Difference sets and doubly transitive actions on Hadamard matrices

Padraig Ó Catháin [*]

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

February 27, 2012

Abstract

Non-affine groups acting doubly transitively on a Hadamard matrix have been classified by Ito. Implicit in this work is a list of Hadamard matrices with non-affine doubly transitive automorphism group. We give this list explicitly, in the process settling an old research problem of Ito and Leon.

We then use our classification to show that the only cocyclic Hadamard matrices developed from a difference set with non-affine automorphism group are those that arise from the Paley Hadamard matrices.

If H is a cocyclic Hadamard matrix developed from a difference set then the automorphism group of H is doubly transitive. We classify all difference sets which give rise to Hadamard matrices with non-affine doubly transitive automorphism group. A key component of this is a complete list of difference sets corresponding to the Paley Hadamard matrices. As part of our classification we uncover a new triply infinite family of skew-Hadamard difference sets. To our knowledge, these are the first skew-Hadamard difference sets to be discovered in non-abelian p-groups with no exponent restriction.

As one more application of our main classification, we show that Hall's sextic residue difference sets give rise to precisely one cocyclic Hadamard matrix.

[*] *E-mail: p.ocathain1@nuigalway.ie*

1 Introduction

In [27], we showed that Hadamard matrices developed from twin prime power difference sets are not cocyclic. In this paper we generalise that result to all 'non-affine' $(4n-1, 2n-1, n-1)$-difference sets. We call a $(4n-1, 2n-1, n-1)$-difference set *affine* if the automorphism group of the corresponding Hadamard matrix has a normal elementary abelian subgroup acting regularly on the rows of the matrix. All necessary concepts will be introduced in Sections 2 and 3. In this paper, we address the following problems:

- We extend work of Ito to give a classification of Hadamard matrices with non-affine doubly transitive automorphism groups.
- We observe that the classification solves an old problem of Ito and Leon from [18].
- For each matrix in the classification we determine all associated difference sets. In the process we uncover a previously unknown triply infinite family of skew difference sets. This is a step towards the solution of a research problem of Jungnickel posed in [19].

In order to discuss this paper's concerns in more detail, we recall some elementary definitions and concepts.

Definition 1. We say that Hadamard matrices H and $\overline{H}$ are *(Hadamard) equivalent* if there exist $\{\pm 1\}$-monomial matrices P and Q such that $PHQ^\top = \overline{H}$. The *automorphism group* of H, $\mathrm{Aut}(H)$, consists of all pairs (P, Q) of $\{\pm 1\}$-monomial matrices satisfying $PHQ^\top = H$. An important subgroup of $\mathrm{Aut}(H)$ is $\mathrm{PermAut}(H)$, which consists of the (P, Q) such that P and Q are permutation matrices.

We deal with Hadamard matrices up to equivalence. That is, any claims of uniqueness, classification etc. are made only up to equivalence.

The following will allow us to apply deep results from the theory of permutation groups to the study of $\mathrm{Aut}(H)$.

Definition 2. Let X be a $\{\pm 1\}$-monomial matrix of order n. Then X has a unique factorization $D_X E_X$ where D_X is a diagonal matrix and E_X is a permutation matrix. For a Hadamard matrix H, and $(P, Q) \in \mathrm{Aut}(H)$, define $\nu(P, Q) = E_P$.

So each automorphism (P, Q) of a Hadamard matrix H induces a permutation of the rows of H. That is, ν is a homomorphism and gives a permutation representation of $\mathrm{Aut}(H)$ in the symmetric group on the rows of H. For ease of notation, we will refer to $\mathcal{A}(H) = \nu(\mathrm{Aut}(H))$ as a permutation group on $\{1, 2, \ldots, n\}$ where i represents the i^{th} row of H. We use standard permutation group terminology for $\mathcal{A}(H)$. Henceforth, when $\mathcal{A}(H)$ has a permutation group property, we will say that $\mathrm{Aut}(H)$ has this property.

The literature on Hadamard matrices bears witness to extensive interest in the study of various group actions on Hadamard matrices. Among these results is the correspondence between $(4n-1, 2n-1, n-1)$-difference sets and regular actions on the rows and columns of the cores of Hadamard matrices (as in Section 2). Another correspondence associates $(4n, 2, 4n, 2n)$-relative difference sets to certain induced regular actions of subgroups of $\mathrm{Aut}(H)$ on the rows and columns of H. Hadamard matrices supporting this latter type of action are called *cocyclic*. In this paper we deal almost entirely with the permutation action of $\mathcal{A}(H)$ on the rows of H, which is not the standard action considered in the study of cocyclic Hadamard matrices.

Definition 3. Let G be a finite group. A binary *(2-)cocycle* is a map $\psi : G \times G \to \langle -1 \rangle$ which obeys the following identity for all $g, h, k \in G$.

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

An $n \times n$ Hadamard matrix H is *cocyclic* if there exists a group G of order n and a cocycle $\psi : G \times G \to \langle -1 \rangle$ such that

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

where rows and columns of H are indexed by the elements of G. We say that *ψ is a cocycle of H*, that H is *cocyclic over G*, and that the extension of $\langle -1 \rangle$ by G determined by ψ is an *extension group of H*.

Cocyclic Hadamard matrices possess a rich algebraic theory. For basic results, we refer the reader to [14, 25, 6]. The only result on cocyclic Hadamard matrices which will be used in later sections is that $\mathcal{A}(H)$ is transitive if H is cocyclic (see Lemma 6 of [27]). A study of Hadamard matrices supporting the structure of both a $(4n, 2, 4n, 2n)$-relative difference set and a $(4n-1, 2n-1, n-1)$-difference set was the original motivation of this work.

An outline of the rest of the paper follows. We begin Section 2 by recalling some further necessary definitions and results from the study of Hadamard matrices and symmetric 2-designs. In Section 3 we classify the Hadamard matrices H with $\mathcal{A}(H)$ non-affine doubly transitive. Then in the following sections we will consider in turn cocyclic development for the matrices in our classification, and difference sets associated with the matrices in the classification. We conclude the paper with two applications of the classification result of Section 3: we show that the Hadamard matrices developed from Hall's sextic residue difference sets are cocyclic in only one case, and we describe a new family of skew-Hadamard difference sets. These are the only skew difference sets giving rise to cocyclic Hadamard matrices.

2 Hadamard matrices and related combinatorial structures

We recall now the relationships between Hadamard matrices, symmetric designs and difference sets. Some of the material in this section is standard.

Definition 4. Let $V = \{p_1, p_2, \ldots, p_v\}$ be a set of *points* and let $B = \{b_1, b_2, \ldots, b_v\}$ be a set of subsets of V (*blocks*) such that the following hold:

- $|b_i| = k, \quad 1 \leq i \leq v$
- $|b_i \cap b_j| = \lambda, \quad 1 \leq i < j \leq v.$

Then $\mathcal{S} = (V, B)$ is a *symmetric* 2-(v, k, λ) *design.* Define $\chi : V \times B \to \{0, 1\}$ by $\chi(p_i, b_j) = 1$ if and only if $p_i \in b_j$. An *incidence matrix* $\mathcal{M}$ *of* $\mathcal{S}$ has entry $\chi(p_i, b_j)$ in its i^{th} row and j^{th} column. That is,

$$\mathcal{M} = [\chi(p_i, b_j)]_{1 \leq i,j \leq v} .$$

Definition 5. Let $\mathcal{S} = (V, B)$ be a symmetric 2-(v, k, λ) design, and let G be the symmetric group on V. Then G has an induced action on the k-subsets of V. The setwise stabiliser of B is the *automorphism group* of $\mathcal{S}$, $\mathrm{Aut}(\mathcal{S})$. Any symmetric 2-design of the form $\overline{\mathcal{S}} = (V, B^g)$ for some $g \in G$ is *equivalent to* $\mathcal{S}$.

