Difference sets and Hadamard matrices

Padraig Ó Catháin

National University of Ireland, Galway

6 February 2012

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

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

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

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 $|V| = |B|$.

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

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

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 $HH^\top = nI_n$.

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

Hadamard matrices

- 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.

2-designs and Hadamard matrices

Lemma

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

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. □

For this reason, a symmetric 2-$(4t-1, 2t-1, t-1)$ design is called a **Hadamard design**.

Automorphisms of 2-designs

Definition

An ***automorphism*** of a symmetric 2-design Δ is a permutation $\sigma \in \mathrm{Sym}(V)$ which preserves B setwise.

The automorphisms of Δ form a **group**, $\mathrm{Aut}(\Delta)$. **Difference sets** correspond to regular subgroups of $\mathrm{Aut}(\Delta)$.

Difference sets

- 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 Δ are subsets of G.
- G also acts regularly on the blocks.
- So all the blocks are translates of one another, and the elements of any block form a **difference set**.

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.

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.

- From a (v, k, λ)-difference set, we can construct a symmetric 2-(v, k, λ) 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.

Families of Hadamard difference sets

Difference set	Matrix	Order
Singer	Sylvester	2^n
Paley	Paley Type I	$p^\alpha + 1$
Stanton-Sprott	TPP	$p^\alpha q^\beta + 1$
Sextic residue	HSR	$p + 1 = x^2 + 28$

- 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.

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 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.

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 $\mathcal{A}_H$.

Induced automorphisms

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

$$M = PMQ^\top$$

Lemma

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

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

So every automorphism of Δ induces an automorphism of H.

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

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

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

- 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.

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.

- 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 $\Gamma \leq \mathcal{A}_H$ 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 (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 $PSL_2(q) \trianglelefteq \mathcal{A}_H$, then H is the Paley matrix of order $q+1$.
- $Sp_6(2)$ acts on a unique matrix of order 36. (Computation)

□

TPP matrices are not cocyclic

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. □

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

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. (Also includes a new family of skew-Hadamard difference sets.) To appear (soon hopefully!).