Inequivalence of difference sets: On a remark of Baumert

Padraig Ó Catháin*

School of Mathematics and Physics,

University of Queensland, QLD 4072, Australia.

January 9, 2013

Abstract

An often cited statement of Baumert in his book *Cyclic difference sets* asserts that four well known families of cyclic $(4t-1, 2t-1, t-1)$ difference sets are inequivalent, apart from a small number of exceptions with $t \leqslant 8$. We are not aware of a proof of this statement in the literature.

Three of the families discussed by Baumert have analogous constructions in non-cyclic groups. We extend his inequivalence statement to a general inequivalence result, for which we provide a complete and self-contained proof. We preface our proof with a survey of the four families of difference sets, since there seems to be some confusion in the literature between the cyclic and non-cyclic cases.

2010 Mathematics Subject Classification: 05B20

* *E-mail: p.ocathain@gmail.com*

1 Introduction

While (v, k, λ)-difference sets were first investigated by Kirkman in the 1850s [15], it was not until the work of Singer and Hall in the 1930s and 1940s that they became a topic of general mathematical interest [23, 9]. At first interest was focussed for the most part on difference sets with $\lambda = 1$, since any such difference set corresponds to a finite projective plane with a regular group of collineations. A Hadamard difference set is at the opposite end of the spectrum, having the maximum possible value of λ for a given group order. We will make this more precise in the next section.

Already in the 1930s the connections between Hadamard matrices, symmetric designs with parameters $(4t-1, 2t-1, t-1)$ and difference sets were realized [21]. We give a brief introduction to difference sets and their relation to symmetric designs and Hadamard matrices in Section 2. The material in Section 2 is standard: it is included for completeness. A good reference for this section is [3].

In Section 3 we introduce automorphisms of 2-designs, and discuss difference sets in detail. We include a discussion of multipliers of difference sets. Throughout we assume familiarity with the theory of permutation groups. We will occasionally appeal to sophisticated results on permutation groups (e.g. the classification of doubly transitive groups, the classification of the maximal subgroups of S_n). Sometimes this is unnecessary; the same result can be proved by a more lengthy elementary argument. However, we prefer the brevity and clarity of this more algebraic approach.

In Section 4 we specialize to difference sets with parameters $(4t-1, 2t-1, t-1)$, which we call Hadamard. We are mostly concerned with four families of Hadamard difference sets which were discovered in the mid-twentieth century. Three of the families are *cyclotomic*, which is to say they are constructed from n^{th} power residues in a finite field [24]. The fourth is a special case of Singer's construction.

In Section 5, we give the content of Baumert's remark on the inequivalence of these families of difference sets. We extend this to the non-cyclic case and state our main theorem.

Section 6 contains some necessary number theoretic preliminaries and the proof of the main theorem. This concludes the paper.

2 2-designs and Hadamard matrices

Definition 1. Let V be a finite set of size v, and let B be a set of k-subsets of V. We say that $\Delta = (V, B)$ is a t-(v, k, λ) *design* if for any t-subset T of V, $|\{b \in B \mid T \subseteq b\}| = \lambda$, for some fixed λ. We call a t-(v, k, λ) design *non-trivial* if $v - 1 > k > \lambda > 0$ and $t > 1$.

Definition 2. An *incidence matrix* M for Δ is a $\{0, 1\}$-matrix with rows indexed by elements of V and columns indexed by elements of B, whose entry in row x and column b is 1 if $x \in b$ and 0 otherwise. Note that M is an incidence matrix of a 2-(v, k, λ) design if and only if

$$MM^\top = (k - \lambda)I + \lambda J \tag{1}$$

where I is the $v \times v$ identity matrix, and J is the $v \times v$ all 1s matrix.

Clearly, the orderings of V and B used to index rows and columns of M are irrelevant. So M is unique only up to row and column permutations. This motivates the definition of equivalence for designs.

Definition 3. We say that designs $\Delta_1 = (V_1, B_1)$ and $\Delta_2 = (V_2, B_2)$ are *equivalent* if there exists a bijection $\phi : V_1 \to V_2$ which induces an incidence preserving bijection of blocks. Thus Δ_1 and Δ_2 are equivalent if and only if their incidence matrices are the same, modulo row and column permutations.

Definition 4. Consider a 2-(v, k, λ) design $\Delta = (V, B)$ with $|V| = |B|$. We say that Δ is *symmetric* in this case. An incidence matrix M of Δ is square. Note that $M^\top$ is also the incidence matrix of a 2-(v, k, λ) design, called the *dual*, which is not necessarily equivalent to Δ.

