Classification of cocyclic Hadamard matrices

Padraig Ó Catháin

NUI Galway

35$^{\text{th}}$ ACCMCC, 5 December 2011

Outline

1. Motivation: Difference sets, group development
2. Hadamard matrices
3. Cocyclic development
4. Classification of cocyclic Hadamard matrices

Motivation: Difference sets

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

A permutation $\sigma \in \mathrm{Sym}(V)$ is an *automorphism* of Δ if and only if $B^\sigma = B$.

- 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.

- Classification of symmetric 2-(v, k, λ) designs occurs in a search space of size approximately 2^{v^2}.
- Classification of (v, k, λ) difference sets occurs in a space of size 2^v.
- **And** we can consider difference sets as group ring elements allowing us to apply methods from representation theory, algebraic number theory, etc.
- A classification of difference sets yields a classification of an algebraically interesting subclass of 2-designs.

Group development

Definition

A *permutation automorphism* of a matrix M is a pair of permutation matrices (P, Q) such that

$$PMQ^\top = M.$$

Theorem

Let M be a matrix with entries in a commutative ring R. The following are equivalent.

- *M contains a subgroup of permutation automorphisms isomorphic to G with induced regular actions on the rows and columns of M.*
- *There exists a labelling of the rows and columns of M with elements of G and a function $\psi : G \to R$ such that*

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

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 $HH^\top = nI_n$.

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

Classification of Hadamard matrices

- Classification for orders ≤ 8 can be achieved by hand.
- Classification for order 12 was achieved by Marshall Hall (using non-trivial results from design theory).
- Orders 16 to 28 required the combined efforts of many mathematicians and substantial computer searches.
- Order 32 is ongoing; massive searches by Orrick, Kharaghani and Tayfeh-Rezaie, and others.

Order	Equivalence Classes
12	1
16	5
20	3
24	60
28	487
32	$> 13 \times 10^6$

Equivalence of Hadamard matrices

Suppose that H is a Hadamard matrix.

- Negations and permutations of rows and columns preserve the Hadamard property.
- Group action of pairs of monomial $\{\pm 1\}$-matrices.
- Orbit: Equivalence class of Hadamard matrices.

$$H \cong H' \Longleftrightarrow H = PH'Q^\top$$

- Stabiliser: Aut(H).

$$\left\{(P, Q) \mid PHQ^\top = H\right\}$$

- Suppose $G \leq \mathrm{PermAut}(H)$ acts regularly on rows and columns of H.
- Then we can identify rows of H with elements of G.
- Columns then correspond to $\mathbb{Z}G$ elements.
- In fact: if ζ is the group ring element associated to one columns, all other columns are associated to group ring elements ζg for $g \in G$.
- Denoting by $* : g \mapsto g^{-1}$, such a ζ satisfies the group ring equation $\zeta\zeta^* = n$ in the group ring.
- Such group ring elements correspond to Menon-Hadamard difference sets.
- But these difference sets necessarily have $v = 4N^2$.

Cocyclic development

A generalisation of group 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 $\psi : G \times G \to \langle -1 \rangle$ and set map $\phi : G \to \langle -1 \rangle$ such that

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

Theorem (De Launey, Flannery & Horadam)

The following statements are equivalent.

- *There is a cocyclic Hadamard matrix over G.*
- *There is a normal relative* $(4t, 2, 4t, 2t)$ *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.*

Definition

Let G be a finite group, with normal subgroup 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.

Lemma (Ó C.)

Let R be a $(4t, 2, 4t, 2t)$-RDS. Then R corresponds to at least one and at most two equivalence classes of cocyclic Hadamard matrices. If there are two equivalence classes, then they are transpose equivalent. Every cocyclic Hadamard matrix corresponds to at least one equivalence class of $(4t, 2, 4t, 2t)$-RDSs.

A procedure to construct all cocyclic Hadamard matrices of order $4t$

1. For each group of order $8t$, construct all $(4t, 2, 4t, 2t)$-RDSs.
2. From each RDS construct a Hadamard matrix and its transpose.
3. Test each new Hadamard matrix for equivalence with each Hadamard matrix previously found.

Step 2 is straightforward. (Linear algebra - milliseconds.)
Step 3: testing equivalence of Hadamard matrices is computationally expensive. We place each matrix in a canonical form, then test for **equality** with all previously found matrices. (For several thousand matrices - minutes.)

Our computations were aided by:

- The Small Groups Library, which contains information on all groups of orders 64 and 72.
- Marc Röder's GAP package, *rds*, which was used to construct the relative difference sets.
- The MAGMA database of Hadamard matrices, and implementation of various algorithms for Hadamard matrices (e.g. computing canonical forms).
- The concept of *coset signatures* which reduced the size of the search.

Theorem (Bruck)

Let G be a group of order mn. Let R be a (m, n, k, λ)-RDS in G, with forbidden subgroup N, of order n. Let U be a normal subgroup of G, and denote by $T = \{g_1, g_2, \ldots, g_{|G:U|}\}$ a transversal of U in G. Furthermore, let $v_i = |R \cap g_i U|$ and $v_{ij} = \left|R \cap g_i g_j U\right|$. Then the following relations hold.

$$\sum_{i\in T} v_i = k \tag{1}$$

$$\sum_{i\in T} v_i^2 = \lambda\left(|U| - |U \cap N|\right) + k \tag{2}$$

$$\sum_{j\in T} v_j v_{ij} = \lambda\left(|U| - |g_i U \cap N|\right) \text{ for } g_i \notin U \tag{3}$$

The computer search

1. Calculate all normal subgroups of order 2, in the group G, of order $8t$.
2. Calculate a system of representatives $\mathcal{N}$ of Aut(G) orbits on the normal subgroups or order 2.
3. Find $U \triangleleft G$ with unique signature of the form $\{i, \ldots, i\}$ (all entries the same).
4. Next, we generate all relative difference sets coset-wise. Initialise with the coset U and the set $P = \{\{1\}\}$ of partial difference sets.
5. Calculate $P' := \bigcup_{p \in P} \{p \subset p' \subset U \mid |p'| = |p| + 1, \text{ and } p' \text{ is pRDS}\}$
6. Calculate a system of representatives P'' of equivalence classes on P'.

Steps 5 and 6 are iterated to get partial difference sets of length i in U.

Results

- Using this algorithm we calculated all $(4t, 2, 4t, 2t)$-RDSs in the groups of order 64 and 72.
- These were then converted into Hadamard matrices and tested for equivalence.
- Since Hadamard matrices are not generally transpose equivalent, the transposes of all surviving matrices were added to the list, and the list was reduced once more.
- 7373 RDSs were found in groups of order 64; these correspond to 100 inequivalent cocyclic Hadamard matrices of order 32.

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	$100/\geq 13\times 10^6$	49/51	261/267
36	$35/\geq 3\times 10^6$	12 /14	21 / 50