Doubly transitive group actions on designs and Hadamard matrices

Padraig Ó Catháin

National University of Ireland, Galway

16 November 2011

Outline

Incidence Structures

Definition

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

Definition

An ***automorphism*** of Δ is a permutation $\sigma \in \mathrm{Sym}(V)$ 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 Δ is a matrix

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

$$\begin{aligned}
\text{Incidence structure} &\quad\longleftrightarrow\quad \{0,1\}\text{-matrix (without repeated columns)} \\
\Delta &\quad\longleftrightarrow\quad M \\
\sigma \in \mathrm{Aut}(\Delta) &\quad\longleftrightarrow\quad (P,Q) \text{ s.t. } PMQ^{\top} = M
\end{aligned}$$

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, λ) ***design*** if and only if any t-subset of V occurs in exactly λ blocks.

Definition

The design Δ is ***symmetric*** if $|V| = |B|$.

Example

A 3-$(8, 4, 1)$ design Δ with $V = \{1, \ldots, 7, \infty\}$ and blocks

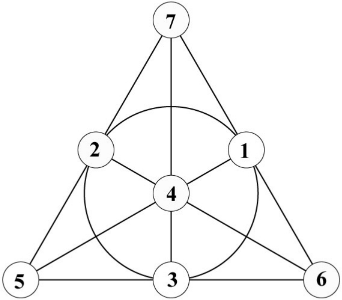
$$\begin{array}{llll} \{\infty, 1, 2, 3\} & \{4, 5, 6, 7\} & \{\infty, 1, 4, 5\} & \{2, 3, 6, 7\} \\ \{\infty, 1, 6, 7\} & \{2, 3, 4, 5\} & \{\infty, 2, 4, 6\} & \{1, 3, 5, 7\} \\ \{\infty, 2, 5, 7\} & \{1, 3, 4, 6\} & \{\infty, 3, 4, 7\} & \{1, 2, 5, 6\} \\ \{\infty, 3, 5, 6\} & \{1, 2, 4, 7\} & & \end{array}$$

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

Example

A symmetric 2-$(7, 3, 1)$ design, Δ (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, $\mathrm{Aut}(\mathcal{D}) \cong PGL_3(2)$.

Lemma

The $v \times v$ $(0,1)$-matrix M is the incidence matrix of a 2-(v, k, λ) 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 λ blocks $\Longleftrightarrow$ Every pair of blocks intersect in λ 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 λ representations of the form $d_i d_j^{-1}$ where $d_i, d_j \in \mathcal{D}$.
- Then $\mathcal{D}$ is a (v, k, λ)-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 $G < \mathrm{Sym}(V)$ 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, λ)-difference set then there exists a symmetric 2-(v, k, λ) design on which G acts regularly. Conversely, a 2-(v, k, λ) design on which G acts regularly corresponds to a (v, k, λ)-difference set in G.

Proof - the first half

Proof.

- Denote by $\mathcal{D}$ the difference set in G (written multiplicatively).
- Define an incidence structure, Δ, by $V = \{g \mid g \in G\}$ and $B = \{g\mathcal{D} \mid g \in G\}$.
- Let $g \in V$ be incident with $h\mathcal{D} \in \mathcal{B}$ 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 $d_i d_j^{-1} = g^{-1}h$.
- There are precisely λ solutions, since $\mathcal{D}$ is a difference set.
- So every pair of blocks meet in λ points.
- Thus Δ^* 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 $HH^\top = nI_n$.

$$\left(\begin{array}{c} 1 \end{array} \right) \quad \left(\begin{array}{rr} 1 & 1 \\ 1 & -1 \end{array} \right) \quad \left(\begin{array}{rrrr} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array} \right)$$

- Sylvester constructed Hadamard matrices of order 2^n.
- Hadamard showed that the determinant of a Hadamard matrix $H = \left[h_{i,j}\right]$ of order n is maximal among all matrices of order n over $\mathbb{C}$ whose entries satisfy $\left\|h_{i,j}\right\| \leq 1$ 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 $\mathcal{A}_H$.

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 $\mathrm{Aut}(\mathcal{D}) < \mathcal{A}_H$.

Proof.

Let M be an incidence matrix for $\mathcal{D}$. Then M satisfies $MM^\top = nI + (n-1)J$. So $(2M-J)(2M-J)^\top = 4nI - J$. 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 *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 χ be the quadratic character of 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

$$H = \begin{pmatrix} 1 & \overline{1} \\ \overline{1}^\top & Q - I \end{pmatrix}$$

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 $\mathcal{A}_H$ contains a regular subgroup.

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.*

With Marc Röder: The cocyclic Hadamard matrices of order less than 40, *Designs, Codes and Cryptography*, 2011.

Table of results

Order	Cocyclic	Indexing Groups	Extension Groups
2	1	1	2
4	1	2	3 / 5
8	1	3 / 5	9 / 14
12	1	3 / 5	3 / 15
16	5	13 / 14	45 / 51
20	3	2 / 5	3 / 14
24	16 / 60	8 / 15	14 / 52
28	6 / 487	2 / 4	2 / 13
32	$100/ \geq 3 \times 10^6$	49/51	261/267
36	$35 / \geq 3 \times 10^6$	12 /14	21 / 50

Comprehensive data available at: 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:

n	Hadamard matrices	Cocyclic Hadamard matrices
2	0.25	0.25
4	7×10^{-4}	0.125
8	1.3×10^{-13}	7.8×10^{-3}
12	2.5×10^{-30}	1.4×10^{-4}
16	1.1×10^{-53}	1.7×10^{-4}
20	1.0×10^{-85}	1.1×10^{-6}
24	1.2×10^{-124}	1.8×10^{-7}
28	1.3×10^{-173}	1.0×10^{-8}

Doubly transitive group actions on Hadamard matrices

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 $\mathcal{A}_H$ 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 Ω is *doubly transitive* if the induced action of G on ordered pairs of Ω is transitive.

Lemma

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

Theorem

The finite doubly transitive permutation groups are known.

Proof: Burnside, Hering, CFSG.

Doubly transitive group actions on Hadamard matrices

Lemma

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

Corollary

If H is a cocyclic Hadamard matrix which is also developed from a difference set, then $\mathcal{A}_H$ is a doubly transitive permutation group.

The groups

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 Γ is one of the following.

- $\Gamma \cong M_{12}$ *acting on* 12 *points.*
- $PSL_2(p^k) \trianglelefteq \Gamma$ *acting naturally on* $p^k + 1$ *points, for* $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.
- $\Gamma \cong Sp_6(2)$, *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 $\mathcal{A}_H \cong M_{12}$. (Hall)
- If $PSL_2(q) \trianglelefteq \mathcal{A}_H$, 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.

With Dick Stafford: On twin prime power Hadamard matrices, *Cryptography and Communications*, 2011.

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 familes 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: $\mathcal{A}_H \cong P\Sigma L_2(q)$, $q > 11$.
- 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 $\mathcal{A}_H$.

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

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

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*

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

- *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* $\mathcal{A}_H$ *is transitive.*
- *These are the only skew difference sets which give rise to Hadamard matrices in which* $\mathcal{A}_H$ *is transitive.*