The Paley Matrices and their Automorphism Groups.

Richard M. Stafford

[1] National Security Agency

2nd International Conference on Hadamard, cocyclic matrices, and applications. National University of Ireland, Galway July 1-3, 2009

Overview

Let $q = p^m$ where p is an odd prime.

- The Paley matrices consist of the conference matrix, C, of order $q+1$, and two classes of Hadamard matrices:
- The type I Hadamard matrix, H_1, of order $q+1$ where $q \equiv 3 (\text{ mod } 4)$.
- The type II Hadamard matrix, H_2, of order $2(q+1)$ where $q \equiv 1 (\text{ mod } 4)$
- These matrices comprise the densest known classes of conference and Hadamard matrices.
- Moreover, they have a very rich algebraic structure. In particular, they are cocyclic.
- This talk is a summary of my results with Warwick de Launey on this topic.

Goal

- Yesterday, Dane discussed the following problems:
- Problem 1: If W is group developed describe all ways in which W can be group developed.
- Problem 2 : Classify all ways in which a given matrix, W is cocyclic.
- Cocyclic development of a weighing matrix, W, is related to regular group actions on its associated design, A_W. Thus solving problem 1 for the associated design A_W, solves problem 2 for W.
- For each Paley matrix we completly classify the regular actions on its associated design.

W is a $(0,\pm 1)$ Marix.

- pair of monomial matrices (P, Q) is an automorphism of W iff
$$PWQ^T = W.$$
- PermAut$(E) = \{(P, Q) \in Aut(W)\}$ with P and Q permutation matrices.
- Expanded design: $E_W = \begin{bmatrix} W & -W \\ -W & W \end{bmatrix}$.
- The design, A_w associated with W is obtained from E_W by replacing all -1 entries of E_W with 0 .

Theorem: Let W be a weighing matrix and C be a balanced weighing matrix, then

- Aut$(W) \cong$ PermAut(E_W), Aut$(C) \cong$ Aut(E_C) , A_C, E_C can be
- indexed so that groups PermAut(E_W), Aut(E_C) are identical.
- Moving a row in C corresponds to moving a pair of rows in E_C.
- negation of a row in C corresponds to interchanging corresponding rows in E_C.

Finite near fields

- Let F be a set, $(F,+,\cdot)$ *is a left near field if* $(F,+)$ *is an abelian group,* $(F^*,\cdot)$ *is a group, and* $a(b+c)=ab+ac$.
- Multiplication on the left induces a regular action on F^*.
- $q=p^m$, p odd prime p. $F_2=\mathrm{GF}(q^2)$, $F_1=$ subfield of order q.
- V is F_2 viewed as a 2-dimensional vector space over F_1. For $x,y\in V$ define $\sigma(x,y)=(x^p,y^p)$ and GL(V) be the group of linear maps on V
- Define GΓL(V) to be the group generated by GL(V) and σ.
- Suppose $R\subset$ GΓL(V) acts regularly on V^*, for each $x\in V^*\exists r_x\in R$ with $x^{r_x}=1$, if you define $\cdot$ on V^* by the equation

$$a\cdot b=b^{r_a^{-1}}=1^{(r_ar_b)^{-1}}$$

- then $(V,+,\cdot)$ is a near field and $(V^*,\cdot)\cong R$.
- There are three infinite families of Dickson near fields and seven exceptional near fields of orders $5^2,7^2,11^2,23^2,29^2$ or 59^2.

The Paley Matrices

- Let F_1, F_2, V, $\mathrm{G\Gamma L}(V)$, σ be defined as on the previous slide.
- $\{u, v\}$ be a basis and let $x = (x_1, x_2)$, $y = (y_1, y_2)$ and define $A_{xy} = \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}$.
- Define $\det(x, y) = |A_{x,y}|$. Let $\infty = (0, 1)$, and $a_+ = (1, a)$.
- $S = \{\infty\} \cup \{a_+ | a \in F_1\}$, $\chi =$ the quadratic character on F_1.
- The the Paley conference matrix $C = [\chi(\det(x, y))]_{xy \in S}$.
- The Paley Type I Hadamard matrix $H = I_q + C$.
- The Paley Type II Hadamard matrix $H_2 = \begin{bmatrix} I + C & -I + C \\ -I + C & -I - C \end{bmatrix}$.

