Cocyclic matrices

Padraig Ó Catháin

National University of Ireland, Galway

September, 2008

Outline

- Let M be an $n \times n$ matrix with entries in a set A, and let G be a group of order n
- M is group developed over G if there exists a function $\phi : G \to A$ such that
$$H = [\phi(gh)]_{g,h \in G}$$
- Each row of M contains at most n different entries, and every row and column is a permutation of the first row

Example: A matrix group developed from C_4

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

	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

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

Determining group development

- Group development is a property of matrices only up to permutation equivalence.
- Matrices are group developed if and only if the rows and columns may be permuted transitively, leaving the entries of the matrix unchanged.
- Formally: There exists a permutation subgroup of the automorphism group that acts regularly on the matrix.

Cocycles

- Let G be a group and A be an Abelian group. $\psi : G \times G \to C$ is a cocycle if

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

- Cocycles can be used to describe central extensions of A by G.
- The canonical extension given by ψ is $E(\psi) = \{(g,a)\,|g \in G, a \in A\}$ with multiplication given by:

$$(g,a)(h,b) = (gh, ab\psi(g,h))$$

- It can be verified that this is a group precisely when the cocycle ψ is normalised. That is $\psi(1,1) = 1$.

Cocycles

- Let G be a group and A be an Abelian group. $\psi : G \times G \to C$ is a cocycle if

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

- Cocycles can be used to describe central extensions of A by G.
- The canonical extension given by ψ is $E(\psi) = \{(g,a)\,|g \in G, a \in A\}$ with multiplication given by:

$$(g,a)(h,b) = (gh, ab\psi(g,h))$$

- It can be verified that this is a group precisely when the cocycle ψ is normalised. That is $\psi(1,1) = 1$.

Cocyclic development

- Group development is a generalisation of cocyclic development.
- Let M be an $n \times n$ matrix with entries in an Abelian group, A, and let G be a group of order n.
- M is cocyclic over G if and only if there exists a cocycle $\psi : G \times G \to A$ such that

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

- Cocyclic development is a property of matrices up to A-equivalence. That is multiplying rows and/or columns by elements of A as well as permuting them.

Cocyclic development

- Group development is a generalisation of cocyclic development.
- Let M be an $n \times n$ matrix with entries in an Abelian group, A, and let G be a group of order n.
- M is cocyclic over G if and only if there exists a cocycle $\psi : G \times G \rightarrow A$ such that

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

- Cocyclic development is a property of matrices up to A-equivalence. That is multiplying rows and/or columns by elements of A as well as permuting them.

Relation to group development

- Suppose that M is cocyclic over G.
- Define E_M as follows:

$$E_M = \begin{pmatrix} a_1Ma_1 & a_1Ma_2 & \dots & a_1Ma_n \\ a_2Ma_1 & a_2Ma_2 & \dots & a_2Ms_n \\ \vdots & \vdots & \ddots & \vdots \\ a_nMa_1 & a_nMa_2 & \dots & a_nMa_n \end{pmatrix} = \left[a_ia_j\right] \otimes M$$

- Theorem: E_M is group developed over the canonical extension of A by G given by ψ.

Hadamard matrices

- A Hadamard matrix is a square $\{\pm 1\}$-matrix of order n with determinant $n^{n/2}$.
- Equivalently, a Hadamard matrix is one that has the property
$$HH^T = nI_n$$
- Hadamard showed that they only exist when n is a multiple of 4.
- He conjectured that a Hadamard matrix of order $4n$ exists for all $n \in \mathbb{N}$.
- The smallest order for which existence is open is 668.

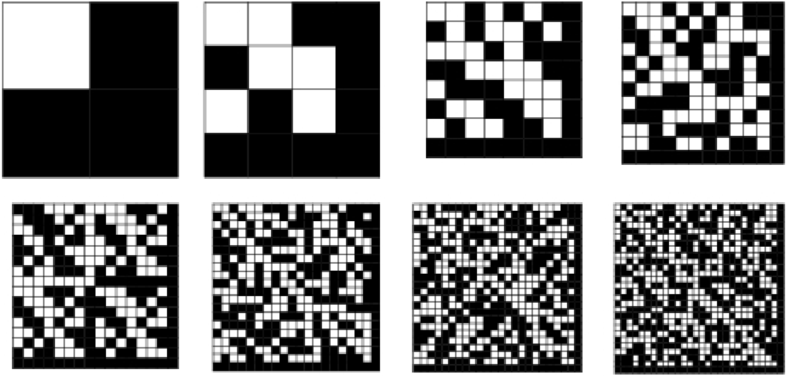

Figure: Anallagmatic pavements of small order

Hadamard matrix constructions

- Sylvester Hadamard matrices occur at orders 2^n for $n \in \mathbb{N}$.

