character theoretic information on the doubly transitive groups.
- This can be used to show that most doubly transitive groups do not act on Hadamard matrices. (Ito)
- Then the Hadamard matrices can be classified, and we can test whether the TPP and HSR-matrices are among them.
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.

1. $\Gamma \cong M_{12}$ acting on 12 points.
2. $PSL_2(p^k) \subseteq \Gamma$ acting naturally on $p^k + 1$ points, for $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.
3. $\Gamma \cong Sp_6(2)$, and $H$ is of order 36.
The matrices

Theorem (Ó C.?)

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 $\mathcal{A}_H \cong M_{12}$. (Hall)
- If $\text{PSL}_2(q) \trianglelefteq \mathcal{A}_H$, 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.*

Proof.

A twin prime power matrix has order $p^\alpha q^\beta + 1$. Non-affine: The only order of this form among those in Ito’s list is 36, but $Sp_6(2)_1$ does not contain a regular subgroup. So no TPP-matrix has a non-affine doubly transitive permutation group.

Affine: The result follows from an application of Zsigmondy’s theorem.

HSR matrices are not cocyclic

Corollary

*The sextic residue difference sets are not cocyclic.*

Proof.

Non-affine: An argument using cyclotomy shows that the sextic residue difference sets and Paley difference sets never co-incide. Affine: An old result of Mordell shows that $2^n = x^2 + 7$ has a solution only for $n = 3, 4, 5, 7, 15$. Now, $2^{n+2} = (2x)^2 + 28$ is of the form $p + 1$ only if $p \in \{31, 127, 131071\}$. We deal with these via ad hoc methods.

Ó C.: Difference sets and doubly transitive group actions on Hadamard matrices. (Includes a full classification of the difference sets for which $H$ is non-affine cocyclic and a new family of skew-Hadamard difference sets.) *JCTA*, 2012.