Cocyclic-generated Hadamard matrices

Padraig Ó Catháin

National University of Ireland, Galway

PGTC, 2008

Outline

Hadamard matrices

- Hadamard's determinant bound: $|detH| \leq n^{n/2}$
- A ± 1 matrix of order n which satisfies the equation $HH^T = nI_n$ is called a Hadamard matrix
- A necessary condition for the existence of Hadamard matrices is that n be 1, 2, or a multiple of 4
- The Hadamard conjecture states that this condition is sufficient

Hadamard matrices

- Hadamard's determinant bound: $|detH| \leq n^{n/2}$
- A ± 1 matrix of order n which satisfies the equation $HH^T = nI_n$ is called a Hadamard matrix
- A necessary condition for the existence of Hadamard matrices is that n be 1, 2, or a multiple of 4
- The Hadamard conjecture states that this condition is sufficient

Hadamard matrices

- Hadamard's determinant bound: $|detH| \leq n^{n/2}$
- A ± 1 matrix of order n which satisfies the equation $HH^T = nI_n$ is called a Hadamard matrix
- A necessary condition for the existence of Hadamard matrices is that n be 1, 2, or a multiple of 4
- The Hadamard conjecture states that this condition is sufficient

Construction

- Hadamard matrices of all orders less than 668 have been found using a variety of constructions
- Existence of Hadamard matrices at all powers of 2 was proved by Sylvester
- The n^{th} Sylvester Hadamard matrix is $\otimes^n S$ where

$$S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- All Sylvester Hadamard matrices are cocyclic

Group Development

- A Hadamard matrix, H is group developed over a group G if there exists a function $\phi : G \mapsto \langle -1 \rangle$ such that
$$H = (\phi(gh))_{g,h \in G}$$
- Such a Hadamard matrix necessarily has constant row and column sum. We call such a matrix regular

Example: A matrix group developed from C_4

	1	c	c^2	c^3
1	1	c	c^2	c^3
c	c	c^2	c^3	1
c^2	c^2	c^3	1	c
c^3	c^3	1	c	c^2

Let $\phi(1) = \phi(c) = \phi(c^3) = 1$ and $\phi(c^2) = -1$

Example: A matrix group developed from C_4

- Application of this function to the Cayley table of C_4 yields the following Hadamard matrix:

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

- In fact, normalising this matrix (along with some rearrangement of rows) gives us the Sylvester Hadamard matrix of order 4. This matrix is no longer regular

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

Hadamard equivalence

- $H_1 \cong H_2$ only if there exist a pair of signed permutation matrices, (P, Q) such that
$$PH_1Q^T = H_2$$
- Both matrices of order 4 given above are equivalent, and there is only one equivalence class of Hadamard matrices of order 4

Limitations of group development

- Group developed Hadamard matrices exist only at orders $4n^2$
- Development over an arbitrary function $\varphi : G \times G \mapsto \langle -1 \rangle$ is too coarse however
- Cocyclic development provides an interesting solution

Limitations of group development

- Group developed Hadamard matrices exist only at orders $4n^2$
- Development over an arbitrary function $\varphi : G \times G \mapsto \langle -1 \rangle$ is too coarse however
- Cocyclic development provides an interesting solution

Limitations of group development

- Group developed Hadamard matrices exist only at orders $4n^2$
- Development over an arbitrary function $\varphi : G \times G \mapsto \langle -1 \rangle$ is too coarse however
- Cocyclic development provides an interesting solution

Cocycles

- Let G be a finite group, and C a finitely generated Abelian group. A 2-cocycle is a map $\varphi : G \times G \mapsto C$ which satisfies the equation
$$\varphi(g,h)\varphi(gh,k) = \varphi(g,hk)\varphi(h,k) \quad \forall g,h,k \in G$$
- We call a cocycle normalised if for all $g \in G$,
$$\varphi(1,g) = \varphi(g,1) = 1_C$$
- If φ is a normalised cocycle, then $E(\varphi) = \{(g,a) | g \in G, a \in C\}$, with suitably defined multiplication, is a group extension of C by G

