The Cocyclic Hadamard matrices of order less then 40

Padraig Ó Catháin

National University of Ireland, Galway
Ollscoil na hÉireann, Gaillimh

Introduction

- A ± 1 matrix of order n which satisfies the equation $HH^T = nI_n$ is called a Hadamard matrix.
- Hadamard matrices are used in coding theory, statistics, combinatorial design theory, and many other fields of mathematics.
- Cocyclic Hadamard matrices are Hadamard matrices whose automorphism groups have a subgroup with an almost-regular action.
- A classification of the cocyclic Hadamard matrices of order 36 was begun by Ito in the 1990s.
- In this poster we describe the methods that we used to complete this classification. We also provide a summary of our classification for all smaller orders.

Cocyclic matrices

Let M be an $n \times n$ matrix with entries in an Abelian group A, and let G be a group of order n. Then we say that M is *group developed* over G if there exists a function $\phi : G \to A$ such that $M = [\phi(gh)]_{g,h \in G}$. Equivalently, M is group developed over G if there exists a regular subgroup of $Aut(M)$ isomorphic to G.

Cocyclic development is a generalisation of group development. A cocycle is a map $\psi : G \times G \to A$ that obeys the identity

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

Equivalence classes of cocycles are central objects of study in group cohomology; the cocycles defined above determine central extensions of A by G. The matrix M, is *cocyclic* if there exists a group G, of order n, a cocycle $\psi : G \times G \to A$ and a set map: $\phi : G \to A$ such that

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

A more natural description of cocyclic development is in terms of group development of the expanded matrix of M over an extension of A by G. We define the expanded matrix of M to be the block matrix

$$E_M = [abM]_{a,b \in A}\,.$$

Then, by a result in [2], M is cocyclic developed over G if and only if there exists a group extension of A by G over which E_M is group developed. Thus cocyclic development over a group G is equivalent to the existence of a subgroup of $Aut(M)$, isomorphic to an extension of A by G, which acts regularly on E_M.

Relative Difference sets

Let G be a group of order mn with a normal subgroup N of order n. A subset R of G of size k such that the multiset of quotients $r_1 r_2^{-1},\ r_i \in R, r_1 \neq r_2$ contains each element of $G \backslash N$ exactly λ times and contains no element of N is called a (m,n,k,λ)-Relative Difference Set in G with forbidden subgroup N.

RDSs in non-Abelian groups have received relatively little attention from either group theorists or design theorists. A result of de Launey [3] states that cocyclic Hadamard matrices are equivalent to $(4t, 2, 4t, 2t)$-RDSs. These are relative difference sets of maximal size in groups of order $8t$.

On the relation between RDSs and CHMs

To ensure the correctness of our classification, we need to explicitly describe the relationship between CHMs and HRDSs. We begin by defining an equivalence relation on each of these objects.

Let H be a Hadamard matrix. Then H is equivalent to H' if and only if there exist signed permutation matrices P and Q, such that

$$H = PH'Q^{\top}$$

Let R be a HRDS. Then R is *equivalent* to R', briefly $R \approx R'$, if and only if there exists $g \in G$ and $\vartheta \in AntiAut(G)$ such that

$$R' = R^{\vartheta} g = \{\vartheta(x)\, g \mid x \in R\}\,.$$

Each of these definitions of equivalence is standard in its field. They do not coincide. Every HRDS is equivalent to its complement. The corresponding notion for Hadamard matrices is transpose-equivalence. In [4] we show that an equivalence class of HRDSs generates at least one and at most two equivalence classes of CHMs. If it gives rise to two equivalence classes, then the matrices in one class are precisely the transposes of those in the other.

Results

All Hadamard matrices are known only for orders ≤ 28, see for example, [1]. For these orders we examined the automorphism groups of all matrices for subgroups acting regularly on the expanded matrix. At orders 32 and 36, millions of inequivalent matrices are known, furthermore, not all such matrices have been classified. We generated all HRDSs in the groups of order 64 and 72, and generated all cocyclic Hadamard matrices from these. Up to equivalence, there are 7373 HRDSs in groups of order 64, but only 100 inequivalent cocyclic Hadamard matrices of order 32.

Order	Cocyclic	Indexing Groups	Extension Groups
2	1	1	2
4	1	2	5 / 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	18 / 60	6 / 15	15 / 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

Future Work

This work, of which further details can be found in [4], extends a classification of cocyclic Hadamard matrices begun in the author's Masters Thesis, [2]. We have shown that generating Hadamard matrices using Relative Difference Sets is computationally feasible, at least for small orders. This approach still suffers from exponential complexity, however. An alternative approach is to consider the implications of cocyclic development in the context of Hadamard 3-designs.

[1] E. Spence. Classification of Hadamard matrices of order 24 and 28. Discrete Mathematics, volume 140, pages 185-243, 1995.

[2] P. Ó Catháin. Regular actions on Hadamard matrices. National University of Ireland, Galway, 2008.

[3] W. de Launey, D. Flannery and K. Horadam. Cocyclic Hadamard matrices and difference sets. Discrete Applied Mathematics, volume 102, pages 47-61, 2000.

[4] P. Ó Catháin and M. Röder. The cocyclic Hadamard matrices of order at most 40. In preparation, preprint available at http://www.maths.nuigalway.ie/~padraig

School of Mathematics, Statistics and Applied Mathematics, National University of Ireland, Galway.