Difference sets and Hadamard matrices

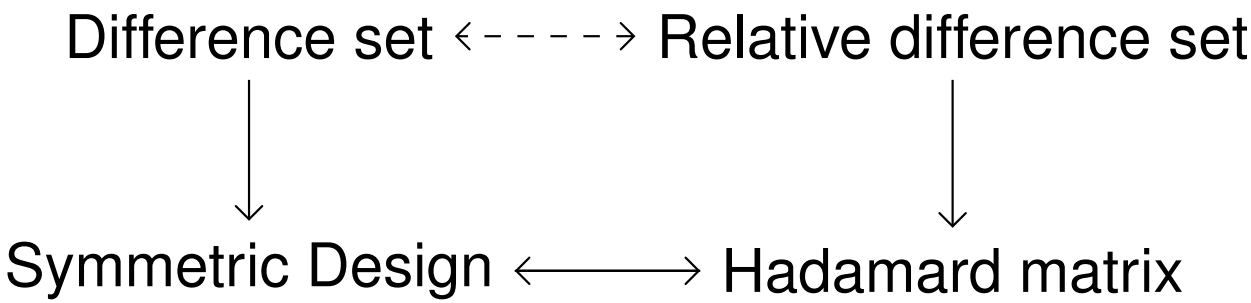
Padraig Ó Catháin

University of Queensland

5 November 2012

Outline

Overview


Difference set
Relative difference set
Symmetric Design
Hadamard matrix

Hadamard's Determinant Bound

Theorem

Let M be an $n \times n$ matrix with complex entries. Denote by r_i the i^{th} row vector of M. Then

$$\det(M) \leq \prod_{i=1}^{n} \|r_i\|,$$

with equality precisely when the r_i are mutually orthogonal.

Corollary

Let M be as above. Suppose that $\|m_{ij}\| \leq 1$ holds for all $1 \leq i, j \leq n$. Then $\det(M) \leq \sqrt{n}^n = n^{\frac{n}{2}}$.

Hadamard matrices

Matrices meeting Hadamard's bound exist trivially. The character tables of abelian groups give examples for every order n. The problem for real matrices is more interesting.

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 $\det(H) = n^{\frac{n}{2}}$.

H is Hadamard if and only if $HH^\top = nI_n$.
Equivalently, distinct rows of H are orthogonal.

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

- 1867: Sylvester constructed Hadamard matrices of order 2^n.
- 1893: 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, and proposed investigation of when Hadamard matrices exist.
- 1934: 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.

Equivalence, automorphisms of Hadamard matrices

Definition

A ***signed permutation matrix*** is a matrix containing precisely one non-zero entry in each row and column. The non-zero entries are all 1 or -1. Denote by $\mathcal{W}$ the group of all signed permutation matrices, and let H be a Hadamard matrix. Let $\mathcal{W} \times \mathcal{W}$ act on H by $(P, Q) \cdot H = PHQ^{\top}$.

- The ***equivalence class*** of H is the orbit of H under this action.
- The ***automorphism group*** of H, $\mathrm{Aut}(H)$ is the stabiliser.
- $\mathrm{Aut}(H)$ has an induced permutation action on the set $\{r\} \cup \{-r\}$.
- The 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 $\mathcal{A}_H$.

Numerics at small orders

Order	Hadamard matrices	Proportion
2	1	0.25
4	1	7×10^{-4}
8	1	1.3×10^{-13}
12	1	2.5×10^{-30}
16	5	1.1×10^{-53}
20	3	1.0×10^{-85}
24	60	1.2×10^{-124}
28	487	1.3×10^{-173}
32	13,710,027	3.5×10^{-212}
36	$\geq 3 \times 10^{6}$	?

The total number of Hadamard matrices of order 32 is
6326348471771854942942254850540801096975599808403992777086
2019356599724585340056371200000000000000!

Applications of Hadamard matrices

- Design of experiments: designs derived from Hadamard matrices provide constructions of Orthogonal Arrays of strengths 2 and 3.
- Signal Processing: sequences with low autocorrelation are provided by designs with circulant incidence matrices.
- Coding Theory: A class of binary codes derived from the rows of a Hadamard matrix are optimal with respect to the Plotkin bound. A particular family of examples (derived from a $(16, 6, 2)$ design) are linear, and were used in the Mariner 9 missions. Such codes enjoy simple (and extremely fast) encryption and decryption algorithms.
- Quantum Computing: Hadamard matrices arise as unitary operators used for entanglement.

