National University of Ireland, Galway
Ollscoil na hÉireann, Gaillimh

Skew Hadamard Difference Sets

Padraig Ó Catháin

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.
- Most known infinite families of Hadamard matrices come from difference sets.
- We use results on 2-transitive groups to describe the automorphism groups of these matrices under the assumption that the automorphism group is transitive.
- In the process, we discover a new triply infinite family of skew-Hadamard difference sets.

Difference sets

Let G be a group of order v, and let $\mathcal{D}$ be a subset of G of cardinality k. We say that $\mathcal{D}$ is a (v, k, λ)-*difference set* if every non-identity element of G may be expressed in exactly λ ways as a quotient of elements of $\mathcal{D}$. Let $\chi_{\mathcal{D}}$ denote the characteristic function of $\mathcal{D}$. Then the *development* of $\mathcal{D}$ is the matrix

$$Dev(\mathcal{D}) = [\chi_{\mathcal{D}}(gh)]_{g,h\in G}.$$

We call a difference set with parameters $(4n-1, 2n-1, n-1)$ a *Hadamard difference set* as it gives rise to a Hadamard matrix in a natural way.

Lemma 1. *Let $\mathcal{D}$ be a $(4n-1, 2n-1, n-1)$-difference set. Define D to be $2\,\mathrm{Dev}\,(\mathcal{D}) - J$, and $\overline{1}$ to be the all 1s vector of length $4n-1$. Then*

$$H = \begin{pmatrix} 1 & \overline{1} \\ \overline{1}^\top & D \end{pmatrix}$$

is Hadamard. Furthermore, $\mathrm{PermAut}(H)$ *is isomorphic to* $\mathrm{Aut}(\mathcal{D})$.

Several infinite families of Hadamard difference sets are known, see for example [1].

Two-transitive groups

Let G be a group acting on a set X. We say that the action of G is 2-transitive if for any four distinct elements $w, x, y, z \in X$ there exists $g \in G$ such that $wg = y$ and $xg = z$ both hold.

Lemma 2. *If H is a Hadamard matrix arising from a difference set, then* $\mathrm{Aut}(H)$ *is transitive if and only if it is 2-transitive.*

Now, deep results in group theory yield a complete classification of the finite 2-transitive groups. Furthermore Ito classifies the groups which act doubly transitively on a Hadamard matrix. Building on his work we obtain the following theorem.

Theorem 3. *Let $\Gamma \leq \mathrm{Aut}(H)$ be a doubly transitive permutation group acting on the set of rows of a Hadamard matrix, H. Then one of the following holds:*

- $\Gamma \cong M_{12}$ *and H is the unique Hadamard matrix of order* 12.
- $PSL_2(p^k) \trianglelefteq \Gamma$, *acting naturally on $p^k + 1$ points, for $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$ and H is a Paley type I matrix.*
- $\Gamma \cong Sp_6(2)$, *and H is unique and of order* 36.
- Γ *contains a regular elementary abelian subgroup, and H is a Sylvester matrix of order* 2^n.

Regular subgroups of $A\Gamma L(1, q)$

Suppose that H is a Hadamard matrix arising from a difference set, and that $\mathrm{Aut}(H)$ is transitive, so that Theorem 3 applies. We wish to find all difference sets that occur in the non-affine case.
Now by Theorem 3, there are two sporadic cases, which we consider first.

Lemma 4. *Suppose that H is a Hadamard matrix of order* 12*, then it is developed from a difference set in $\mathbb{Z}/11\mathbb{Z}$ given by $\{1, 3, 4, 5, 9\}$. If $\mathrm{Aut}(H) \cong Sp_6(2)$, then H is not developed from any difference set.*

Proof. For the first part, we apply the multiplier theorems for cyclic difference sets. For the second, we observe that this action of $Sp_6(2)$ has point stabiliser isomorphic to S_8, acting on 35 points. But S_8 has no subgroups of order 35 so there are no regular subgroups in this action. □

This leaves for consideration only the Paley Hadamard matrices.

Theorem 5 (Kantor)**.** *Let H be a Paley Hadamard matrix of order > 12. Then* $\mathrm{Aut}(H) \cong P\Sigma L(2, q)$.

Now a difference set corresponding to one of these matrices is contained in a regular subgroup of the stabiliser of a point of the automorphism group of H. This group is isomorphic to $A\Gamma L(1, q)$ in its natural action on the field of size q, considered as an extension over its prime subfield.

Theorem 6 (Ó C. 2011)**.** *Let p be a prime, and $n = kp^\alpha \in \mathbb{N}$.*

- *Define*

$$G_{p,k,\alpha} = \left\langle a_1, \ldots, a_n, b \mid a_i^p = 1, [a_i, a_j] = 1, b^{p^\alpha} = 1, a_i^b = a_{i+k} \right\rangle.$$

- *The subgroups*

$$R_e = \left\langle a_1 b^{p^e}, a_2 b^{p^e} \ldots a_n b^{p^e} \right\rangle$$

for $0 \leq e \leq \alpha$ contain skew Hadamard difference sets.

- *Each difference set gives rise to a Paley Hadamard matrix.*
- *These are the only non-affine difference sets which give rise to Hadamard matrices in which* $\mathrm{Aut}(H)$ *is transitive.*

A new family of skew Hadamard difference sets

Definition 1. *Let D be a difference set in a group G, and let $D^{(-1)} = \left\{d^{-1} \mid d \in D\right\}$. Then D is skew if $G = D \cup D^{(-1)} \cup \{1_G\}$. If D is skew then D has Hadamard parameters.*

The set of quadratic residues in $\mathbb{F}_q$ forms a Hadamard difference set in $(\mathbb{F}_q, +)$ whenever $q \equiv 3 \mod 4$. These are called the Paley difference sets. It is well known that -1 is not a quadratic residue in $\mathbb{F}_q$, so that precisely one of x and $-x$ is a residue. It follows that the Paley differnce sets are skew. For many years these were the only known examples of skew Hadamard difference sets, and it was conjectured that there were no others.
This conjecture was disproved in 2005 by Ding and Yuan, who constructed new difference sets in groups of order 3^5 and 3^7 using Dickson polynomials. Numerous papers outlining new constructions have followed in the past few years. All known examples have been in groups of orders 3^n or q^3.

Lemma 7 (Ó C. 2011)**.** *The difference sets in Theorem 5 are all skew.*

These difference sets provide examples of skew Hadamard difference sets at infinitely many new orders.

[1] T. Beth, D. Jungnickel, H. Lenz Design Theory, Vol. 1. Cambridge, 1999.
[2] N. Ito Hadamard matrices with doubly transitive automorphism groups. *Arch. Math. (Basel), 35*:100-111, 1980.
[3] P. Ó Catháin Cocyclic development, Paley Hadamard matrices and skew difference sets. *in preparation.*

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