We will be interested in symmetric designs in this paper. We observe that the parameters of a symmetric design obey some identities. By counting the number of blocks containing a given point in two different ways, we obtain

$$\lambda(v - 1) = k(k - 1).$$

Thus, we can express λ as a function of v and k: $\lambda = \frac{k(k-1)}{v-1}$. If Δ is a symmetric 2-(v, k, λ), then the *complementary* design $\overline{\Delta} = (V, \overline{B})$ where $\overline{B} = \{V - b \mid b \in B\}$ has parameters $(v, v - k, \frac{(v-k)(v-k-1)}{v-1})$. So without loss of generality, we may assume that $k \leqslant \frac{v}{2}$.

We are interested in the maximum value obtained by λ (equivalently k) for fixed v, subject to the constraint $k \leqslant \frac{v}{2}$. Our main interest is in the case that $v \equiv 3 \mod 4$. If we choose $k = \frac{(v-1)}{2}$, we obtain the parameters $(4t - 1, 2t - 1, t - 1)$. These are then the parameters of a symmetric 2-(v, k, λ) design which maximize λ for fixed v.

It is conjectured that symmetric designs with these parameters exist for all $t \in \mathbb{N}$. A design with these parameters is known as a *Hadamard design* in the literature. The usage of Hadamard design for two families of symmetric designs, with parameters $(4N^2, 2N^2 - N, N^2 - N)$ and $(4t - 1, 2t - 1, t - 1)$, associated in different ways to Hadamard matrices is unfortunate, but probably too well established at this point to be altered. In this paper we consider only the latter family. When confusion could arise, we refer to the first type as Menon-Hadamard and the second as Paley-Hadamard.

Suppose that $v = 2u$ is even and $k = u$: then $\lambda = \frac{u(u-1)}{2u-1}$. We observe that $\gcd(2u - 1, u(u-1)) \leqslant 3$. Hence there are no non-trivial designs with these parameters. When v is even, the upper bound $v = \frac{k}{2}$ is achieved asymptotically by the Menon-Hadamard designs which have parameters $(4N^2, 2N^2 - N, N^2 - N)$.

It seems that the problem of finding the maximal value of λ for which a symmetric 2-design exists when $v \equiv 0, 1, 2 \mod 4$ has not received much attention.

2.1 Hadamard matrices

Definition 5. Let H be an $n \times n$ matrix with real entries satisfying $|h_{i,j}| \leqslant 1$. We say that H is *Hadamard* if and only if $|\det(H)| = n^{\frac{n}{2}}$.

It is well known that a Hadamard matrix of order n necessarily has entries drawn from $\{\pm 1\}$, and that $n = 1, 2$ or $4|n$. Each of the following conditions is sufficient for a $\{\pm 1\}$-matrix H to be Hadamard.

- $HH^\top = nI_n$.
- The dot product of any pair of distinct rows of H is 0.

Definition 6. We say that a Hadamard matrix $H = [h_{i,j}]_{1 \leqslant i,j \leqslant n}$ is *normalized* if and only if $h_{i,1} = h_{1,j} = 1$ for all $1 \leqslant i, j \leqslant n$. Any Hadamard matrix can be transformed into a normalized Hadamard matrix by negation of rows and columns.

The following lemma is standard; see e.g. Lemma I.9.3 of [3].

Lemma 7. *Let Δ be a symmetric 2-$(4n-1, 2n-1, n-1)$-design with incidence matrix M. Define J to be the $(4n-1) \times (4n-1)$ all 1s matrix, and T to be $2M - J$. 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.

Definition 8. Two Hadamard matrices H and H' are *equivalent* if there exist $\{\pm 1\}$-monomial matrices P and Q such that $PHQ^\top = H'$. The group of all pairs of monomial matrices (P, Q) such that $PHQ^\top = H$ is the *automorphism group* of H. This group has an induced permutation action on the set of rows of H and their negations. The set of pairs of rows $\{r, -r\}$ is a system of imprimitivity for $\mathrm{Aut}(H)$. So $\mathrm{Aut}(H)$ has an induced permutation action on the set of such pairs. We refer to this permutation group as $\mathcal{A}_H$. For a detailed discussion of this group see [19].

Lemma 7 has a converse: the existence of a symmetric 2-$(4n-1, 2n-1, n-1)$ design is equivalent to the existence of a Hadamard matrix of order $4n$. In one direction this process is canonical: a symmetric 2-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. A single equivalence class of Hadamard matrices can correspond to many inequivalent symmetric 2-designs.