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 (v, k, λ)-***design*** if and only if any pair of elements of V occurs in exactly λ blocks.

Definition

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

Incidence matrices

Definition

Define a function $\phi : V \times B \to \{0, 1\}$ by $\phi(x, b) = 1$ if and only if $x \in b$. An ***incidence matrix*** for Δ is a matrix

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

Lemma

Denote the all 1s matrix of order v by J_v. The $v \times v$ $(0, 1)$-matrix M is the incidence matrix of a 2-(v, k, λ) symmetric design if and only if

$$MM^\top = (k - \lambda)I_v + \lambda J_v$$

Proof.

Entry (i, j) in $MM^\top$ is the inner product of the i^{th} and j^{th} rows of M. This is $|b_i \cap b_j|$. □

A projective plane is an example of a symmetric design with $\lambda = 1$.

Example

Let $\mathbb{F}$ be any field. Then there exists a projective plane over $\mathbb{F}$ derived from a 3-dimensional $\mathbb{F}$-vector space. In the case that $\mathbb{F}$ is a finite field of order q we obtain a geometry with

- $q^2 + q + 1$ points and $q^2 + q + 1$ lines.
- $q + 1$ points on every line and $q + 1$ lines through every point.
- Every pair of points determine a unique line.
- Every pair of lines intersect in a unique point.

Automorphisms of 2-designs

Definition

An ***automorphism*** of a symmetric 2-design Δ is a permutation $\sigma \in \mathrm{Sym}(V)$ which preserves B set-wise. Let M be an incidence matrix for Δ. Then σ corresponds to a pair of permutation matrices such that $PMQ^\top = M$.

The automorphisms of Δ form a **group**, $\mathrm{Aut}(\Delta)$.

Example

Let Δ be a projective plane of order $q+1$. Then $\mathrm{PSL}_2(q) \leq \mathrm{Aut}(\Delta)$.

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, and G also acts regularly on the blocks.
- So all the blocks are translates of one another: every block is of the form bg relative to some fixed base block b.
- So $|b \cap bg| = \lambda$ for any $g \neq 1$. This can be interpreted in light of the multiplicative structure of the group.
- Identifying b with the $\mathbb{Z}G$ element $\hat{b} = \sum_{g \in b} g$, and doing a little algebra we find that $\hat{b}$ satisfies the identity $\hat{b}\hat{b}^{(-1)} = (k - \lambda) + \lambda G$.

Difference sets

Definition

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.

Example

The difference set $\mathcal{D} = \{1, 2, 4\}$ in $\mathbb{Z}_7$ gives rise to a 2-$(7, 3, 1)$ design as follows: we take the group elements as points, and the translates $\mathcal{D} + k$ for $0 \leq k \leq 6$ as blocks.

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

- $MM^\top = (3 - 1)I + J$: M is the incidence matrix of a 2-$(7, 3, 1)$ design.
- In fact this is an incidence matrix for the Fano plane.

Example

Theorem (Singer)

The group $\mathrm{PSL}_n(q)$ *contains a cyclic subgroup acting regularly on the points of projective n-space.*

Corollary

Every desarguesian projective plane is described by a difference set.

- Difference sets in abelian groups are studied using character theory and number theory.
- Many necessary and sufficient conditions for (non-)existence are known.
- Most known constructions for infinite families of Hadamard matrices come from difference sets.

Let H be a normalised Hadamard matrix of order $4t$.

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

Denote by J_{4t-1} the all ones matrix of order $4t-1$. Then $\frac{1}{2}(M + J_{4t-1})$ is a $(0,1)$-matrix.

$$\begin{aligned} MM^\top &= (4t)I_{4t-1} - J_{4t-1} \\ \frac{1}{4}(M + J_{4t-1})(M + J_{4t-1})^\top &= tI_{tn-1} + (t-1)J_{4t-1} \end{aligned}$$

So $\frac{1}{2}(M + J_{4t-1})$ is the incidence matrix of a symmetric $(4t-1, 2t-1, t-1)$ design.

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 $4t$. Difference sets with these parameters are called *Paley-Hadamard*.