Our results on the conference matrix

- The general linear group, $\mathrm{GL}(2,q)$ together with $\sigma(x,y)=(x^p,y^p)$ act on C. This action is not faithful, its kernel $K=\{\lambda^2 I_{q+1}|\lambda\in \mathrm{GF}(q)\}$.
- $\mathrm{Aut}(C)\cong <\mathrm{GL}(2,q),\sigma>$.
- The subgroups which act regularly on A_C, are in $1-1$ correspondence with the regular subgroups of $<\mathrm{GL}(2,q),\sigma>$ which contain Q.
- Let E be a regular subgroup of, $<\mathrm{GL}(2,q),\sigma>$ then C is cocyclic over E/L with extension group E/Q if and only $L\subset R$.
- We carried out our Agenda on all near fields of order q^2. Determining which ones give regular actions on E_C.
- Five of the exceptional near fields regular actions on A_C.
- This gives a complete classification of the regular actions on A_C.

An example

Example

The exceptional near field of order 59^2.

- It has a nonsolvable multiplication $\cong \mathrm{SL}(2,5) \times \mathbb{Z}_{29}$. A sample embedding R is generated by the matrices
$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 9 & 15 \\ -10 & -10 \end{bmatrix} \quad \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$$
- The group $R' = R/Q \cong \mathrm{SL}(2,5)$ and has a normal $RDS(120,59,59,2)$.
- $R'/Z(R') \cong \mathrm{Alt}(5)$ with extension group equal to $\mathrm{SL}(2,5)$.
- Thus the Paley conference matrix of order 60 is cocyclic over $\mathrm{Alt}(5)$ with extension group $\mathrm{SL}(2,5)$.

Our results on the type I Hadamard matrix, H_1.

- Let $\mathrm{GS}(V)$ be the set of linear maps, A, such that $\chi(|A|) = 1$.
- $A \in \mathrm{GS}(V)$ if and only if the determinate of A is a square.
- $< \mathrm{GS}(V), \sigma >$ *acts* on H_1. The kernel of the action is Q.
- for $q > 11$ $\mathrm{Aut}(H_1) \cong < \mathrm{GS}(V), \sigma > /Q$ (Bill Kantor 1969).
- $q = 11$, $\mathrm{Aut}(H_1)/Z(\mathrm{Aut}(H_1)) \cong M_{12}$. (Marshall Hall 1962).
- The subgroups which act regularly on A_{H_1}, are in $1-1$ correspondence with the regular subgroups of $< \mathrm{GS}(2, q), \sigma >$ which contain Q.
- Let E be a regular subgroup of , $< \mathrm{GS}(2, q), \sigma >$ then H_1 is cocyclic over E/L with extension group E/Q if and only $L \subset R$.
- We carried out our agenda on all near fields of order q^2. Determining which ones give regular actions on A_{H_1}. We found no new regular actions.
- This classifies all the regular actions on A_{H_1} for $q > 11$.

Our results on H_1 continued.

- $q \neq 3, 7, 11, 23$, or 59, the generalized quaternion group of order $2(q+1)$ is the only abstract group which acts regularly on A_{H_1}.
- $q = 3, 7$, and 11 the group $\mathrm{Aut}(H_1)$ is some what larger due to the fact that H_1 is equivalent to other classical constructions.
- $\mathrm{Aut}(A_{H_1})$ has regular subgroups that do not come from near fields.
- $q = 3$ all noncyclic groups of order 8 act regularly. Of these all but the dihedral group act normally, that is they induce cocyclic development of H_1.
- $q = 7$ all 14 groups of order 16 except the cyclic and dihedral act normally.
- $q = 11$ the group $Q_8 \times \mathbb{Z}_3$ acts normally.
- This completes the classification of the regular actions on A_{H_1}.

Our results on the Hadamard matrix of type II, H_2.

