Automorphisms of Hadamard matrices and skew difference sets

Padraig Ó Catháin

National University of Ireland, Galway

Algebraic Combinatorics: in memory of Bob Liebler
Fort Collins, 4 November 2011

Outline

1. Designs, difference sets and Hadamard matrices
2. Cocyclic development
3. Doubly transitive group actions on Hadamard matrices

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 $|V| = |B|$.

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

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

An automorphism σ of Δ induces permutations of the rows and columns of M, represented as a pair of permutation matrices (P, Q) such that $PMQ^\top = M$.

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.
- We say $\mathcal{D}$ is *skew* if $G = \mathcal{D} \cup \mathcal{D}^{(-1)} \cup \{1_G\}$.

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.

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 $HH^\top = nI_n$.

$$\begin{pmatrix} 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

The Hadamard conjecture: does there exist a Hadamard matrix of order $4t$ for all $t \in \mathbb{N}$?

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 $4t$ *if and only there exists a* $2\text{-}(4t-1, 2t-1, t-1)$ *design* $\mathcal{D}$*. Furthermore* $\text{Aut}(\mathcal{D}) < \mathcal{A}_H$*.*

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.*

Group development

Definition

An $n \times n$ R-matrix, M, is group developed over G, a group of order n, if and only if there exists a set map $\phi : G \to R$ such that

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

Lemma

M is group developed over G if and only if $\mathrm{Aut}(M)$ contains a subgroup of pairs of permutation matrices isomorphic to G, which acts regularly on the rows and regularly on the columns of M.

Lemma

Suppose that H is a $4t \times 4t$ Hadamard matrix with constant row sums. Then t is a perfect square.

Corollary

A group developed Hadamard matrix has square order.

What about regular subgroups of $\mathcal{A}_H$?

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

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

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

Definition

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

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

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.*

In particular: if H is cocyclic then $\mathcal{A}_H$ is transitive.

Definition

Let G be a finite group of order mn, with normal subgroup N of order n. We say that $R \subset G$ is a relative difference set (RDS) with respect to N if in the multiset of elements $\left\{r_1 r_2^{-1} \mid r_1, r_2 \in R\right\}$ every element of $G - N$ occurs exactly λ times, and no non-trivial element of N occurs.

If $|R| = k$ we speak of a (m, n, k, λ)-RDS.

Theorem

A classification of $(4t, 2, 4t, 2t)$*-RDSs in the groups of order* $8t$ *yields a classification of cocyclic Hadamard matrices of order* $4t$*.*

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?

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, $\mathcal{D}$ 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.

Classifying 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 $q+1$. 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*

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

- *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 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.*