Let $\mathcal{M}$ be an incidence matrix of $\mathcal{S}$. Define $\mathrm{Aut}(\mathcal{M})$ to be the set of all pairs (P, Q) of permutation matrices such that $P\mathcal{M}Q^\top = \mathcal{M}$. It is easily seen that $\mathrm{Aut}(\mathcal{M})$ and $\mathrm{Aut}(\mathcal{S})$ are isomorphic.

We will rely on the following result, which relates the action of $\mathrm{Aut}(\mathcal{S})$ on points to its action on blocks.

Theorem 6 (Theorem III.4.1, [2])**.** *Let $\mathcal{S}$ be a non-trivial symmetric design, and let $G \leq \mathrm{Aut}(\mathcal{S})$. Then the number of orbits of G on points is equal to the number of orbits of G on blocks.*

The following lemma is standard; see e.g. Lemma I.9.3 of [2].

Lemma 7. *Let $\mathcal{S}$ be a symmetric 2-$(4n-1, 2n-1, n-1)$ design. Define J to be the $(4n-1) \times (4n-1)$ all 1s matrix, and T to be $2\mathcal{M} - J$. Let $\overline{1}$ be the all 1s vector of length $4n-1$. Then*

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

is a Hadamard matrix.

Proof. First, we observe that $\mathcal{M}\mathcal{M}^\top = nI + (n-1)J$. It follows that

$$\begin{aligned} TT^\top &= (2\mathcal{M} - J)(2\mathcal{M}^\top - J) \\ &= 4\mathcal{M}\mathcal{M}^\top - 2\mathcal{M}J - 2J\mathcal{M}^\top + J^2 \\ &= 4(nI + (n-1)J) - (4n-2)J - (4n-2)J + (4n-1)J \\ &= 4nI - J. \end{aligned}$$

Thus, adding an initial row and column of +1s to T gives a Hadamard matrix. □

Remark 8. So a Hadamard matrix of order $4n$ exists if a symmetric 2-$(4n-1, 2n-1, n-1)$ design exists. The converse is also true: one obtains an incidence matrix for a symmetric 2-$(4n-1, 2n-1, n-1)$ design from the core of a normalised Hadamard matrix by replacing every occurrence of -1 by 0. Notice that the equivalence class of a symmetric 2-$(4n-1, 2n-1, n-1)$ design corresponds to a unique equivalence class of Hadamard matrices via the construction of Lemma 7. But the equivalence operations for 2-designs are finer than those for Hadamard matrices. So a single equivalence class of Hadamard matrices can give rise to many inequivalent 2-designs.

In the next few results we work towards a description of $\mathrm{Aut}(\mathcal{S})$ as a subgroup of $\mathcal{A}(H)$.

Lemma 9. *Let H be a Hadamard matrix. Then $\nu(\mathrm{PermAut}(H)) \cong \mathrm{PermAut}(H)$.*

Proof. Note that $\mathrm{Ker}(\nu)$ consists of automorphisms of H which are diagonal in the first component. But a diagonal permutation matrix is trivial; hence $\mathrm{Ker}(\nu) \cap \mathrm{PermAut}(H) = 1$. The lemma follows. □

Doubly transitive actions on Hadamard matrices are a central concern of this paper. We recall Burnside's Theorem (see e.g. Theorem XI.7.12 of [15]): a doubly transitive permutation group is either of affine type and contains an elementary abelian normal subgroup acting regularly, or it is almost simple. We restrict our classification results to the non-affine case. The affine case requires methods different to those developed here and falls outside the scope of this paper. The non-affine doubly transitive groups which act on Hadamard matrices have been completely classified by Ito up to permutation isomorphism.

Theorem 10 (Ito, [16])**.** *Let H be a Hadamard matrix such that $\mathcal{A}(H)$ is non-affine and doubly transitive. Then the action of $\mathcal{A}(H)$ is one of the following.*

- *$\mathcal{A}(H) \cong \mathrm{M}_{12}$ in its natural action on 12 points.*
- *$\mathrm{PSL}_2(p^k) \trianglelefteq \mathcal{A}(H)$ acting naturally on $p^k + 1$ points, for $p^k \equiv 3 \mod 4$, $p^k \neq 3, 11$.*
- *$\mathcal{A}(H) \cong \mathrm{Sp}_6(2)$ acting on 36 points.*

Now we can state our main result about the relationship between actions on designs and actions on corresponding Hadamard matrices.

Theorem 11. *Let $\mathcal{S}$ be a symmetric 2-$(4n-1, 2n-1, n-1)$ design, and let H be the Hadamard matrix constructed from $\mathcal{S}$ as in Lemma 7. Then $\mathrm{Aut}(\mathcal{S}) \cong \mathrm{PermAut}(H)$.*

Suppose that $\mathrm{Aut}(\mathcal{S})$ is transitive on the points of $\mathcal{S}$, and denote by G the subgroup $\nu(\mathrm{PermAut}(H))$ of $\mathcal{A}(H)$. Then G is transitive on $\{2, \ldots, 4n\}$ and exactly one of the following holds.

- *G is the full stabiliser of a point in $\mathcal{A}(H)$.*
- *H is Sylvester.*

- *H is of order* 12.

Proof. We extend $(P, Q) \in \mathrm{Aut}(\mathcal{S})$ to an automorphism

$$\left(\begin{pmatrix} 1 & \overline{0} \\ \overline{0}^\top & P \end{pmatrix}, \begin{pmatrix} 1 & \overline{0} \\ \overline{0}^\top & Q \end{pmatrix} \right)$$

of H, which fixes the first row and column and acts as (P, Q) on the submatrix T. Thus $\mathrm{Aut}(\mathcal{S})$ embeds in $\mathrm{PermAut}(H)$. In the other direction: $(P, Q) \in \mathrm{PermAut}(H)$ must fix the unique first row and first column of 1s, and hence restricts to an automorphism of $\mathcal{S}$. So $\mathrm{PermAut}(H) \cong \mathrm{Aut}(\mathcal{S})$.

It is clear that every element of $G \leq \mathcal{A}(H)$ fixes the first row of H. Now suppose that $\mathrm{Aut}(\mathcal{S})$ is transitive on the points of $\mathcal{S}$. Then by Lemma 9 and the above, G is transitive on the remaining rows of H. We show that either G is the full stabiliser $\mathcal{A}(H)_1$ of 1, or H is Sylvester or of order 12.

First, we define the group

$$K = \langle E_Q \mid (P, Q) \in \mathrm{Aut}(H) \text{ and } \nu(P, Q) \in \mathcal{A}(H)_1 \rangle.$$

Clearly K contains a subgroup isomorphic to $\mathrm{PermAut}(H)$ which fixes the first column. By Theorem 6, this group is transitive on the remaining columns. So K is either intransitive, or doubly transitive on columns. From the definition we see that K is a covering group of $\mathcal{A}(H)_1$.

If K is intransitive, then for every automorphism (P, Q) of H such that $\nu(P, Q)$ is in $\mathcal{A}(H)_1$, E_Q fixes the first column of H. Thus either (P, Q) or $(-P, -Q) \in \mathrm{PermAut}(H)$. This implies that $G = \mathcal{A}(H)_1$.