- $\mathrm{Aut}(H_2)$ contains a subgroup, Π of index 2 isomorphic to $< \mathrm{GL}(2,q), \sigma >$.
- $\mathrm{Aut}(H_2)$ contains an extra element, ξ, of order 4. $\xi^2 = (-I_{2(q+1),} - I_{2(q+1)})$ and $< \xi >$ is a normal subgroup.

$$\mathrm{Aut}(H_2) =< \Pi, \xi >. \ |\mathrm{Aut}(H_2)| = 4m(q+1)q(q-1).$$

- The action of Π on the first $q+1$ rows of H_2 is permutation isomorphic to the action of $\mathrm{Aut}(C)$ on the rows of the conference matrix.
- If E acts regularly on rows of A_{H_2}, then the subgroup, R, of E which fixes the first $q+1$ rows of H_2 acts regularly on rows A_C and is of index 2 in E.
- Thus R comes from a near field and so we can use our previous knowledge to determine the regular actions on A_C.

Our results on H_2 continued.

- We determined a representative for each conjugacy class of regular subgroups of A_{H_2}.
- All our regular actions are new.
- This gives a complete classification of the regular actions on A_{H_2}.

Here is an interesting comparison.

Fact

The Paley type I Hadamard matrix has just one conjugacy class of regular subgroups.

Corollary

The number of distinct conjugacy classes of regular subgroups of the Paley type II Hadamard matrix of order $2(q+1)$ is unbounded as q grows.

An application

- Since there is just one Hadamard matrix of order 12,
- H_1, $q = 11$ is equivalent to H_2, $q = 5$.
- Since there are many cases where H_1 and H_2 have the same order it is natural to ask whether there are any other equivalent type I and type II matrices.

Corollary

Paley's type I is equivalent to Paley's type II iff it has order 12.

Proof.

if $q > 5$, $\mathrm{Aut}(H_2)$ has a normal subgroup of order 4. If $q > 11$, $\mathrm{Aut}(H_1)$ does not. □

Objectives for the rest of talk

I would like to cover the following:

1. Our proof that $\mathrm{Aut}(C) \cong < \mathrm{GL}(2,q)/Q, \sigma >$ is elementary and uses a pretty result on finite fields due to Carliz so I would like to give a brief sketch of that proof.
2. Our proof that $\mathrm{Aut}(H_2) \cong < \mathrm{GL}(2,q)/Q, \sigma, \xi >$

- is a proof by contradiction that divides into five parts.

The five parts

1. An argument that $\mathrm{GL}(2,q)$, and σ induce automorphisms of H_2 plus ξ exists.
2. A counting argument that shows that the induced action of $\mathrm{Aut}(H_2)$ on the $2(q+1)$ rows of H_2 has order less than $\frac{2(q+2)}{2}!$.
3. A proof that the kernel of this action is $< (-I_{2(q+1)}, -I_{2q(+1)})$.
4. A proof that if $|\mathrm{Aut}(H_2)| > 4m(q+1)q(q-1)$ then $\mathrm{Aut}(H_2)$ induces a 2-transitive action on the rows of H_2
5. A case by case argument based on the classification of the doubly transitive permutation groups that shows that $\mathrm{Aut}(H_2)$ cannot be doubly transitive unless it contains $\mathrm{Alt}(2(q+1)$.

- I think my most important objective is try and convince you how useful a tool the classification of the 2-transitive groups are. So I want to sketch how we eliminated a few of the "small" doubly transitive actions.

- I believe our counting argument is general and novel and so I would like to give you an outline of that.

- A first step in our proof which is the first step in both Hall's and Kantor's proof is to exhibit a large group of automorphisms. So I would like to show you that $\mathrm{GL}(2, q)$ and ξ act on H_2.

If $|\mathrm{Aut}(H_2)| > 2m(q+1)q(q-1)$ then $\mathrm{Aut}(H_2)$ is 2-transitive.