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

- Given a Hadamard Relative Difference Set in a group of order $8n$ a Hadamard matrix of order $4n$ may be derived.
- The Paley construction generates such HRDSs from finite fields. If p^a is a prime power $\cong 3 \ mod \ 4$ there exists a Hadamard matrix of order $p^a + 1$, while if $p^a \cong 1 \ mod \ 4$, there exists a Hadamard of order $2\left(p^a + 1\right)$.

The automorphism group of a Hadamard matrix

- Two $\{\pm 1\}$-matrices, H and H', are Hadamard equivalent if and only if there exist monomial $\{\pm 1\}$-matrices, P and Q such that
$$A = PBQ^\top$$
- Formally, H and H' lie in the same orbit under the action of $\mathrm{Mon}\,(n, \{\pm 1\}) \times \mathrm{Mon}\,(n, \{\pm 1\})$.
- The automorphism group of a Hadamard matrix is its stabiliser under this action.
- So (P, Q) is an automorphism of H if
$$PHQ^\top = H$$

The automorphism group of a Hadamard matrix

- Two $\{\pm 1\}$-matrices, H and H', are Hadamard equivalent if and only if there exist monomial $\{\pm 1\}$-matrices, P and Q such that
$$A = PBQ^{\top}$$
- Formally, H and H' lie in the same orbit under the action of $\mathtt{Mon}\,(n, \{\pm 1\}) \times \mathtt{Mon}\,(n, \{\pm 1\})$.
- The automorphism group of a Hadamard matrix is its stabiliser under this action.
- So (P, Q) is an automorphism of H if
$$PHQ^{\top} = H$$

The automorphism group of a Hadamard matrix

- Two $\{\pm 1\}$-matrices, H and H', are Hadamard equivalent if and only if there exist monomial $\{\pm 1\}$-matrices, P and Q such that
$$A = PBQ^{\top}$$
- Formally, H and H' lie in the same orbit under the action of $\mathtt{Mon}\,(n, \{\pm 1\}) \times \mathtt{Mon}\,(n, \{\pm 1\})$.
- The automorphism group of a Hadamard matrix is its stabiliser under this action.
- So (P, Q) is an automorphism of H if
$$PHQ^{\top} = H$$

Limitations of group development

- Regular Hadamard matrices have constant row and column sums.
- Regular Hadamard matrices exist only at orders $4n^2$.
- Let H be an s-regular Hadamard matrix of order n and let J be the matrix consisting entirely of $+1$ entries. Then:

$$\begin{aligned} JH = JH^\top &= sJ \\ nJ &= JHH^\top \\ &= sJH^\top \\ &= s^2 J \\ n &= s^2 \end{aligned}$$

- Thus group developed Hadamard matrices occur only at square orders.

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. Cocycles do not even preserve invertibility.

A useful isomorphism

- Recall our definition of the expanded matrix. For a Hadamard matrix, H, it is defined to be

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

- Let X be a monomial $\{\pm 1\}$-matrix. Then there exist unique matrices Y, Z such that $X = Y - Z$. Define

$$\theta(X) = \begin{pmatrix} Y & Z \\ Z & Y \end{pmatrix}$$

- Then if $(P, Q) \in \mathtt{Aut}(H)$, $(\theta(P), \theta(Q)) \in \mathtt{Aut}(E_H)$
- E_H is not Hadamard, but it does have constant row and column sums.

Cocyclic development

- So by our earlier theorem, H is cocyclic developed if and only if E_H is group developed.
- We calculate the automorphism group of the expanded matrix of a Hadamard matrix, and search for regular subgroups containing the central subgroup $\langle -1 \rangle$
- We factor out by this central involution to find out over which groups H is cocyclic
- We could extract the cocycle from the extension group if we wanted to

Sample 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 Groups
$C_2^2 \times C_3$	$Q_8 \times C_3$
$Alt(4)$	$SL(2,3)$
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

Current work

- We are attempting to construct all cocyclic Hadamard matrices of order ≤ 50.
- We use a result by de Launey which states that: there is a cocyclic Hadamard matrix over G if and only if there is a normal relative $(4t, 2, 4t, 2t)$ difference set in a central extension of $\langle -1 \rangle$ by G, relative to $\langle -1 \rangle$.
- At the moment we search for all RDSs in the groups of order 64, and the generate Hadamard matrices of order 32 from these.

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 $4n$?