Now let K be doubly transitive. Suppose that K is almost simple. But then $K \leq \mathcal{A}(H^\top)$ is doubly transitive on the rows of a Hadamard matrix and Theorem 10 applies. We consider each case in turn. The point stabiliser of $\mathrm{P\Sigma L}_2(q)$ is a subgroup of $\mathrm{A\Gamma L}_1(q)$, which cannot have a transitive action on $q + 1$ points. So this case does not yield an example. The point stabiliser of $\mathrm{Sp}_6(2)$ is S_8, but S_8 has no doubly transitive permutation representation on 36 points. Finally, the stabiliser of a point in M_{12} is M_{11}, which has an induced 3-transitive action on 12 points. It can be verified that this is indeed the action of K on the columns of the Hadamard matrix of order 12. Hence $\mathrm{Aut}(\mathcal{S}) \cong \mathrm{PSL}_2(11)$ in this case, which is of index 144 in M_{12}.

Now suppose that K is an affine group acting doubly transitively on the rows of $H^\top$, and the kernel of ν contains $\mathrm{soc}(K)$, which is regular on columns. Then $\mathrm{soc}(K)$ is a transitive translation group (in the sense of [21]) on the 3-design of $H^\top$, and hence $H^\top \sim H$ is a Sylvester Hadamard matrix by Theorem 8 of [21]. □

Difference sets are also naturally related to symmetric 2-designs.

Definition 12. Let G be a group of order v, and let $\mathcal{D}$ be a k-subset of G. Suppose that every non-trivial element of G may be represented in the form $d_i d_j^{-1}$ in exactly λ different ways, for $d_i, d_j \in \mathcal{D}$. Then $\mathcal{D}$ is a (v, k, λ)-*difference set* in G. Two difference sets $\mathcal{D}$ and $\overline{\mathcal{D}}$ in G are *equivalent* if $\mathcal{D} = g\overline{\mathcal{D}}^\sigma$ for some $g \in G$ and $\sigma \in \mathrm{Aut}(G)$.

Theorem 13. *Suppose G contains a (v,k,λ)-difference set $\mathcal{D}$. Then there exists a symmetric 2-(v,k,λ) design on which G acts regularly. Conversely, a symmetric 2-(v,k,λ) design on which G acts regularly corresponds to a (v,k,λ)-difference set in G.*

Proof. Set $V = \{g \mid g \in G\}$ and $B = \{\mathcal{D}g \mid g \in G\}$. Then $\mathcal{S} = (V, B)$ is a symmetric 2-(v,k,λ) design. The right regular action of G on V gives an embedding of G into $\mathrm{Aut}(\mathcal{S})$ as a regular subgroup.

In the other direction, suppose that $\mathcal{S}$ is a symmetric 2-(v,k,λ) design with $G \leq \mathrm{Aut}(\mathcal{S})$ acting regularly. Identify the points of $\mathcal{S}$ with the elements of G. Blocks of $\mathcal{S}$ become subsets of G. By Theorem 6, G acts regularly on blocks. Then one finds that all blocks are of the form $b_0 g^{-1}$ for some fixed block b_0. But $\left|b_0 g^{-1} \cap b_0 h^{-1}\right| = \lambda$ for arbitrary $g, h \in G$, $g \neq h^{-1}$ implies that $x_i x_j^{-1} = h^{-1}g$ has precisely λ solutions with $x_i, x_j \in b_0$. So b_0 is a (v,k,λ)-difference set in G as required. □

Remark 14. If $\mathcal{S}_1$ and $\mathcal{S}_2$ are equivalent designs and G acts regularly on $\mathcal{S}_1$, then G acts regularly on $\mathcal{S}_2$. Furthermore, any difference set in G obtained from $\mathcal{S}_1$ via the construction of Theorem 13 is equivalent to a difference set obtained in the same way from $\mathcal{S}_2$. Conversely, equivalent difference sets give rise to equivalent symmetric designs via the construction of Theorem 13.

Note that $\mathrm{Aut}(\mathcal{S})$ can contain many conjugacy classes of regular subgroups which are isomorphic as abstract groups. Let R_i $(i = 1, 2)$ be regular subgroups of $\mathrm{Aut}(\mathcal{S})$, and let $\mathcal{D}_i$ be the difference set in R_i constructed as in the proof of Theorem 13. If R_1 and R_2 are $\mathrm{Aut}(\mathcal{S})$-conjugate, then there is an isomorphism $\alpha : R_1 \rightarrow R_2$ such that $\alpha(\mathcal{D}_1)$ is equivalent to $\mathcal{D}_2$. Conversely, if R_1 and R_2 are isomorphic but not $\mathrm{Aut}(\mathcal{S})$-conjugate, then there need not be such an isomorphism α.

Definition 15. Let H be a Hadamard matrix, $\mathcal{D}$ a difference set and $\mathcal{S}$ a symmetric design. If $\mathcal{D}$ and $\mathcal{S}$ are related as in Theorem 13, then we say that $\mathcal{S}$ underlies $\mathcal{D}$, or that $\mathcal{D}$ is over $\mathcal{S}$. If H is a Hadamard matrix related to $\mathcal{S}$ as in Lemma 7, then we say that H is developed from $\mathcal{S}$, or that $\mathcal{S}$ corresponds to H. We use the same terminology for the relationship between $\mathcal{D}$ and H as for $\mathcal{S}$ and H.

So by Lemma 9, (the first part of) Theorem 11, and Theorem 13, we see that a $(4n-1, 2n-1, n-1)$-difference set in a group G corresponds in a natural way to a Hadamard matrix H such that G is isomorphic to a subgroup of $\mathcal{A}(H)_1$ acting regularly on $\{2, \ldots, 4n\}$. For this reason, a difference set with parameters $(4n-1, 2n-1, n-1)$ is called *Hadamard.*

3 Hadamard matrices with doubly transitive automorphism groups

The relevance of doubly transitive permutation groups to the subject matter of this paper is further exemplified by the following lemma.

Theorem 16 (Cf. [27], Lemma 11)**.** *Let H be a Hadamard matrix developed from a $(4n-1, 2n-1, n-1)$-difference set as in Lemma 7 and Theorem 13. Then $\mathcal{A}(H)$ is transitive if and only if $\mathcal{A}(H)$ is doubly transitive.*

Proof. By Lemma 7 and Theorem 13, $\mathrm{PermAut}(H)$ fixes the first row and column of H, and acts transitively on the remaining rows. So by Lemma 9, $\mathcal{A}(H)_1$ is transitive on $\{2, \ldots, 4n\}$. Thus if $\mathcal{A}(H)$ is transitive, then it is 2-transitive. □

In light of Theorem 10, it is not difficult to list all Hadamard matrices H with $\mathcal{A}(H)$ non-affine doubly transitive. We do so in the remainder of this section.

Lemma 17 (M. Hall, [10])**.** *All Hadamard matrices of order* 12 *are (Hadamard) equivalent, and for any such matrix H, $\mathcal{A}(H) \cong \mathrm{M}_{12}$ acting sharply* 5*-transitively.*

The action of $\mathrm{Sp}_6(2)$ in Theorem 10 is not its natural action on a 6-dimensional $\mathbb{F}_2$-vector space; rather the stabiliser of a point is a maximal subgroup isomorphic to S_8. This is the only action of $\mathrm{Sp}_6(2)$ that we will consider. In this action, S_8 acts primitively on the 35 remaining points. In [18], Ito and Leon construct a Hadamard matrix H of order 36 with $\mathcal{A}(H) \cong \mathrm{Sp}_6(2)$, and conjecture that it is the unique such Hadamard matrix. We now observe that this is the case.