- We assume for each $A \in \mathrm{GL}(2,q)$, there are to two monomial matrices, π_A and ψ_A such that $\pi_A H_2 \psi_A^T = H_2$. Set $\kappa = (\pi_A, \psi_a)$. The map $\Theta(A) = \kappa$ defines a homomorphism from $\mathrm{GL}(2,q) \rightarrow \mathrm{Aut}(H_2)$ with kernel Q.
- If $\chi(|A|) = 1$ then κ fixes each quadrant of H_2.
- If $\chi(|A|) = -1$ then κ fixes as a set the first and last $q+1$ rows of H_2.
- Set $\Lambda = \Theta(\mathrm{GL}(2,q))$ then the action Λ on the first $q+1$ rows is permutation isomorphic to $\mathrm{PGL}(2,q)$ in its triply transitive action on the projective line.
- Set E,O be the first and last $q+1$ rows of H_2 and let $\alpha \in \mathrm{E}$ then Λ_α has 2 orbits on E and two on O each of lengths $1, q$, thus $\mathrm{Aut}(H_2)_\alpha$ has at most 4 orbits.

$\mathrm{Aut}(H_2)$ is not a small 2-transitive group.

We assume all other steps in the proof have been done.

We assume $\mathrm{Aut}(H_2)$ induces a 2-transitive group, Γ, on the $2(q+1)$ rows of H_2.

Some basic facts about 2-transitive groups:

1. If G is $2-$ transitive then G has a unique normal subgroup, $\mathrm{soc}(G)$.
2. The unique normal subgroup is transitive.
3. If $\mathrm{soc}(G)$ abelian then $\mathrm{soc}(G)$ regular p-subgroup.

Lemma

The socle of Γ is nonabelian

Proof.

Suppose $\mathrm{soc}(\Gamma')$ is abelian, then by part 3, $2(q+1) = p^d$, hence $p = 2$. Since $q \equiv 1 (\mathrm{mod}\ 4)$, $d = 2$. □

$\mathrm{Aut}(H_2)$ is not a small 2-transitive group continued.

- A unital is a $2-(s^3+1, s+1, 1)$ BIBD. There are two unitals with doubly transitive automorphism groups. In both cases s is of prime power order.
- As a final example we eliminate both these cases.
- Suppose $s > 3$ and B be a block of the design. So $|B| \geq 4$ and since ξ interchanges E and O, we can assume $B \cap \mathrm{E} \geq 2$. Let $\alpha, \beta, \in B \cap \mathrm{E}$. Since Λ is transitive on $\mathrm{E} - \{\alpha\}$, $\mathrm{E} \subset B$. Since $2(q+1) = s^3+1$, we have $2(s+1) \geq s^3+1$ which can not happen when $s \geq 3$.

A bound on the order of Aut(H_2)

- The matrix $B = [\chi(y-x)]_{x,y \in F_1}$, is called the core of C.
- $BJ_q = 0$ and $B^T B = BB^T = qI_q - J_q$, J_q all ones matrix.

$D =$ top half of H_2. Index rows and columns of D as shown below.

	∞_+	0_+	1_+	$\ldots$	$(q-1)_+$	∞_-	0_-	1_-	$\ldots$	$(q-1)_-$
∞	1	1	1	.....	1	$-$	1	1	.....	1
0	1					1				
$\vdots$	$\vdots$			$I+B$		$\vdots$			$-I+B$	
$q-1$	1					1				

- We assume kernel of $\Pi =< \zeta >$ and $\mathrm{soc}(\Gamma') \cong \mathrm{Alt}(2(q+1)$.
- Then Γ has a subgroup, $\Gamma(E)$, that fixes the E pointwise and $\Theta(\Gamma(E)) \cong \mathrm{Sym}(q+1)$.

A bound on the order of Aut(H_2) continued

- Let M be the matrix whose columns comprise of all pointwise products of distinct columns of D and set $M' = \begin{bmatrix} M & -M \end{bmatrix}$.
- Let $\kappa \in \Gamma(\mathrm{E})$ and apply the row operations prescribed by α on the pointwise product of 2 columns of D then we obtained a column or a negation of a column of M'. Define $s(a, b)$ to be the pointwise product of a, and b.
- Thus Aut(D) embeds into Aut($(M \mid -M)$). now choose $a \neq 0$.
- Observe that a_+ is orthogonal to ∞_- therefore $s(a_+, \infty_-)$ has $\frac{q+1}{2}$ ones and $\frac{q+1}{2}$ minus's.
- Since $\Theta(\Gamma(\mathrm{E}))$ is $q+1$ transitive on rows, the action of $\Gamma(\mathrm{E})$ on rows of D produces $\binom{q+1}{\frac{q+1}{2}}$ distinct columns in M'.
- But M' has at most $2(q+1)(2q+1)$columns. Thus $\binom{q+1}{\frac{q+1}{2}} \leq 2(q+1)(2q+1)$.