3 Automorphisms of 2-designs and difference sets

Definition 9. An *automorphism* of the design $\Delta = (V, B)$ is a permutation of V which preserves B setwise. The set of automorphisms of Δ forms a subgroup of $\mathrm{Sym}(V)$, denoted

$\mathrm{Aut}(\Delta)$. There is a natural isomorphism between $\mathrm{Aut}(\Delta)$ and the set of pairs (P, Q) of permutation matrices such that $PMQ^\top = M$, where M is an incidence matrix of Δ. We denote the image of this isomorphism by $\mathrm{Aut}(M)$.

We observe that $\mathrm{Aut}(\Delta)$ has an induced action on the set B of blocks of Δ. In the case that Δ is a symmetric design, the actions on points and blocks are closely related. Denote the isomorphism from $\mathrm{Aut}(\Delta)$ to $\mathrm{Aut}(M)$ by $\phi : \sigma \mapsto (P, Q)$. Then the projections $\psi_1 : \sigma \mapsto P$ and $\psi_2 : \sigma \mapsto Q$ give the actions of $\mathrm{Aut}(\Delta)$ on points and blocks respectively. Since the incidence matrix of a symmetric 2-design is invertible over $\mathbb{C}$, we have that $\psi_1(\sigma) = M\psi_2(\sigma)M^{-1}$, and so ψ_1 and ψ_2 are conjugate as linear representations. They are not in general conjugate as permutation representations however.

The following result is often known as the orbit theorem.

Theorem 10 (cf. Theorem III.4.1, [3])**.** *Let Δ be a non-trivial symmetric 2-design, and let $G \leqslant \mathrm{Aut}(\Delta)$. Then the number of orbits of G on points is equal to the number of orbits of G on blocks.*

Suppose now that there exists a subgroup G of $\mathrm{Aut}(\Delta)$ which acts regularly on V. We can choose some $x \in V$, and label it with the identity of G. We then obtain a bijection $\beta : V \to G$, given by $\beta(x^g) = g$. It is often convenient to identify $b \in B$ with the element

$$\hat{b} = \sum_{x \in b} \beta(x) \tag{2}$$

of the integral group ring $\mathbb{Z}G$. We define $\hat{b}^{(-1)} = \sum_{x \in b} \beta(x)^{-1}$. As usual in this area, we identify G with the sum of its elements in the group ring, $G = \sum_{g \in G} g$.

Now, $\mathrm{Aut}(\Delta)$ has a natural induced action on the elements of G, which preserves $\hat{B} = \left\{ \hat{b} \mid b \in B \right\}$ setwise. In particular, $\hat{b}g$ is a block for any $g \in G$. Now, we note that $G \leqslant \mathrm{Aut}(\Delta)$ acts in its right regular representation in this action. By Theorem 10, G must be fixed point free in its action on $\hat{B}$. We conclude that the $\hat{b}$s are all translates of one another: $\hat{B} = \left\{ \hat{b}g \mid g \in G \right\}$, for any $b \in B$. Thus for any block, we see that

$$\hat{b}\hat{b}^{(-1)} = \sum_{g \in \hat{b}} \hat{b}g^{-1}$$

So $\hat{b}\hat{b}^{(-1)}$ is a sum of k of the $\hat{b}'s$, all of which contain 1_G. By the definition of Δ, every non-identity element of G occurs λ times in these k blocks; we have shown that

$$\hat{b}\hat{b}^{(-1)} = (k - \lambda) + \lambda G.$$

In particular, $\hat{b}\hat{b}^{(-1)}$ is constant on the non-identity elements of G. It is standard to refer to the underlying set of $\hat{b}$ as a *difference set* in G. This discussion leads us to the following definition and theorem.

Definition 11. Let G be a group of order v, and let $\mathcal{D}$ be a k-subset of G. We say that $\mathcal{D}$ is a (v,k,λ)-*difference set* in G if for each $g \neq 1 \in G$, there exist precisely λ pairs of elements $d_i, d_j \in \mathcal{D}$ such that $d_i d_j^{-1} = g$. We say that $\mathcal{D}$ is nontrivial if $v-1 > k > \lambda > 0$. If $\mathcal{D}$ is a difference set in G, then so too is $G-\mathcal{D}$. So, up to replacing $\mathcal{D}$ by its complement in G, we can assume that a (v,k,λ)-difference set has $k \leqslant \frac{v}{2}$.