Theorem 18. *Suppose that H is a Hadamard matrix with $\mathcal{A}(H) \cong \mathrm{Sp}_6(2)$ in its doubly transitive action on* 36 *points. Then H is unique (up to Hadamard equivalence).*

Proof. By Lemma 1 of [17], $\mathrm{Ker}(\nu)$ has order 2. Thus $|\mathrm{Aut}(H)| = 2 \cdot |\mathrm{Sp}_6(2)| = 2,903,040$. Now see Tables 8 and 9 of [4], where an exhaustive computer search shows that there is a unique Hadamard matrix of order 36 with automorphism group of order $2,903,040$. □

Remark 19. Alternatively, we may argue as follows. It may be verified, for a Hadamard matrix H of order n, that $|\mathcal{A}(H)_1 : \nu(\mathrm{PermAut}(H))|$ divides n. So the automorphism group of a symmetric 2-$(35, 17, 8)$ design corresponding to H will have index dividing 36 in S_8. Theorem 2 of [5] states that there are four symmetric 2-$(35, 17, 8)$ designs with automorphisms of order 7. One of these has S_8 as its automorphism group; the others have automorphism groups of order at most 420. By Remark 8, this gives another proof of the uniqueness of H.

This resolves the two sporadic cases of Ito. We consider now the case that $\mathrm{PSL}_2(p^k)$ acts on the rows of H.

Definition 20. Let $q \equiv 3 \mod 4$ be a prime power. Then the quadratic residues of $\mathbb{F}_q$ form a difference set in the additive group of $\mathbb{F}_q$. Such a difference set is known as a *Paley difference set.* A *Paley design* is the underlying symmetric 2-design of a Paley difference set, and a *Paley Hadamard matrix* is a Hadamard matrix developed from a Paley difference set (these are generally known as Type I Paley matrices.)

The Paley matrices are well studied. In particular, their automorphism groups were determined by Kantor.

Theorem 21 ([20], [7]). *Let H be a Paley Hadamard matrix of order $p^n + 1 > 12$. Then $\mathrm{Aut}(H)$ is an extension of C_2 by $\mathrm{P\Sigma L}_2(p^n)$ (that is, $\mathrm{PSL}_2(p^n)$ extended by field automorphisms).*

Definition 22. Let $q = p^n$ for a prime p. Then $\mathrm{A\Gamma L}_1(q)$ is the group of semilinear transformations of $\mathbb{F}_q$; that is, transformations of the type $x \mapsto ax^\sigma + b$ for $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, where we consider $\mathbb{F}_q$ as a field extension of $\mathbb{F}_p$. The group $\mathrm{AGL}_1(q)$ is a normal subgroup of $\mathrm{A\Gamma L}_1(q)$, consisting of the transformations of the form $x \mapsto ax + b$.

Theorem 23. *Let H be a normalised Hadamard matrix of order $q + 1$, for a prime power $q \equiv 3 \mod 4$, $q > 11$. Then $\mathrm{PSL}_2(q)$ in its natural doubly transitive action is a normal subgroup of $\mathcal{A}(H)$ if and only if H is equivalent to a Paley Hadamard matrix.*

Proof. Suppose that $\mathrm{PSL}_2(q)$ is a normal subgroup of $\mathcal{A}(H)$. Then the stabiliser of a point in $\mathcal{A}(H)$ contains a subgroup of index 2 in $\mathrm{AGL}_1(q)$. This contains a normal elementary abelian subgroup R of order q acting regularly on the remaining points. It is clear that R fixes a point in its action on columns. Hence, R is a regular subgroup of $\mathrm{Aut}(\mathcal{S})$, where $\mathcal{S}$ is a symmetric design corresponding to H. Thus by Theorem 13, H is developed from a difference set $\mathcal{D}$ in R. We show that $\mathcal{D}$ is necessarily of Paley type: this guarantees that H is equivalent to a Paley Hadamard matrix by Remarks 8 and 14.

Consider $\mathcal{A}(H)_{1,2}$, the stabiliser of a point in $\mathcal{A}(H)_1$. This has two orbits on the remaining rows, one labelled by quadratic residues and one by non-residues. By Bruck's characterisation of the multipliers of a difference set ([2], Definition VI.2.1), we have that the quadratic residues are multipliers of $\mathcal{D}$. Now, by Lemma VI.2.5 of [2], there exists a translate of $\mathcal{D}$ fixed by every multiplier. This translate either consists entirely of quadratic residues or of quadratic non-residues. In either case $\mathcal{D}$ is equivalent to a Paley difference set.

Conversely, by Theorem 21, if H is of order $q+1 > 12$, and H is equivalent to a Paley Hadamard matrix, it is clear by Theorem 21 that $\mathrm{PSL}_2(q) \trianglelefteq \mathcal{A}(H)$. □

The previous results yield the following classification.

Corollary 24. *H is a Hadamard matrix such that $\mathcal{A}(H)$ is non-affine doubly transitive if and only if one of the following holds.*

- *H is of order 12.*
- *H is in the unique equivalence class of Hadamard matrices of order 36 on which $\mathrm{Sp}_6(2)$ acts.*
- *H has order greater than 12 and is equivalent to a Paley Hadamard matrix.*

Remark 25. The (Paley) Hadamard matrices of order less than 12 are excluded from the list of Corollary 24 because their automorphism groups are affine doubly transitive rather than non-affine. Indeed, these matrices are equivalent to Sylvester matrices.

We note that an unpublished paper [22] of Moorhouse classifies all complex Hadamard matrices with doubly transitive automorphism groups. Our classification agrees with his in the special case considered here.

4 Cocyclic development

Theorem 16 implies that if H is a cocyclic Hadamard matrix developed from a difference set, then $\mathcal{A}(H)$ is doubly transitive. In this short section, we describe all the groups over which the Hadamard matrices of Corollary 24 are cocyclic. This can be achieved for any Hadamard matrix H by classifying subgroups of the permutation automorphism group which act regularly on the rows and columns of the expanded matrix

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

and contain the central involution $(-I, -I)$. This turns out to be equivalent to classifying regular subgroups of $\mathcal{A}(H)$ which possess some additional properties (specifically, the preimage in $\mathrm{Aut}(H)$ of such a regular subgroup must project onto a regular permutation group on the columns of H).

We consider the sporadic cases first. The next two results were obtained using the computational techniques developed in [25] from ideas due to de Launey.

Lemma 26 ([25], Section 5.3)**.** *A Hadamard matrix of order* 12 *is cocyclic over the alternating group A_4, the dihedral group of order* 12 *and $C_2 \times C_6$, with extension groups* $\mathrm{SL}_2(3)$*,* $C_3 \rtimes Q_8$ *and* $C_3 \times Q_8$ *respectively.*

The cocyclic Hadamard matrices of order 36 are classified in [26]. The Hadamard matrix of Ito and Leon is not contained in the classification. In fact the Paley Type II matrix is the only cocyclic Hadamard matrix at this order with a non-solvable automorphism group.

Lemma 27. *Let H be in the unique equivalence class of Hadamard matrices of order* 36 *with $\mathcal{A}(H) \cong \mathrm{Sp}_6(2)$. Then H is not cocyclic over any group.*

This leaves only the Paley Hadamard matrices to consider. The groups over which a Paley Hadamard matrix is cocyclic have been described by de Launey and Stafford. This result is deep, and relies on detailed knowledge about the finite near-fields, amongst other things.