Automorphism of the conference matrix

- Define $\pi_A(x) = Ax, \phi_A(x) = |A|AX$.
- $\det(\pi(x), \phi(y)) = \det(Ax, |A|Ay) = |A|^2 \det(x, y)$.
- Recall $\infty = (0,1), a_+ = (1, a)$, $a \in F_1$, $S = \{\infty, a_+ | x \in F_1\}$,
- and $C = [\det(\chi(x,y)]_{xy \in S}$, the above shows $(\pi, \phi) \in \mathrm{Aut}(C)$.
- So $\mathrm{GL}(2,q)$ acts on C. Recall $\sigma(x,y) = (x^p, y^p)$.
- $\det(\sigma(x), \sigma(y)) = \det(x^p, y^p) = \det(x,y)^p$. Since p odd, $\sigma \in \mathrm{Aut}(C)$.
- $\mathrm{Aut}(C)$ contains a subgroup $\Pi \cong < \mathrm{GL}(2,q), \sigma >$. $\chi(\det(x_+, y_+)) = \chi(y - x)$.

Theorem

$G = \mathrm{Aut}(A_C) \cong \mathrm{Aut}(C) \cong \mathrm{G\Gamma L}(2,q)/Q$.

Sketch of Proof

$$C = \begin{array}{c} \\ \infty \\ \infty \\ 0_+ \\ \vdots \\ \infty \end{array} \begin{array}{cccc} \infty & 0_+ & \cdots & (q-1)_+ \\ 0 & -1 & \cdots & -1 \\ 1 & & & \\ \vdots & & [\chi(y-x)]_{x,y\in F_1} & \\ 1 & & & \end{array}$$

- $G\Gamma L(2,q) \subseteq G$ act's 3-transitively on the rows of C. That is the subgroup which fixes 2 rows is transitive on the remaining rows.
- An automorphism of C must permute the zero entries of C.
- Thus G must fix the main diagonal. This implies that
- If $\phi \in G$ fixes the ith row of C then ϕ fixes the ith column.
- P and Q induce the same permutation, ϕ on $\{0,\cdots,(q-1)\}$.

$\mathrm{Aut}(C) \cong G\Gamma\mathrm{L}(2,q)/Q$

- Suffices to show $G_{\infty,0_+,1_+}$ has order $2m$, where $q = p^m$.
- Let $\psi = (P,Q) \in G_{\infty,0_+,1_+}$. Since ψ fixes the main diagonal,
- Thus $\psi = (P,Q) \in G_{\infty,0_+,1_+}$ if and only if $\phi(0) = 0$, $\phi(1) = 0$

$$\chi(\phi(y) - \phi(x)) = \chi(y - x).$$

- An old result of Carlitz implies $\phi(x) = x^{p^k}$. Thus
- the permutation group induced by action of G on rows has order

$$m(q+1)q(q-1).$$

- The Kernel, K, of this action fixes all rows and columns of C.
- Thus $\kappa \in K \Rightarrow \kappa$ just negates some of the rows and columns of C. This implies $K = \mathbb{Z}_2$.

Automorphisms of H_2.