The next theorem follows from our discussion of difference sets.

Theorem 12 (Theorem VI.1.6, [3])**.** *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.*

Definition 13. We call a map $\vartheta : G \to G$ an *antiendomorphism* of G if $\vartheta(gh) = \vartheta(h)\vartheta(g)$, for all $g,h \in G$. An *antiautomorphism* is a bijective antiendomorphism.

We denote the group consisting of all automorphisms and antiautomorphisms of G by $\mathrm{AntiAut}(G)$. We observe that $\mathrm{Aut}(G)$ is a normal subgroup of index at most 2 in $\mathrm{AntiAut}(G)$, and that this group is generated by $\mathrm{Aut}(G)$ and the inversion map. (Thus $\mathrm{AntiAut}(G) = \mathrm{Aut}(G)$ if and only if G is abelian.)

Since there is no consensus in the literature on when two difference sets $\mathcal{D}_1$ and $\mathcal{D}_2$ are equivalent, give our own definition.

Suppose that $\mathcal{D}$ is a difference set in G. Let $\vartheta \in \mathrm{AntiAut}(G)$ and $g \in G$. Then it is easily verified that $\mathcal{D}^\vartheta$ and $\mathcal{D}g$ are difference sets in G.

Definition 14. Difference sets $\mathcal{D}_1$ and $\mathcal{D}_2$ in G are *equivalent* if there exist $g \in G$ and $\sigma \in \mathrm{AntiAut}(G)$ such that $\mathcal{D}_1 = \mathcal{D}_2^\sigma g$.

Equivalently, $\mathcal{D}_1$ and $\mathcal{D}_2$ are equivalent as difference sets if and only if they lie in the same orbit of $G \rtimes \mathrm{AntiAut}(G)$ under the action $\mathcal{D} \cdot (g,\sigma) = \mathcal{D}^\sigma g$. The stabilizer under this action is the *multiplier group*, discussed further in the next section.

Our definition of equivalence differs slightly from others in the literature, (e.g. p.77 of [12]). Usually σ is required to be an automorphism of G. Our inclusion of antiautomorphisms removes the distinction between left and right multiplication in nonabelian groups, in particular, $g\mathcal{D} = \mathcal{D}^\sigma g^{-1}$ is equivalent to $\mathcal{D}$ under our definition.

Remark 15. Let Δ be a 2-symmetric design. Note that $\mathrm{Aut}(\Delta)$ can contain many conjugacy classes of regular subgroups which are isomorphic as abstract groups. Let R_i $(i = 1,2)$ be regular subgroups of $\mathrm{Aut}(\Delta)$, and let $\mathcal{D}_i$ be the difference set in R_i constructed as in equation (2). If R_1 and R_2 are $\mathrm{Aut}(\Delta)$-conjugate, then there is an isomorphism $\alpha : R_1 \to R_2$ such that $\alpha(\mathcal{D}_1)$ is equivalent to $\mathcal{D}_2$. On the other hand, if R_1 and R_2 are isomorphic but not $\mathrm{Aut}(\Delta)$-conjugate, then there need not be such an isomorphism α.

Just as for the underlying 2-designs, we refer to a difference set with parameters $(4t-1, 2t-1, t-1)$ as Hadamard. We obtain a Hadamard matrix from such a difference

set in two steps: given a $(4t-1, 2t-1, t-1)$-difference set $\mathcal{D}$ we first construct the symmetric 2-design underlying $\mathcal{D}$, then we apply Lemma 7 to obtain a Hadamard matrix.

In fact our principal objective in studying difference sets with these parameters is to obtain new families of Hadamard matrices. We will need some basic results on multipliers of difference sets in later sections, which we introduce now. This will be followed by a discussion of the known families of Hadamard difference sets.

3.1 Multipliers

Let G be a group containing a (v, k, λ)-difference set $\mathcal{D}$, and let Δ be the underlying 2-design. So $\mathrm{Aut}(\Delta)$ contains a regular subgroup R isomorphic to G. The multiplier group of $\mathcal{D}$ is essentially the normalizer in $\mathrm{Aut}(\Delta)$ of R. This can, in some sense, be considered the intersection of $\mathrm{Aut}(\Delta)$ and $\mathrm{AntiAut}(R)$.

The standard exposition of the theory of multipliers is normally in terms of finite abelian groups. Many important results on multipliers rely on the isomorphism between a finite abelian group and its character group, and then use algebraic number theory to derive conclusions. Such an approach is not valid with non-abelian groups. We give our exposition in terms of certain automorphisms of the underlying symmetric design of a difference set. First we fix some notation.

