The cocyclic Hadamard matrices of order less than 40

Padraig Ó Catháin

National University of Ireland, Galway

Inteernational conference on design theory and applications, 1-3 July 2009

Outline

Introduction

- We completely classify all cocyclic Hadamard matrices of order < 40.
- For orders < 30, all Hadamard matrices have been previously classified.
- So for these orders, an algorithm which determines whether a given Hadamard matrix is cocyclic is sufficient.
- For orders $32, 36$, we use a theorem of de Launey, Flannery and Horadam which relates CHMs to relative difference sets.
- The results of both methods agree for orders < 30.

Introduction

- We completely classify all cocyclic Hadamard matrices of order < 40.
- For orders < 30, all Hadamard matrices have been previously classified.
- So for these orders, an algorithm which determines whether a given Hadamard matrix is cocyclic is sufficient.
- For orders $32, 36$, we use a theorem of de Launey, Flannery and Horadam which relates CHMs to relative difference sets.
- The results of both methods agree for orders < 30.

Cocyclic development

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 $\psi : G \times G \rightarrow \langle -1 \rangle$ such that

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

How do we test whether a given Hadamard matrix is cocyclic?

Determining whether a matrix is cocyclic

Recall the following:

Definition

A $\{\pm 1\}$-matrix M, of order n, is group developed over G, a group of order n, if and only if there exists a set map $\phi : G \rightarrow \langle -1 \rangle$ such that

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

Lemma

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

Definition

Define the expanded matrix of H, E_H, to be:

$$\begin{pmatrix} H & -H \\ -H & H \end{pmatrix}$$

Note that

$$\zeta = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I_n, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes I_n \right)$$

is an automorphism of E_M.

Theorem

Let M be an $n \times n$ matrix with entries in $\langle -1 \rangle$. Let G be a group of order n. Then, M is cocyclic over G if and only if $\mathrm{Aut}\,(M)$ contains as a subgroup a central extension of C_2 by G, which acts regularly on the rows and columns of E_M, and contains ζ.

An algorithm for determining whether a Hadamard matrix is cocyclic

(Recall that ζ is a special automorphism of E_H.)
Input: A Hadamard matrix, H.
Output: All groups, G, over which H is cocyclic.

- Construct E_H.
- Compute PermAut(E_H).
- Determine all regular subgroups, Γ, of PermAut(E_H).
- Return the factor groups $G = \Gamma/\zeta$.

(A generalisation of this algorithm - for non-singular matrices with entries in an abelian group - is implemented in MAGMA.)

Relative difference sets: 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.
- We are interested in difference sets with parameters $(4t, 2, 4t, 2t)$. That is difference sets in groups of order $8t$, relative to a forbidden subgroup of order 2, such that each element of $G - N$ may be expressed as a quotient of elements of the relative difference set in exactly $2t$ different ways.

Relative difference sets: 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.
- We are interested in difference sets with parameters $(4t, 2, 4t, 2t)$. That is difference sets in groups of order $8t$, relative to a forbidden subgroup of order 2, such that each element of $G - N$ may be expressed as a quotient of elements of the relative difference set in exactly $2t$ different ways.

Relation to Hadamard matrices

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.*

Theorem

(Ó C. 2009) 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.*

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.

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 32; these correspond to 100 inequivalent cocyclic Hadamard matrices.

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

Summary

- Cocyclic Hadamard matrices are a subset of Hadamard matrices possessing distinctive algebraic properties.
- They are equivalent to Relative Difference Sets with certain parameters.
- Searching for these RDSs seems computationally easier then searching for CHMs directly, and has allowed us to classify all Hadamard matrices of order at most 40.

Future Work: It should be possible to use a similar method to produce classifications of other classes of designs, e.g. generalised Hadamard matrices.

All data available at: www.maths.nuigalway.ie/∼padraig

Preprint: The cocyclic Hadamard matrices of order less than 40*.*