- For $q = 3 \pmod 4$, $H_1 = I + C$, since $C^T = -C$,
- $H_1 H_1^T = (q+1)H_1$. In this case $H_1 = [h(x,y)]_{x,y \in S}$ where

$$h(x,y) = \begin{cases} \chi(\frac{x}{y}) & ,\text{if} \frac{x}{y} \in \mathrm{GF}(q) \\ \chi(\det(x,y)) & \text{if} \frac{x}{y} \notin \mathrm{GF}(q). \end{cases}$$

- If x and y linearly dependent, $A \in \mathrm{GL}(2,q)$, then

$$h(\pi(x), \phi(y)) = \begin{cases} 1 & \text{if } \chi(|A|) = 1 \\ -1 & \text{if } \chi(|A|) = -1 \end{cases}$$

- $(\pi, \phi) : (I + C) \longrightarrow -I + C$, thus
- $(\pi_A, \varphi_A) \in \mathrm{Aut}(H_1)$ iff $\chi(Det(A)) = 1$.
- $H_2 = \begin{bmatrix} I + C & -I + C \\ -I + C & -I - C \end{bmatrix}$

Automorphisms of $\Gamma = \mathrm{Aut}(H_2)$ continued.

- $A \in \mathrm{GL}(2,q)$ and apply $\kappa_A \in (\pi_A, \phi_A)$ to each quadrant of H_2
- if $\chi(|A|) = 1$, κ_A fixes each quadrant of H_2 and so $\kappa_A \in \Gamma$.
- $\chi(|A|) = -1$, $\kappa_A : \pm(I + C) \to \mp I \pm C$. Thus
- $\kappa_A : \begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix} \to \begin{bmatrix} -I+C & I+C \\ I+C & I-C \end{bmatrix}$ but
- $H_2 = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} -I+C & I+C \\ I+C & I-C \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}$ and so A induces
- an automorphism ι_A that moves the quadrants of H_2.
- Notice ι_A fixes as a set the first $q+1$ rows of H_2
- We obtain an embedding Λ of $\mathrm{G\Gamma L}(2,q)/Q$ in Γ.
- We call the first $q+1$ rows of H_2 the even points, $\mathscr{E}$,
- the last $q+1$ rows the odd points, $\mathscr{O}$ and $\mathscr{G} = \mathscr{E} \cup \mathscr{O}$.

Another automorphism.

$$E_{H_2} = \begin{bmatrix} H_2 & -H_2 \\ -H_2 & H_2 \end{bmatrix} = \begin{bmatrix} I+C & -I+C & -I-C & I-C \\ -I+C & -I-C & I-C & I+C \\ -I-C & I-C & I+C & -I+C \\ I-C & I+C & -I+C & -I-C \end{bmatrix}.$$

- E_{H_2} can be developed by cyclically shifting the first column or the first row.
- $P = \begin{bmatrix} 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \end{bmatrix}$, $Q = P^T$, $PE_{H_2}Q^T = E_{H_2}$, $\xi = (P, Q)$.
- $P^2 = Q^2 = \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \end{bmatrix}$ so ξ^2 interchanges each row and each column of E_{H_2} with its negation. Thus $\xi^2 = \zeta$.

Some Subgroups

- $\Pi =< \Lambda, \xi >$, $\xi^2 = \zeta$, $\xi^\sigma = \xi$, and
- $A \in \mathrm{GL}(2,q)$, $\xi^A = \xi^{\chi(|A|)}$. Λ, $< \xi >$ are normal in Π.
- $\omega \in \Gamma$ induces a permutation $\Theta(\omega)$ on the rows of H_2.
- $\Gamma' = \Theta(\Gamma)$, $\Pi' = \Theta(\Pi)$, $\Lambda' = \Theta(\Lambda)$, $K =$ kernel of Θ.
- Π' acts transitively on the rows of H_2.
- Λ' induces a 3-transitive subgroup of Sym(E).
- $\omega \in \Lambda'$ induces the same permutation on O as it does on $\mathscr{E}$.
- Λ'_ω has 4 orbits on the rows of H_2 of lengths $1, 1, q, q$.

References

- W. de Launey, R. M. Stafford, *On cocyclic matrices and the regular group actions of certain Paley matrices*, Discrete Applied Mathematics, 102 (2000) 63-101.
- W. de Launey, R. M. Stafford, *On the automorphisms of Paley's type II Hadamard matrix*, Discrete Mathematics 308 (2008) 2910-2924
- W. de Launey and R. M. Stafford, *The regular subgroups of the Paley type II Hadamard matrix*,, preprint.