Definition 16. Let $\mathcal{D}$ be a difference set in G. The *right multiplier group* of $\mathcal{D}$, $M(\mathcal{D})$, is the subgroup of $\mathrm{AntiAut}(G)$ consisting of antiautomorphisms ϕ such that $\mathcal{D}^\phi = \mathcal{D}g$ for some $g \in G$. The elements of $M(\mathcal{D})$ are called *right multipliers* of $\mathcal{D}$.

Remark 17. We consider difference sets $\mathcal{D}_1$ and $\mathcal{D}_2$ in G to be equivalent if they lie in the same $G \rtimes \mathrm{AntiAut}(G)$-orbit under the action $\mathcal{D} \cdot (g, \sigma) = \mathcal{D}^\sigma g$. We observe that the elements of $M(\mathcal{D})$ are in bijection with the stabilizer of $\mathcal{D}$ under the action of $G \rtimes \mathrm{AntiAut}(G)$.

We warn the reader that our definition of multiplier is somewhat non-standard in its use of antiautomorphisms. It coincides with the usual definition of multipliers for abelian difference sets, but may be larger in the nonabelian case. Let G be a group containing a difference set $\mathcal{D}$, and let $\phi \in \mathrm{Aut}(G)$. Hall ([11, Section 11.4]) defines a multiplier of $\mathcal{D}$ to be $\mathcal{D}^\phi = g\mathcal{D}h$ for some $g, h \in G$. By allowing ϕ to be an antiautomorphism, we remove the distinction between left and right multipliers.

There seems to be some confusion in the literature over the terminology used for multipliers. The term multiplier originally referred to automorphisms of cyclic groups written additively, in which all automorphisms take the form $x \mapsto tx$ for some t co-prime to the group order. As soon as one considers more general abelian groups, one finds multipliers not of this form, and so one creates the distinction between *numerical* and *non-numerical* multipliers. The concept of a numerical multiplier for a nonabelian group is rather an artificial one, and is inconsistently interpreted in the literature.

The following results relating the multiplier group of $\mathcal{D}$ to the automorphism group of $\mathrm{Aut}(\Delta)$ are of fundamental importance in the theory of difference sets. Denote by

$N_{\mathrm{Aut}(\Delta)}(G)$ the normaliser of G in $\mathrm{Aut}(\Delta)$. Note that we do *not* require the group G to be abelian.

Theorem 18 (Theorem VI.2.18, [3]). *Let Δ be the underlying symmetric design of a difference set $\mathcal{D} \subset G$. Then, identifying G with its right regular representation in $\mathrm{Aut}(\Delta)$, we have that $M(\mathcal{D}) \cong N_{\mathrm{Aut}(\Delta)}(G)/G$.*

Theorem 19 (Theorem VI.2.19, [3]). *Let $\mathcal{D}$ be a difference set in G and let $K \leqslant M(\mathcal{D})$. Suppose that $|K|$ is coprime to $|G|$. Then there exists a translate of $\mathcal{D}$ which is fixed by every multiplier in K.*

Theorem 19 implies that, up to equivalence, $\mathcal{D}$ is the union of K-orbits of G. This result often allows us to construct difference sets with relative ease, given some suitable subgroup of $M(\mathcal{D})$. We use this result in Section 4.2 to derive the uniqueness of the Paley difference sets.

3.2 Cyclotomy

The theory of *cyclotomy* is essentially a study of generalizations of the Paley difference sets. One of the goals of the theory is the determination of necessary and sufficient conditions on a prime power q for the e^{th} powers in the multiplicative group $\mathbb{F}_q^*$ to form a difference set in the additive group $(\mathbb{F}_q, +)$. One may modify this problem to consider unions of cosets of e^{th} powers in $\mathbb{F}_q^*$, or the e^{th} powers with 0, etc. There is also a theory of generalized cyclotomy, which considers more generally difference sets in direct sums of additive groups of fields. A general reference for this material is the monograph of Storer [24].

Definition 20. Let $\mathbb{F}_q$ be a finite field, $q = ef + 1$, and let α be a primitive element of $\mathbb{F}_q$. Then the (non-zero) e^{th} powers of $\mathbb{F}_q$ are precisely those elements of $\mathbb{F}_q$ which lie in the unique subgroup U_0 of index e and order f in $\mathbb{F}_q^*$. The cosets of the e^{th} powers are called the e^{th} *cyclotomic classes* of $\mathbb{F}_q$.

