Doubly transitive groups and Hadamard matrices

Padraig Ó Catháin

National University of Ireland, Galway

International workshop on Hadamard matrices and applications
RMIT, 29 November 2011

Outline

1. The permutation group of a matrix
2. 2-Designs, Difference sets, Hadamard matrices
3. Doubly transitive group actions on Hadamard matrices

Automorphisms of a matrix

- Let M be an $n \times n$ matrix with entries in a commutative ring R.
- Then a pair (P, Q) of $U(R)$-monomial matrices is an *automorphism* of M if and only if

$$PMQ^{-1} = M.$$

- The set of all automorphisms of M forms a group under composition, denoted $\mathrm{Aut}(M)$.

But this is not a permutation group...

Definition

Denote by A the set of all entries in M together with 1_R. Then the *expanded matrix* of M is

$$E_M = \left[a_i a_j M\right]_{a_i, a_j \in A}.$$

Lemma

There exists a homomorphism $\alpha : \mathrm{Aut}(M) \to \mathrm{Aut}(E_M)$*, such that the image of* $(P, Q) \in \mathrm{Aut}(M)$ *is a pair of permutation matrices.*

A permutation quotient

Suppose that M is invertible (possibly over some extension of R).

- Then P uniquely determines Q:

$$PMQ^{-1} = M \iff P = MQM^{-1}$$

- So the map $\beta : (P, Q) \mapsto P$ is an isomorphism of groups.
- Thus we can consider $\beta\alpha(\mathrm{Aut}(M))$ as a permutation group on the $n\,|A|$ rows of E_M.
- Linearity of the $\mathrm{Aut}(M)$ action gives an obvious system of imprimitivity: blocks are $\{ar_i \mid a \in A\}$.
- Consider the induced action on this block system.
- A monomial matrix P can be written in the form XY where X is diagonal and Y is a permutation matrix. The map $\rho : P \mapsto Y$ is a homomorphism on any monomial group.
- This permutation group of degree n is $\mathcal{A}(M) = \rho\beta(\mathrm{Aut}(M))$.

Cocyclic development

Definition

Let G be a finite group and C an abelian group. Then $\psi : G \times G \to C$ is a (2-)cocycle if it obeys the identity

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

for all $g, h, k \in G$.

Definition

Let R be a commutative ring, M an $n \times n$ matrix R-matrix. Suppose there exist a cocycle $\psi : G \times G \to U(R)$ and a set map $\phi : G \to R$ such that

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

Then M is *cocyclic* over G.

Which matrices are cocyclic?

Theorem (de Launey & Flannery)

The matrix M is cocyclic over G if and only if $\mathrm{Aut}(M)$ *contains a subgroup* Γ *such that*

- Γ *contains a central subgroup* Θ *isomorphic to a finite subgroup of* $U(R)$.
- $\Gamma/\Theta \cong G$.
- $\alpha(\Gamma)$ *has induced regular actions on the rows and columns of* E_M.

Cocyclic development and $\mathcal{A}(M)$

- Suppose that M is cocyclic over G.
- Then $\mathrm{Aut}(M)$ contains a subgroup Γ as in the Theorem.
- The image of Γ in $\mathcal{A}(M)$ is a regular subgroup.
- So cocyclic development $\Rightarrow$ existence of a regular subgroup in $\mathcal{A}(M)$.
- Unfortunately the converse is not so straightforward: we require a regular subgroup of $\mathcal{A}(M)$ to satisfy some additional conditions.

Designs

Definition

Let V be a set of order v (whose elements are called points), and let B be a set of k-subsets of V (whose elements are called blocks). 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 $|V| = |B|$.

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

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

Definition

The automorphism group of M consists of all pairs of $\{1\}$-monomial (i.e. permutation) matrices such that

$$PMQ^{\top} = M.$$

Definition

An ***automorphism*** of the design Δ is a permutation $\sigma \in \mathrm{Sym}(V)$ which preserves B setwise.

- An automorphism σ of Δ induces a permutation of the rows of M.
- In fact, $\mathrm{Aut}(\Delta) = \mathcal{A}(M)$.
- It is known that for symmetric 2-designs

$$\mathrm{Aut}(\Delta) \cong \mathrm{Aut}(M) \cong \mathcal{A}(M).$$

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.
- e.g. $\{1, 2, 4\}$ in $\mathbb{Z}_7$.

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.

Hadamard matrices, automorphisms

Definition

An automorphism of a Hadamard matrix H is a pair of $\{\pm 1\}$-monomial matrices such that

$$PHQ^\top = H.$$

The set of all automorphisms form a group, $\mathrm{Aut}(H)$.

- $\mathcal{A}(H)$ is a permutation group on the rows of H.
- The kernel of the map $\mathrm{Aut}(H) \to \mathcal{A}(H)$ consists of automorphisms whose first component is diagonal.
- $(-I, -I)$ is always an automorphism of H, so that this kernel if always non-trivial.
- If H is cocyclic, then $\mathcal{A}(H)$ contains a regular subgroup.

Hadamard matrices, 2-designs and difference sets

Lemma

There exists a Hadamard matrix H of order $4t$ if and only if there exists a 2-$(4t-1, 2t-1, t-1)$ design $\mathcal{D}$. Furthermore $\text{Aut}(\mathcal{D})$ embeds into the stabiliser of a point in $\mathcal{A}(H)$.

Corollary

Suppose that H is developed from a $(4t-1, 2t-1, t-1)$-difference set. Then the stabiliser of the first row of H in $\mathcal{A}(H)$, is transitive on the remaining rows of H.

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 $4t$.

- 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 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.

Doubly transitive group actions on Hadamard matrices

Two constructions of Hadamard matrices: from $(4t-1, 2t-1, t-1)$ difference sets, and from (orthogonal) cocycles.

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?

Doubly transitive group actions on Hadamard matrices

Lemma

Let H be a Hadamard matrix developed from a $(4t-1, 2t-1, t-1)$-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.

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.

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.

Which of these matrices is cocyclic?

- The two sporadic examples can be tested by hand.
- Only the Paley type I matrices remain:
- Classified by de Launey & Stafford.

Corollary

Let H be a Hadamard matrix with $\mathcal{A}(H)$ non-affine doubly transitive. Then either H is cocyclic, or H a specific matrix of order 36.

Which of these matrices is developed from a difference set?

- The two sporadic examples can be tested by hand.
- The Paley type I matrices are defined in terms of difference sets.

Corollary

Let H be a Hadamard matrix developed from a difference set (with $\mathcal{A}(H)$ non-affine). Then H is cocyclic if and only if H is a Paley matrix.

Classifying these difference sets

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.

Theorem (Kantor)

Let H be the Paley Hadamard matrix of order $q+1$, $\mathbf{q > 11}$. Then $\mathcal{A}(H) \cong P\Sigma L_2(q)$.

- 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

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.

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, Xiang, ...).

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 to $\mathcal{D}$ 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 skew difference sets which give rise to Hadamard matrices in which $\mathcal{A}(H)$ is transitive.*
- *If $\mathcal{A}(H)$ is transitive and H is developed from a difference set $\mathcal{D}$, then $\mathcal{D}$ is one of the difference sets described above.*