Theorem 28 ([7], Section 5)**.** *Let H be a Paley Hadamard matrix of order $q+1$. Then H is cocyclic over the dihedral group of order $q+1$, with dicyclic extension group. There are additional extension groups only for $q \in \{3, 7, 11, 23, 59\}$.*

The additional extensions in Theorem 28 are described in Section 5 of [7]. The matrices of orders $4, 8, 12$ and 24 are also discussed in Chapter 5 of [25]. There is just one additional extension group for the Paley Hadamard matrix of order 60, namely $\mathrm{SL}_2(5)$.

Corollary 29. *Let H be a Hadamard matrix with $\mathcal{A}(H)$ non-affine doubly transitive. Then H is cocyclic if and only if either H is of order 12, or H is equivalent to a Paley Hadamard matrix. In both cases all groups over which H is cocyclic and all extension groups for H are known.*

5 A classification of $(4n-1, 2n-1, n-1)$-difference sets with 'transitive extensions'

In this section, we classify up to equivalence (in the sense of Definition 12) the $(4n-1, 2n-1, n-1)$-difference sets which correspond to the Hadamard matrices of Corollary 24.

Suppose that H is a Hadamard matrix such that $\mathcal{A}(H)$ is non-affine doubly transitive. Let $\mathcal{S}$ be a symmetric $2-(4n-1, 2n-1, n-1)$ design underlying H. We may assume (by Theorem 12) that $\mathrm{Aut}(\mathcal{S})$ is transitive, so that $\mathrm{Aut}(\mathcal{S}) \cong \mathcal{A}(H)_1$ by Theorem 10, or H is of order 12. Then by Theorem 13, the difference sets corresponding to H are in bijection with the regular subgroups of $\mathcal{A}(H)_1$. Note that we do not describe all difference sets in these groups (a listing of all difference sets in elementary abelian groups is well beyond the bounds of existing techniques!), but only those for which the corresponding Hadamard matrix H has $\mathcal{A}(H)$ non-affine doubly transitive.

To summarise: for each of the doubly transitive groups identified by Ito, we classify the regular subgroups of a point stabiliser on the remaining points. We choose a representative from each conjugacy class of regular subgroups and describe the difference sets in these groups which correspond to the Hadamard matrices of Corollary 24.

Lemma 30. *Suppose that H is a Hadamard matrix of order 12. Let $\mathcal{S}$ be a symmetric design corresponding to H. Then $\mathrm{Aut}(\mathcal{S})$ has precisely one conjugacy class of regular subgroups, each of which contains the Paley difference set of that order.*

Proof. The stabiliser of a point in M_{12} is the simple group M_{11}, but the automorphism group of $\mathcal{S}$ is $\mathrm{PSL}_2(11)$. This group has a unique conjugacy class of regular subgroups. The First Multiplier Theorem (see Theorems VI.2.6 and VI.2.11 of [2]) allows us to settle this case by hand. We are searching for an $(11, 5, 2)$-difference set in $\mathbb{Z}_{11}$, so 3 is a multiplier. That is, any difference set in $\mathbb{Z}_{11}$ has a translate which is fixed by the automorphism $x \mapsto 3x$. The orbits of this automorphism are $\{1, 3, 4, 5, 9\}$, $\{2, 6, 7, 8, 10\}$ and $\{0\}$. But the first orbit consists precisely of the quadratic residues of $\mathbb{F}_{11}$, so is a Paley difference set. The second orbit also forms a difference set, which is equivalent to the first under the inversion automorphism. □

It is easy to show that S_8 does not contain a subgroup of order 35 (no element of order 5 commutes with an element of order 7 in S_8). Hence in its action on 35 points, S_8 does not contain a regular subgroup.

Lemma 31. *Suppose that H is a Hadamard matrix of order 36, and $\mathcal{A}(H) \cong \mathrm{Sp}_6(2)$ acting doubly transitively. Then H is not developed from any difference set.*

Remark 32. Lemmas 27 and 31 may be compared to [27, Theorem 10].

By Corollary 24, all that remains to be considered are the Paley Hadamard matrices. Let H be the Paley Hadamard matrix of order $q+1$. Then $\mathcal{A}(H) \cong \mathrm{P\Sigma L}_2(q)$, by Theorem 21. Then by Theorem 11, we see that a symmetric 2-design corresponding to the Paley Hadamard matrix of order $q+1$ has a subgroup of index 2 in $\mathrm{A\Gamma L}_1(q)$ as its automorphism group. Thus, our first task is to classify the regular subgroups of this automorphism group. For convenience, we now state the main results of our investigations.

Theorem 33. *Let H be the Paley Hadamard matrix of order $q+1$. Express q as p^{np^e} for a prime p, and n coprime to p. Then $\mathcal{A}(H)_1$ has $e+1$ conjugacy classes of regular subgroups. One is normal and elementary abelian, the remainder are non-normal, non-abelian of exponents p^{2p^t} for $0 \leq t \leq e-1$.*

The difference sets in the abelian regular subgroups are equivalent to the Paley difference sets. A description of the non-abelian difference sets corresponding to the Paley Hadamard matrices is given in the proof of Lemma 46. This will complete the description of all difference sets for which the corresponding Hadamard matrix H has $\mathcal{A}(H)$ non-affine doubly transitive.

Corollary 34. *There exists a difference set corresponding to a Hadamard matrix H with $\mathcal{A}(H)$ non-affine doubly transitive if and only if H is a Paley Hadamard matrix. All such difference sets are known.*

The rest of this section is devoted to a proof of Theorem 33.

5.1 The regular subgroups of $A\Gamma L_1(q)$

Let K/L be a Galois field extension of degree n, with Galois group G. Then the Normal Basis Theorem states that there exists an element of ω of K such that ω^G is a basis for K as an L-vector space. Recall that extensions of finite fields are always Galois, with cyclic Galois group.

We will consider $\mathbb{F}_q$ as a field extension of $\mathbb{F}_p$ for the moment. Extensions of intermediate fields are obtained by replacing the Frobenius automorphism σ by a suitable power, and will be considered later. We now determine the regular subgroups of $\mathrm{A\Gamma L}_1(q)$ in its natural action.

Lemma 35. *Suppose that $q = p^n$ and p does not divide n. Then the only regular subgroup of $\mathrm{A\Gamma L}_1(q)$ is elementary abelian and normal.*

Proof. The subgroup T consisting of the maps $x \mapsto x + a$ for $a \in \mathbb{F}_q$ is a regular normal subgroup of $\mathrm{A\Gamma L}_1(q)$ and is easily seen to be elementary abelian. But a Sylow p-subgroup of $\mathrm{A\Gamma L}_1(q)$ is of order q; hence T is the unique subgroup of order q in $\mathrm{A\Gamma L}_1(q)$. □

We consider now the case that $q = p^p$. (The argument for the general case is almost identical, and is given later.) In this case, a Sylow p-subgroup of $\mathrm{A\Gamma L}_1(q)$ has order p^{p+1}, and a regular subgroup has order p^p. By the Normal Basis Theorem, we may consider $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space V of dimension p, on which the Frobenius automorphism σ acts by cyclic permutation of co-ordinates. We fix some notation: $\{v_1, v_2, \ldots, v_p\}$ is a basis for V, $\mathrm{A\Gamma L}_1(q) = \langle a_1, a_2, \ldots, a_p, \beta, \sigma\rangle$ where the action of each of the generators is given by

$$v^{a_i} = v + v_i, \qquad v^\beta = bv, \qquad v_i^\sigma = v_{i+1},$$

with subscripts interpreted modulo p, b is a primitive element of $\mathbb{F}_q^*$ and the action of σ is extended linearly to all of $V = \mathbb{F}_q$. The subgroup $G = \langle a_1, \ldots, a_p, \sigma\rangle$ is a Sylow p-subgroup of $\mathrm{A\Gamma L}_1(q)$. We can determine a presentation of G with relative ease:

$$G = \langle a_1, \ldots, a_p, \sigma \mid a_i^p = \sigma^p = 1, [a_i, a_j] = 1, a_i^\sigma = a_{i+1}, 1 \le i, j \le p\rangle\,.$$

Remark 36. We observe that the prime subfield of $\mathbb{F}_q$ is fixed by σ; it is the subspace spanned by $v_1 + v_2 + \cdots + v_p$.