We denote by $(i, j)_e$ the number of solutions in $\mathbb{F}_q$ to the equation

$$\alpha^s + 1 = \alpha^t$$

where $s \equiv i \mod e$ and $t \equiv j \mod e$. Then $\{(i, j)_e \mid 0 \leqslant i, j \leqslant e\}$ is the set of *cyclotomic numbers* of $\mathbb{F}_q$ of order e.

Necessary and sufficient conditions for cosets of the e^{th} powers in $\mathbb{F}_q^*$ to form a difference set can be described entirely in terms of the cyclotomic numbers of order e. All results on cyclotomic difference sets may be considered generalizations or special cases of the following theorem, due originally to Emma Lehmer.

Theorem 21 (Theorem 1, [24]). *The e^{th} powers in $\mathbb{F}_q^*$ form a difference set in $(\mathbb{F}_q, +)$ if and only if for all $0 \leqslant i \leqslant e - 1$*

$$(i, 0)_e = \frac{f - 1}{e}.$$

Example 22. We illustrate Theorem 21 with an example. We take $q = 7$, $e = 2$ and $f = 3$. Now, the quadratic residues in $\mathbb{Z}_7$ are $U_0 = \{1, 2, 4\}$, and the non-residues are $U_1 = \{2, 3, 5\}$. In this small example, we need only to check that $(1, 0)_2 = 1$. That is, that $|\{2+1, 3+1, 5+1\} \cap U_0| = 1$. This shows that $\Delta = \{1, 2, 4\}$ is a difference set in $\mathbb{Z}_7$.

Computations with cyclotomic numbers are made feasible by the following identities.

Theorem 23 (pp. 177-178, [11])**.** *The e^{th} cyclotomic numbers of $\mathbb{F}_q$ obey the following identities:*

- $(i, j)_e = (i + k, j + k)_e$
- $(i, j)_e = (-i, j - i)_e$
- $\sum_{j=0}^{e-1}(i, j) = f - n_i$ *where* $n_0 = 1$ *if f is even,* $n_{\frac{e}{2}} = 1$ *if f is odd, and* $n_i = 0$ *otherwise.*

4 Families of Hadamard difference sets

In this section we consider the four families of Hadamard difference sets discussed in [2] and [11]. We describe each in turn.

4.1 Singer difference sets

Let $\mathrm{PG}_n(q)$ be the n-dimensional projective geometry over $\mathbb{F}_q$. There is a natural duality between k-dimensional and $(n-k)$-dimensional subspaces of $\mathrm{PG}_n(q)$. In particular, every statement about k-dimensional subspaces has a dual statement about $(n-k)$-dimensional subspaces.

Now, the intersection of two hyperplanes in $\mathrm{PG}_n(q)$ is an $(n-2)$-dimensional subspace. It is clear that such a subspace contains $\frac{q^{n-2}-1}{q-1}$ projective points. The dual of this statement is that every pair of subspaces of projective dimension 0 (i.e. projective points) is contained in a constant number $\lambda = \frac{q^{n-2}-1}{q-1}$ of hyperplanes. Hence, with the usual definition of incidence, we obtain the classical point-hyperplane designs.

Definition 24. A *classical point-hyperplane design* is a symmetric design with parameters $(\frac{q^n-1}{q-1}, \frac{q^{n-1}}{q-1}, \frac{q^{n-2}}{q-1})$, with points and blocks given by the (projective) points and hyperplanes respectively of $\mathrm{PG}_n(q)$.

We recall Singer's Theorem on the automorphism group of a projective space.

Theorem 25 (Singer, [3], Theorem III.6.2)**.** *The group* $\mathrm{PGL}_n(q)$ *contains a cyclic subgroup of order* $\frac{q^n-1}{q-1}$ *acting regularly on the points and regularly on the hyperplanes of the projective geometry* $\mathrm{PG}_n(q)$*.*

A cyclic subgroup as in Theorem 25 is called a *Singer cycle*. As a corollary of Theorem 12, we obtain the following.

Corollary 26. *The cyclic group of order* $\frac{q^n-1}{q-1}$ *contains a difference set induced from the point-hyperplane design of* $\mathrm{PG}_n(q)$.

We are interested in the case $q = 2$: such a difference set has parameters $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$. Note that the groups $\mathrm{GL}_n(2)$, $\mathrm{SL}_n(2)$, $\mathrm{PSL}_n(2)$ etc. all coincide.