- 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

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

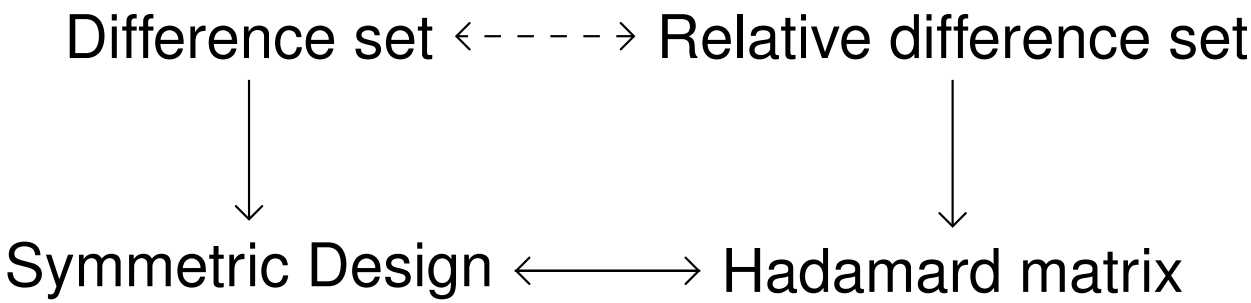
is a Hadamard matrix.

Families of Hadamard difference sets

Difference set	Matrix	$4t$
Singer	Sylvester	2^n
Paley	Paley Type I	$p^\alpha + 1$
Stanton-Sprott	TPP	$p^\alpha q^\beta + 1$, $p^\alpha - q^\beta = 2$
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.

Diagram


Difference set
Relative difference set
Symmetric Design
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

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

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

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

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

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

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?

Recall that any normalised Hadamard matrix has the form

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

where M is a ± 1 version of the incidence matrix of a $(4t-1, 2t-1, t-1)$-design, Δ.
Any automorphism of Δ gives rise to a pair of permutation matrices such that $PMQ^\top = M$. These extend to an automorphism of H:

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

So we obtain an injection $\iota : \mathrm{Aut}(\Delta) \hookrightarrow \mathcal{A}_H$. Furthermore, $\iota(P, Q)$ fixes the first row of H for any $(P, Q) \in \mathrm{Aut}(\Delta)$.

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.

Theorem (Burnside)

Let G be a doubly transitive permutation group. Then G contains a unique minimal normal self-centralising subgroup, N. Either N is elementary abelian, or N is simple.

- In the first case, G is *of affine type*, and $G = N \rtimes H$ where H is quasi-cyclic or a classical group acting naturally.
- In the second case, $G = N \rtimes H$ is almost simple and $H \leq \mathrm{Aut}(N)$ is known.

The groups

Theorem (Kantor, Moorhouse)

If $\mathcal{A}_H$ is affine doubly transitive then $\mathcal{A}_H$ contains $\mathrm{PSL}_n(2)$ and H is a Sylvester matrix.

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.

- $\Gamma \cong \mathrm{M}_{12}$ *acting on* 12 *points.*
- $\mathrm{PSL}_2(p^k) \trianglelefteq \Gamma$ *acting naturally on* $p^k + 1$ *points, for* $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.
- $\Gamma \cong \mathrm{Sp}_6(2)$, *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 $\mathcal{A}_H \cong \mathrm{M}_{12}$. (Hall)
- If $\mathrm{PSL}_2(q) \trianglelefteq \mathcal{A}_H$, then H is the Paley matrix of order $q+1$.
- $\mathrm{Sp}_6(2)$ acts on a unique matrix of order 36. (Computation)

□

The difference sets, I

We classify the $(4t-1, 2t-1, t-1)$ difference sets $\mathcal{D}$ for which the associated Hadamard matrix H is cocyclic.

Theorem (Affine case, Ó C.)

Suppose that H is cocyclic and that $\mathcal{A}_H$ is affine doubly transitive.

- *Then $\mathcal{A}_H$ contains a sharply doubly transitive permutation group.*
- *These have been classified by Zassenhaus. All such groups are contained in $A\Gamma L_1(2^n)$.*
- *So difference sets are in bijective correspondence with conjugacy classes of regular subgroups of $A\Gamma L_1(2^n)$.*
- *Every difference set obtained in this way is contained in a metacyclic group and gives rise to a Sylvester matrix.*

The difference sets, II

Theorem (Non-affine case, Ó C., 2012, JCTA)

Let p be a prime, $k, \alpha \in \mathbb{N}$, and set $n = kp^\alpha$.

- *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.*