Doubly transitive group actions on Hadamard matrices and skew difference sets

Padraig Ó Catháin

National University of Ireland, Galway

De Brún Workshop 5, 11 April 2011

Outline

What is a design?

Definition

Let V be a set of size v, and B a collection of subsets of V, each of (fixed) size $k > 0$. We say that $\mathcal{D} = (V, B)$ is a t-(v, k, λ) *design* if any t-subset of V occurs in exactly λ elements of B.

Definition

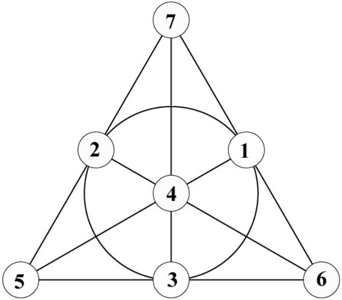
The permutation $\sigma \in \mathcal{S}_P$ is an *automorphism* of $\mathcal{D}$ if $B^\sigma = B$.

Definition

The design $\mathcal{D}$ is *symmetric* if $|V| = |B|$.

Example

- A symmetric 2-$(7,3,1)$ design, $\mathcal{D}$ (the Fano plane).
- $P = \{1,2,3,4,5,6,7\}$, $B =$
$\{\{1,2,3\},\{1,4,5\}, V\{1,6,7\},\{2,4,6\},\{2,5,7\},\{3,4,7\},\{3,5,6\}\}$



A sample automorphism of $\mathcal{D}$ is $(2,4,6)(3,5,7)$. In fact, $\mathrm{Aut}(\mathcal{D}) \cong PGL_3(2)$.

Automorphisms of incidence matrices

Under a suitable labelling of rows and columns, $\mathcal{D}$ is represented by

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathrm{Aut}(\mathcal{D})$ has a representation as pairs (P, Q) of permutation matrices with action $(P, Q)M = PMQ^{\top} = M$. (Permutation action of $\mathrm{Aut}(\mathcal{D})$ on rows of M!)

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 λ representations of the form $d_i d_j^{-1}$ where $d_i, d_j \in D$.
- Then D is a (v, k, λ)-difference set in G.

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 D the difference set in G (written multiplicatively).
- Define an incidence structure, $\mathcal{D}$, by $\mathcal{V} = \{g \mid g \in G\}$ and $\mathcal{B} = \{Dg \mid g \in G\}$.
- Let $g \in \mathcal{V}$ be incident with $Dh \in \mathcal{B}$ if (and only if) $g \in Dh$.
- Every block has size k: $|Dg| = |Dh|$.
- Furthermore $|Dg \cap Dh| = \lambda$: consider the equation $d_i g = d_j h$ with $d_i, d_j \in D$, $g \neq h$. Rewrite as $d_i d_j^{-1} = (hg^{-1})^{d_j^{-1}}$.
- There are precisely λ solutions, since D is a difference set.
- Thus $\mathcal{D}$ is a $2-(v, k, \lambda)$ design as required.

The other direction requires careful labelling of points and blocks, but is similar. □

Example

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

- A circulant matrix: $\mathbb{Z}_7$ acts regularly.
- So there exists a difference set in $\mathbb{Z}_7 : \{1, 2, 4\}$.

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 $HH^\top = nI_n$.

- Sylvester constructed Hadamard matrices of order $n = 2^t$.
- Hadamard constructed matrices of orders 12 and 20, and showed that the order had to be a multiple of 4.
- Paley constructed Hadamard matrices of order $n = p^t + 1$ for primes p, and conjectured that a Hadamard matrix of order n exists whenever $4 \mid n$. (cf. Schmidt)
- 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 D. Furthermore $\mathrm{Aut}(D) < \mathcal{A}_H$.

Proof.

Let M be an incidence matrix for 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. □

Corollary

Suppose that D is a $(4n-1, 2n-1, n-1)$-difference set. Then the stabiliser of the first row in $\mathcal{A}_H$ is transitive on the remaining rows of H_D.

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

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

is a Hadamard matrix.

Lemma

If G is transitive on X and G_α is transitive on $X - \{\alpha\}$ then G is doubly transitive on X.

Corollary

If a Hadamard matrix H is developed from a difference set, and $\mathcal{A}_H$ is transitive, then $\mathcal{A}_H$ is doubly transitive on the rows of H.

Problem

- *Classify the doubly transitive groups which act on Hadamard matrices.*
- *Classify the Hadamard matrices with doubly transitive automorphism groups.*
- *Classify the difference sets (if any) from which these Hadamard matrices are developed.*

Motivation

- Horadam: Do the Hadamard matrices developed from twin prime power difference sets have transitive automorphism groups? (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?

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.

- $\Gamma \cong M_{12}$ *and H is the unique Hadamard matrix of order* 12.
- $PSL_2(p^k) \trianglelefteq \Gamma$ *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.

- M_{12} is the automorphism group of the unique Hadamard matrix of order 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. (Nakic)

□

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, . . .).

Theorem (Ó C.)

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 $\mathcal{A}_H$ is transitive.*

Proof.

- Ito's theorem: suffices to find all regular subgroups of the stabiliser of a point in $\mathcal{A}_H$, where H is Paley.
- Kantor's theorem: $\mathcal{A}_H$ is $P\Sigma L_2(q)$ in its natural action.
- So a point stabiliser is of index 2 in $A\Gamma L_1(q)$.
- We constructed all regular subgroups of this group: there is a single $P\Sigma L_2(q)$ conjugacy class of each of the groups described above.
- A calculation together with Paley's theorem shows that the sets given above are difference sets.
- Assumption of the existence of others leads to a contradiction.

$\square$