Furthermore, since $\mathrm{PG}_n(2)$ is obtained by deleting the origin from an n-dimensional vector space over $\mathbb{F}_2$, in this special case we can define the Singer difference set directly in terms of the non-zero elements of $\mathbb{F}_{2^n}$.

Definition 27. Let $q = 2^n$. We define the *trace function* on $\mathbb{F}_q$ to be the map $x \mapsto \sum_{i=0}^{n-1} x^{2^i}$. The elements of $\mathbb{F}_q^*$ of trace zero form a difference set in $\mathbb{F}_q^*$. (See Theorem 2.1.1 of [22] for a proof.) Such a difference set is known as a *Singer difference set*. A *Sylvester Hadamard matrix* is a Hadamard matrix developed from a Singer difference set.

The Sylvester Hadamard matrices may also be constructed directly. Indeed Sylvester's original construction of the matrices that now bear his name was as the Kronecker powers of the matrix

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

It is clear that there exists a Sylvester Hadamard matrix of order 2^n and a Singer difference set in the cyclic group of order $2^n - 1$ for any value of n. In the remainder of this section, we consider the automorphism groups of the Singer 2-designs and Sylvester Hadamard matrices. As a consequence we determine the full multiplier group of a Singer difference set. While these arguments can as easily be given for arbitrary q, we restrict our attention to the case $q = 2$ since that is all that will be required in the remainder of this paper. We refer the reader to Chapter 3 of [22] for further discussion of Singer difference sets.

Theorem 28 (Theorem 2.26, [1])**.** *Let* $\mathbb{F}_q$ *be any finite field, and* $n \geqslant 3$ *a natural number. Then* $\mathrm{P\Gamma L}_n(q)$ *is the full automorphism group of the projective geometry* $\mathrm{PG}_n(q)$.

Now, an automorphism of $\mathrm{PG}_n(q)$ preserves dimension and incidence of subspaces. Hence $\mathrm{P\Gamma L}_n(2) = \mathrm{PSL}_n(2)$ has a faithful induced action on the Singer design with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$. On the other hand, the automorphism group can be no larger. By [16], $\mathrm{PSL}_n(2)$ is maximal in S_{2^n-1}, and since the automorphism group preserves some nontrivial incidence structure, it cannot be S_{2^n-1}.

Theorem 29. *Let* Δ *be the point-hyperplane design of* $\mathrm{PG}_n(2)$. *Then* $\mathrm{Aut}(\Delta) \cong \mathrm{PSL}_n(2)$.

From this theorem, we easily establish some well known properties of the Singer difference sets.

Corollary 30. *All Singer difference sets in* $\mathbb{F}_{2^n}^*$ *are equivalent.*

Proof. All Singer cycles in $\mathrm{PSL}_n(2)$ are conjugate. By Remark 15, it follows that all cyclic difference sets generated from a point-hyperplane design are equivalent. □

Corollary 31 (cf. Proposition 3.1.1, [22]). *The multiplier group of the Singer difference set in $\mathbb{F}_{2^n}^*$ is of order n, generated by the Frobenius automorphism.*

Proof. We use the definition of the Singer difference set. It is clear that the Frobenius automorphism of $\mathbb{F}_{2^n}$ preserves the trace, and hence is an automorphism of the difference set of order n.

By Theorem II.7.3 of [13], the normalizer of a Singer cycle in $\mathrm{PGL}_n(q)$ is of order $2^n n$, and the quotient by the Singer cycle is cyclic of order n. So the full multiplier group is generated by the Frobenius automorphism. □

Several other families of difference sets with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$ are known. Such difference sets are said to have classical parameters, and their study is closely linked to geometry over field extensions of $\mathbb{F}_2$. Important examples are the Gordon-Mills-Welsh construction and the Maschetti hyperoval construction. A paper by Dillon and Dobertin uses Fourier analysis in the additive group of $\mathbb{F}_{2^n}$ to give a unifying construction for many known families of Hadamard difference sets with classical parameters [7].

4.2 Paley difference sets

Theorem 32 (Paley, [21]). *The non-zero quadratic residues of $\mathbb{F}_q$ form a difference set in $\mathbb{F}_q$, $q \equiv 3 \mod 4$.*

Proof. We use cyclotomy, with $e = 2$, $f = \frac{q-1}{2}$. From the first part of Theorem 23, $(0,0)_2 = (1,1)_2$. From the second part $(1,1)_2 = (1,0)_2$, and from the third, $(0,0)_2 + (0,1)_2 = q - 1$ and $(1,0)_2 + (1,1)_2 = q - 2$. We conclude that $(0,0)_2 = (1,0)_2 = \frac{q-1}{2}$.