Lemma 37. *A non-trivial element of G is either fixed-point-free, or is conjugate to an element of $\langle\sigma\rangle$ and fixes p points.*

Proof. The element σ centralises p^2 elements of G (namely those of the form $a_1^x \cdots a_p^x \sigma^t$), so $|N_G(\langle\sigma\rangle)| = p^2$ and the number of distinct conjugates of $\langle\sigma\rangle$ in G is $p^{p+1}/p^2 = p^{p-1}$. Now σ fixes the prime subfield, so a non-trivial element in the union U of these conjugates fixes at least p points in V. Note that $|U| = p^{p-1}(p-1) + 1$. Since G is transitive on V, it then follows from the Cauchy-Frobenius formula that each non-trivial element of U fixes precisely p points, and that $G \setminus U$ is the set of fixed-point-free elements of G. □

Definition 38. Let E be a multiplicatively written elementary abelian group of order p^k, with fixed minimal generating set $\{e_1, \ldots, e_k\}$. Then the *weight* of an element of E is given by

$$w(e_1^{x_1} \cdots e_k^{x_k}) = \sum_{i=1}^{k} x_i \mod p \quad (0 \le x_i \le p - 1).$$

Definition 39. Each element g of G may be expressed uniquely in the form $a\sigma^t$ for some $a \in \langle a_1, \ldots, a_p\rangle$ and $0 \le t \le p - 1$. Define the weight $w(g)$ of g to be $w(a)$. Also define the *class* of g to be t.

Lemma 40. *The weight and class of an element of G are invariant under conjugation by G.*

Proof. Each quantity is preserved under conjugation by the generators of G. □

Lemma 41. *All conjugates of σ have weight 0. Furthermore, an element of G of weight zero is conjugate to σ^t if and only if it has class t.*

Proof. The first part is immediate from Lemma 40. For the second, it suffices to show that an element of weight zero and class t is conjugate to σ^t.

By Lemma 37, σ^t has p^{p-1} conjugates. Each of these is an element of weight zero and class t. But there are precisely p^{p-1} elements in G with this property. The result follows. □

By definition $\langle a_1, \dots, a_p\rangle$ acts transitively on V; hence it is a regular subgroup of G. As the next theorem shows, this is the only abelian regular subgroup.

Theorem 42. *Let $q = p^p$. Then $\mathrm{A\Gamma L}_1(q)$ has two conjugacy classes of regular subgroups. In particular, all non-abelian regular subgroups are $\mathrm{A\Gamma L}_1(q)$-conjugate.*

Proof. Consider the subgroup

$$T_k = \langle a_i\sigma^k,\ 1 \le i \le p\rangle$$

of G. Note that T_k is abelian if and only if $k = 0$. We claim that $T_k = \{a\sigma^{k\cdot w(a)} \mid a \in T_0\}$. To see this, let $g = a\sigma^{kt}$ and $h = b\sigma^{ks}$ for $a, b \in T_0$ have weights t, s respectively; then

$$gh = a\sigma^{kt}b\sigma^{ks} = ab^{\sigma^{-kt}}\sigma^{k(t+s)}$$

has weight $w(a) + w(b^{\sigma^{-kt}}) = t + s$ and class $k(t + s)$. Since T_k is generated by elements of weight 1 and class k, this implies by induction that the class of $g \in T_k$ is $k \cdot w(g)$, as required.

We show that each T_k is a regular subgroup of G. Let $g \in T_k$, $g \ne 1$. If $w(g) \ne 0$ then g is fixed-point-free by Lemmas 31 and 34. Suppose that $w(g) = 0$. Then the class of g is zero by the previous paragraph. By Lemmas 31 and 35, we see once again that g is fixed-point-free. But T_k has order p^p and acts on a set of this size: it is regular.

In the next part of the proof we establish that the T_k are the only regular subgroups of G. Since a regular subgroup R has index p in G, R must contain the normal subgroup

$$K = \langle a_1a_2^{-1}, a_2a_3^{-1}, \dots, a_{p-1}a_p^{-1}\rangle$$

of G that lies in every T_k. Note that $|K| = p^{p-1}$, K consists of all elements of weight 0 in T_0, and $T_0 = \cup_{i=0}^{p-1} a_1^i K$. If $R \ne T_0$ then $R = \langle a_1^s\sigma^t, K\rangle$ for some $1 \le s, t \le p-1$. But $a_1^s\sigma^t = a_1^s\sigma^{rs}$ where $r \equiv ts^{-1} \mod p$, so that $R = T_r$.

Now choose any r, $1 < r \le p - 1$. Let $c \equiv r^{-1} \mod p$. Then there exists $\gamma \in \langle\beta\rangle$ such that $v^\gamma = cv$ for all $v \in V$. The equalities

$$v_i^{\gamma\sigma} = (cv_i)^\sigma = cv_i^\sigma = c(v_i^\sigma) = v_i^{\sigma\gamma}$$

and

$$v^{\gamma^{-1}a_i\gamma} = (c^{-1}v + v_i)^\gamma = v + cv_i = v^{a_i^c}$$

imply that $\sigma^\gamma = \sigma$ and $a_i^\gamma = a_i^c$. Therefore $T_1^\gamma = \langle a_i^c\sigma,\, 1 \leq i \leq p\rangle = T_r$.

Finally, since a regular subgroup of $\mathrm{A\Gamma L}_1(q)$ is contained in some Sylow p-subgroup, and (as we just showed) all non-abelian regular subgroups of the Sylow p-subgroup G are conjugate, all non-abelian regular subgroups of $\mathrm{A\Gamma L}_1(q)$ are conjugate. □

Corollary 43. *Suppose that F is a field of characteristic p and that K is an extension of F. Then $A\Gamma L_F(K)$, the group of semilinear transformations of K fixing F, contains one conjugacy class of regular subgroups for each power of p dividing the degree of the extension (including p^0).*

Proof. In the case that K is an extension of degree mp where $p \nmid m$, it suffices to consider K as an extension of degree p over a suitable intermediate field. The argument of the previous theorem holds with minor modifications.

Now we consider field extensions of degree p^a. Here we construct a tower of extensions, each of degree p. It is then seen that one additional conjugacy class of regular subgroups is obtained at each level of the tower. □

We recall that the automorphism group of a symmetric Paley 2-design $\mathcal{S}$ is of index 2 in $\mathrm{A\Gamma L}_1(q)$. So its Sylow p-subgroups are the same as those of $\mathrm{A\Gamma L}_1(q)$. Thus the conjugacy classes of regular subgroups of $\mathrm{Aut}(\mathcal{S})$ are in bijection with those of $\mathrm{A\Gamma L}_1(q)$. This completes the proof of Theorem 33.