Cocycles

- Let G be a finite group, and C a finitely generated Abelian group. A 2-cocycle is a map $\varphi : G \times G \mapsto C$ which satisfies the equation
$$\varphi(g,h)\varphi(gh,k) = \varphi(g,hk)\varphi(h,k) \quad \forall g,h,k \in G$$
- We call a cocycle normalised if for all $g \in G$,
$$\varphi(1,g) = \varphi(g,1) = 1_C$$
- If φ is a normalised cocycle, then $E(\varphi) = \{(g,a)|g \in G, a \in C\}$, with suitably defined multiplication, is a group extension of C by G

Cocyclic Development

- A Hadamard matrix, H, is cocyclic developed if it is Hadamard equivalent to some H' where
$$H' = (\varphi(g,h))_{g,h\in G}$$
- Given a cocycle ϕ that generates a Hadamard matrix, it does not follow a cohomologous cocycle generates an equivalent Hadamard matrix

Cocyclic development

- If we begin with a Hadamard matrix, H, there is an efficient method for determining over which groups, if any, H is cocyclic developed
- An automorphism of a Hadamard matrix, H, is an ordered pair of signed permutation matrices, (P, Q) such that $PHQ^T = H$
- The automorphism group of the matrix is then the group of all automorphisms

Cocyclic development

- If we begin with a Hadamard matrix, H, there is an efficient method for determining over which groups, if any, H is cocyclic developed
- An automorphism of a Hadamard matrix, H, is an ordered pair of signed permutation matrices, (P, Q) such that $PHQ^T = H$
- The automorphism group of the matrix is then the group of all automorphisms

A useful isomorphism

- Let X be a signed permutation matrix. Then there exist unique matrices Y, Z such that $X = Y - Z$
$$\theta(X) = \begin{pmatrix} Y & Z \\ Z & Y \end{pmatrix}$$
- Then $Aut(H) \cong Aut(E_H)$, where E_H is defined by
$$E_H = \begin{pmatrix} H & -H \\ -H & H \end{pmatrix}$$
- E_H is not Hadamard, but it is regular

Cocyclic development

- Theorem: A matrix is cocyclic developed, with cocycle $\varphi : G \times G \rightarrow \langle -1 \rangle$, if and only if its automorphism group has a regular subgroup of order $2n$ isomorphic to $E(\varphi)$, containing a special central involution.
- This subgroup acts regularly on the rows and columns of E_H
- E_H is group developed over $E(\varphi)$
- H is cocyclic developed over G.

Cocyclic development

- Theorem: A matrix is cocyclic developed, with cocycle $\varphi : G \times G \rightarrow \langle -1 \rangle$, if and only if its automorphism group has a regular subgroup of order $2n$ isomorphic to $E(\varphi)$, containing a special central involution.
- This subgroup acts regularly on the rows and columns of E_H
- E_H is group developed over $E(\varphi)$
- H is cocyclic developed over G.

Cocyclic development

- Theorem: A matrix is cocyclic developed, with cocycle $\varphi : G \times G \rightarrow \langle -1 \rangle$, if and only if its automorphism group has a regular subgroup of order $2n$ isomorphic to $E(\varphi)$, containing a special central involution.
- This subgroup acts regularly on the rows and columns of E_H
- E_H is group developed over $E(\varphi)$
- H is cocyclic developed over G.

Results

The automorphism group of the Hadamard matrix of order 12 is of order 190,080. In fact it is the Schur cover of M_{12}. It has three regular subgroups, given below.

Indexing Group	Extension Group
$C_2 \times C_6$	$Q_8 \times C_3$
$Alt(4)$	$Q_8 \rtimes C_3$
D_6	$C_3 \rtimes Q_8$

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	18 / 60	6 / 15	15 / 52
28	6 / 487	2 / 4	2 / 13

Goethals-Seidel Construction

- Many construction techniques can be proven to always generate cocyclic Hadamard matrices
- It was unknown whether the construction of Goethals and Seidel was of this type
- We found two inequivalent Goethals-Seidel Hadamard matrices of order 28
- They had automorphism groups of order 24 and 48

Goethals-Seidel Construction

- Many construction techniques can be proven to always generate cocyclic Hadamard matrices
- It was unknown whether the construction of Goethals and Seidel was of this type
- We found two inequivalent Goethals-Seidel Hadamard matrices of order 28
- They had automorphism groups of order 24 and 48

Summary

- Hadamard matrices may be developed from cocycles
- All matrices of order at most 20 have this property

- Outlook
  - The cocyclic Hadamard conjecture:
    Does a cocyclic Hadamard matrix exist for all orders $4n$?