6 Application: Skew-Hadamard difference sets

Definition 44. Let $\mathcal{D}$ be a (v, k, λ)-difference set in G. Then $\mathcal{D}^{-1} = \{d^{-1} \mid d \in \mathcal{D}\}$ is also a (v, k, λ)-difference set in G. We say that $\mathcal{D}$ is *skew* if $\left|\mathcal{D} \cap \mathcal{D}^{-1}\right| = 0$ and $G = \mathcal{D} \cup \mathcal{D}^{-1} \cup \{1\}$.

It is easily seen that all skew difference sets have parameters of the form $(4n-1, 2n-1, n-1)$. Thus the terms 'skew' and 'skew-Hadamard' are interchangeable when referring to difference sets. Skewness is a strong condition to impose on a difference set and it implies several non-existence results.

Theorem 45 ([1], Theorem 4.15)**.** *The only skew difference sets in cyclic groups are the Paley difference sets in groups of prime order.*

For many years the Paley difference sets were the only known examples of skew difference sets, and it was conjectured that they were the only examples. Recently Ding and Yuan [8] used Dickson polynomials to construct new skew difference sets in the additive groups of $\mathbb{F}_{3^5}$ and $\mathbb{F}_{3^7}$. They show that these difference sets are inequivalent to the Paley ones. They conjecture that their construction produces inequivalent difference sets for all elementary abelian groups of order 3^{2n+1}. This paper revitalised the study of skew-Hadamard difference sets: recent results of Feng [9] give a construction for such difference sets in non-abelian groups of order p^3. Muzychuk [24] goes even further: he shows that there are exponentially many equivalence classes of skew-Hadamard difference sets in elementary abelian groups of order q^3. In this section we construct the first triply infinite family of skew difference sets inequivalent to the Paley family. These appear to be the first known skew difference sets in non-abelian p-groups of unbounded exponent.

Lemma 46. *The group T_1 as defined in the proof of Theorem 42 contains a Hadamard difference set.*

Proof. Since T_1 acts regularly on the Paley design, Theorem 13 guarantees the existence of a Hadamard difference set in T_1.

We describe the difference set explicitly. Let $\mathcal{D}$ be a difference set in T_0 (we can take $\mathcal{D}$ to be the set of quadratic residues of $\mathbb{F}_{p^p}$). Recall that $T_1 = \{\sigma^{w(a)}a \mid a \in T_0\}$. Define $\mathcal{D}_1 = \{\sigma^{w(a)}a \mid a \in \mathcal{D}\}$. Now, σ normalises T_1. Hence, σ is a multiplier of $\mathcal{D}_1$ (see Lemma $VI.2.4$ of [2]). So there exists a translate of $\mathcal{D}_1$ which consists of a union of orbits of σ on T_1.

Express this translate of $\mathcal{D}_1$ as $\mathcal{D}'_1 = \cup_{i=0}^{p-1}\sigma^i X_i$. Then since σ is weight preserving, each X_i is a union of orbits of σ. This implies that

$$X_i X_j^{-1} = X_i^{\sigma^k}(X_j^{-1})^{\sigma^k} = (X_i X_j^{-1})^{\sigma^k}$$

for any power k of σ. Then the multiset of quotients

$$\{\sigma^{i-j}(ab^{-1})^{\sigma^{-j}} \mid \sigma^i a, \sigma^j b \in \mathcal{D}'_1\}$$

represents each element of T_1 equally often, because $\mathcal{D}$ is a difference set. Thus $\mathcal{D}_1$ is a difference set in T_1. □

Remark 47. Any group T_k, as a conjugate of T_1, also contains a Hadamard difference set.

One direction of the following lemma is stated in Remark VI.8.24 of [2].

Lemma 48. *Let G be a group containing a difference set $\mathcal{D}$, and let M be the associated $\{\pm 1\}$-matrix of $\mathcal{D}$. That is,*

$$M = [\chi(g_i g_j^{-1})]_{g_i, g_j \in G}$$

where the ordering of the elements of G used to index rows and columns is the same, and where $\chi(g) = 1$ if and only if $g \in \mathcal{D}$. Then $M + I$ is skew-symmetric if and only if $\mathcal{D}$ is skew-Hadamard.

Proof. Suppose that $(M + I)^\top = -M - I$. Then the elements of $\mathcal{D}$ are precisely those for which $\chi(g_i 1^{-1}) = 1$ (i.e. they correspond to positive entries in the first row of M). But by skew-symmetry of $M + I$ we obtain that $\chi(1 g_i^{-1}) = -\chi(g_i 1^{-1})$, so that $g_i \in \mathcal{D}$ if and only if $g_i^{-1} \notin \mathcal{D}$. Hence $\mathcal{D}$ is skew as required.

In the other direction, observe that

$$M^\top = \left[\chi(g_i g_j^{-1})\right]^\top_{g_i, g_j \in G} = \left[\chi(g_j g_i^{-1})\right]_{g_i, g_j \in G} = \left[\chi((g_i g_j^{-1})^{-1})\right]_{g_i, g_j \in G}.$$

So if $\mathcal{D}$ is skew-Hadamard then $(M + I)^\top = -M - I$. □

Theorem 49. *The group T_1 contains a skew-Hadamard difference set.*

Proof. Since the Paley Hadamard matrices are skew, this follows from Lemmas 46 and 48. □

Thus Theorem 49 furnishes a family of skew non-abelian difference sets in groups of order p^{np^e} for any prime $p \equiv 3 \mod 4$, n odd and coprime to p, and $e \geq 1$. These difference sets have not previously appeared in the literature.

To conclude this section, we observe that there are no other skew-Hadamard difference sets for which the corresponding Hadamard matrix has a doubly transitive automorphism group.

Theorem 50. *Let H be a Hadamard matrix of order greater than 8 with affine doubly transitive automorphism group. Then H is not developed from a skew-Hadamard difference set.*

Proof. First, suppose that H is developed from a skew-Hadamard difference set. Then by Lemma 48, the incidence matrix for the underlying 2-design is skew; hence any difference set corresponding to H will be equivalent to a skew difference set.

H has order 2^n for some n, and by a result of Moorhouse [22] is equivalent to the Sylvester matrix of that order. It is well known that the underlying 2-design $\mathcal{S}$ of a Sylvester Hadamard matrix is isomorphic to the point-hyperplane design of projective n-space over $\mathbb{F}_2$. Thus the automorphism group of $\mathcal{S}$ contains a regular cyclic subgroup (a Singer cycle).

But if H is developed from a cyclic skew difference set then H is equivalent to a Paley matrix, by Theorem 45. It is well known that the Paley and Sylvester series of matrices coincide only at orders 4 and 8. □

Corollary 51. *Let $\mathcal{D}$ be a skew difference set, and H the Hadamard matrix developed from $\mathcal{D}$. Then $\mathcal{A}(H)$ is doubly transitive if and only if H is equivalent to a Paley Hadamard matrix.*

7 Application: Hall's sextic residues

We use our classification of Hadamard matrices with non-affine doubly transitive automorphism group to establish necessary and sufficient conditions for a Hall difference set to correspond to a cocyclic Hadamard matrix.

Definition 52. Let p be a prime of the form $4n - 1 = x^2 + 27$ for some positive integer x (there are no non-trivial prime powers of this form). Let $\mathbb{F}$ be a field of size p, and denote by C the multiplicative group of $\mathbb{F}$. Let U be the unique subgroup of index 6 in C and denote by μ a preimage in $\mathbb{F}_p$ of a generator of C/U. Then $U \cup \mu U \cup \mu^3 U$ is a $(p, \frac{p-1}{2}, \frac{p-3}{4})$ difference set in $\mathbb{F}$, which we call a *Hall difference set.* The elements of this difference set are generally known as *Hall's sextic residues.*

Theorem 11.6.7 of [11] proves the existence of these difference sets, and characterises them, together with the Paley difference sets, as the only ones having the sextic residues as multipliers.

We will require the following result, claimed by Ramanujan, and later proved by (among others) Mordell.

Theorem 53 ([23])**.** *The only solutions of the Diophantine equation* $2^n = x^2+7$ *are* $n = 3, 4, 5, 7, 15$.

A *Hall matrix* is a Hadamard matrix developed from a Hall difference set.

Theorem 54. *Suppose that* H *is a Hall matrix of order* t*. Then* H *is cocyclic if* $t = 32$*, and possibly if* $t = 131072$*, but not otherwise.*

Proof. Suppose that H is cocyclic. By Theorem 16, $\mathcal{A}(H)$ is doubly transitive.

We begin with the affine case. By Theorem 53, the only solutions to the equation $2^n = 4x^2 + 28$ occur when $n \in \{5, 6, 7, 9, 17\}$. But of these values of n, the only ones such that $2^n - 1$ is prime are $n \in \{5, 7, 17\}$. A computation in Magma [3] reveals that the Hall matrix of order 32 is equivalent to the Sylvester matrix of that order, and so is cocyclic (see Section 6.4.1 of [14]). Again, by direct computation, the Hall matrix of order 128 does not have a transitive automorphism group, and so is not cocyclic.

In the non-affine case, Theorem 33 and Corollary 34 imply that H is cocyclic only if a Hall difference set corresponding to H is equivalent to a Paley difference set. This does not occur (see Remark VI.8.4 of [2]). □

We conclude with an application of the classification of doubly transitive permutation groups to settle the remaining order 2^{17} in Theorem 54.

Lemma 55. *The Hall matrix* H *of order* 131072 *is not cocyclic.*

Proof. First, we prove that $\mathcal{A}(H)$ is non-solvable. By Theorem 11.6.7 of [11], the 6^{th} powers in $\mathbb{F}_{2^{17}-1}$ are multipliers of the difference set. Thus $\mathrm{PermAut}(H)$ contains a subgroup of order $\frac{2^{17}-2}{6}$. Lemma 9 then implies that $\mathcal{A}(H)$ contains a subgroup of this order. By Theorem XII.7.3 of [15], a solvable doubly transitive group of degree 2^{17} is a subgroup of $\mathrm{A\Gamma L}_1(2^{17})$. But this has order $17(2^{17})(2^{17}-1)$, and so cannot contain a subgroup of order $\frac{2^{17}-2}{6}$.

So the automorphism group of H is non-solvable. Hering has classified the non-solvable affine doubly transitive groups (a list is given in Section 5 of [12] and proved to be exhaustive in [13]). There are only three infinite families of doubly transitive affine groups, and two of these are easily dispatched: both $G_2(q)$ and $\mathrm{Sp}_{2n}(q)$ act on even dimensional vector spaces. Thus if $\mathcal{A}(H)$ is doubly transitive then $\mathcal{A}(H)_1$ contains $\mathrm{SL}_{17}(2)$ as a normal subgroup. Recall that $\mathrm{SL}_n(2) \cong \mathrm{PGL}_n(2)$ is itself doubly transitive. Hence as a transitive extension of $\mathcal{A}(H)_1$, $\mathcal{A}(H)$ is triply transitive. But by Proposition 2 of [17], a Hadamard matrix with triply transitive automorphism group is equivalent to a Sylvester Hadamard matrix. All Singer subgroups of $\mathrm{PSL}_{17}(2)$ are conjugate, but this yields a contradiction of Remark VI.8.4 of [2]. □

Acknowledgments

The author would like to thank Dr Dane Flannery and Dr Richard M Stafford for their advice and support.

References

[1] Leonard D. Baumert. *Cyclic difference sets.* Lecture Notes in Mathematics, Vol. 182. Springer-Verlag, Berlin, 1971.

[2] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, second edition, 1999.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. the user language. *J. of Symbolic Comput.*, 24:235–265, 1997.

[4] Iliya Bouyukliev, Veerle Fack, and Joost Winne. 2-(31,15,7), 2-(35,17,8) and 2-(36,15,6) designs with automorphisms of odd prime order, and their related Hadamard matrices and codes. *Des. Codes Cryptogr.*, 51(2):105–122, 2009.

[5] Dean Crnković and Sanja Rukavina. On Hadamard $(35, 17, 8)$ designs and their automorphism groups. *J. Appl. Algebra Discrete Struct.*, 1(3):165–180, 2003.

[6] Warwick de Launey and Dane Flannery. *Algebraic Design Theory.* Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence, RI, 2011.

[7] Warwick de Launey and Richard M. Stafford. On cocyclic weighing matrices and the regular group actions of certain Paley matrices. *Discrete Appl. Math.*, 102(1-2):63–101, 2000. Coding, cryptography and computer security (Lethbridge, AB, 1998).

[8] Cunsheng Ding and Jin Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.

[9] Tao Feng. Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism. *J. Combin. Theory Ser. A*, 118(1):27–36, 2011.

[10] Marshall Hall, Jr. Note on the Mathieu group M_{12}. *Arch. Math. (Basel)*, 13:334–340, 1962.

[11] Marshall Hall, Jr. *Combinatorial theory.* Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons Inc., New York, second edition, 1986.

[12] Christoph Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata*, 2:425–460, 1974.

[13] Christoph Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II. *J. Algebra*, 93(1):151–164, 1985.

[14] K. J. Horadam. *Hadamard matrices and their applications.* Princeton University Press, Princeton, NJ, 2007.

[15] Bertram Huppert and Norman Blackburn. *Finite groups. III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1982.

[16] Noboru Ito. Hadamard matrices with "doubly transitive" automorphism groups. *Arch. Math. (Basel)*, 35(1-2):100–111, 1980.

[17] Noboru Ito and Hiroshi Kimura. Studies on Hadamard matrices with "2-transitive" automorphism groups. *J. Math. Soc. Japan*, 36(1):63–73, 1984.

[18] Noboru Ito and Jeffrey S. Leon. An Hadamard matrix of order 36. *J. Combin. Theory Ser. A*, 34(2):244–247, 1983.

[19] Dieter Jungnickel. Difference sets. In *Contemporary design theory*, Wiley-Intersci. Ser. Discrete Math. Optim., pages 241–324. Wiley, New York, 1992.

[20] William M. Kantor. Automorphism groups of Hadamard matrices. *J. Comb. Theory*, 6:279–281, 1969.

[21] Marion E. Kimberley. On collineations of Hadamard designs. *J. London Math. Soc. (2)*, 6:713–724, 1973.

[22] G. Eric Moorhouse. *The 2-transitive complex Hadamard matrices. Preprint.* http://www.uwyo.edu/moorhouse/pub/complex.pdf.

[23] L. J. Mordell. The diophantine equations $2^n = x^2 + 7$. *Ark. Mat.*, 4:455–460, 1962.

[24] Mikhail Muzychuk. On skew Hadamard difference sets. *Arxiv.net*, 1012.2089v1, 2010.

[25] Padraig Ó Catháin. *Group Actions on Hadamard matrices.* M. Litt. thesis, National University of Ireland, Galway, 2008.

[26] Padraig Ó Catháin and Marc Röder. The cocyclic Hadamard matrices of order less than 40. *Des. Codes Cryptogr.*, 58(1):73–88, 2011.

[27] Padraig Ó Catháin and Richard M. Stafford. On twin prime power Hadamard matrices. *Cryptogr. Commun.*, 2(2):261–269, 2010.