Thus by Theorem 21, the quadratic residues of $\mathbb{F}_q$ form a difference set. Writing $q = 4t - 1$, we find its parameters to be $(4t - 1, 2t - 1, t - 1)$. □

Definition 33. The difference set in $(\mathbb{F}_q, +)$ consisting of the quadratic residues of $\mathbb{F}_q^*$ is a *Paley difference set*. A *Paley design* is the underlying symmetric 2-design of a Paley difference set, and a *Paley 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 [10], Hall demonstrates that $\mathrm{PSL}_2(q)$ is a subgroup of the automorphism group of the Paley matrix of order $q + 1$. This result was later extended by Kantor, and then by de Launey and Stafford, who determined the full automorphism group.

Theorem 34 (Kantor, [14]; cf. de Launey & Stafford, [6]). *Let H be a Paley matrix of order $p^n + 1 > 12$. Then $\mathrm{Aut}(H)$ is an extension of C_2 by $P\Sigma L_2(p^n)$ (that is, $\mathrm{PSL}_2(p^n)$ extended by field automorphisms).*

As a corollary of this result, we find the multipliers of a Paley difference sets for $q > 11$. (The smaller cases are exceptional, and will be dealt with later.)

Lemma 35. *The multiplier group of the Paley difference set in $\mathbb{F}_q$ is generated by the quadratic residues of $\mathbb{F}_q$ and the Frobenius automorphism of $\mathbb{F}_q$.*

Proof. The stabilizer of a point in $\mathcal{A}_H \cong \mathrm{P\Sigma L}_2(q)$ is a subgroup G of index 2 in the group $\mathrm{A\Gamma L}_1(q)$. Since G cannot have a transitive action on $q+1$ points, this is the full automorphism group of the Paley design (see Theorem 10 of [19]). The group G contains a regular elementary abelian subgroup R, which we identify with $(\mathbb{F}_q, +)$. Now, by Theorem 18, the multiplier group of the Paley difference set is the normalizer in G of R. But R is normal in G. The result follows. □

Caution must be exercised in reading the literature: references such as [2] address only cyclic difference sets. One finds in Theorem 5.19 of that work, a proof that the only multipliers of a Paley difference set are the quadratic residues. This does not contradict our result: the Paley construction yields a cyclic difference set if and only if the field $\mathbb{F}_q$ is prime in which case the Frobenius automorphism is trivial.

An application of Theorem 19 shows that the Paley difference sets are only non-trivial difference sets with the quadratic residues as multipliers. Suppose that $\mathcal{D}$ is a non-trivial difference set in $(\mathbb{F}_q, +)$ (so $1 \leqslant |\mathcal{D}| \leqslant \frac{q-1}{2}$) for which $H = \left\langle x^2 \mid x \in \mathbb{F}_q^* \right\rangle \leqslant M(\mathcal{D})$. Observe that Theorem 19 applies, since $|H| = 2t-1$ and $|G| = 4t-1$ are coprime. Thus there exists a translate of $\mathcal{D}$, $\mathcal{D}+k$ say, which is fixed by H. Now, if $\mathcal{D}+k$ contains a quadratic residue, it contains all quadratic residues, and if it contains a quadratic non-residue, then it contains all the quadratic non-residues. Thus $\mathcal{D}+k$ either consists entirely of quadratic residues, or of quadratic non-residues. In either case $\mathcal{D}$ is equivalent to a Paley difference set.

4.3 Sextic residue difference sets

Sextic residue difference sets were discovered by Marshall Hall, and are a result of the theory of cyclotomy. The associated calculations in showing that certain cosets of the sextic residues form a difference set are lengthy and will be omitted. A proof can be found in Section 11.6 of [11].

Definition 36. Let q be a prime power of the form $x^2 + 27$ for some integer x. Denote by C the multiplicative group of $\mathbb{F}_q$. Let U be the unique subgroup of index 6 in C and denote by μ a preimage in $\mathbb{F}_q$ of a generator of C/U. Then $U \cup \mu U \cup \mu^3 U$ forms a difference set in $(\mathbb{F}_q, +)$, generally known as a *Hall sextic residue difference set* or HSR difference set for short. The underlying 2-design is a *HSR-design*, and the associated Hadamard matrix is a *HSR*-Hadamard matrix.

The following theorem of Marshall Hall provides an important characterization of the HSR and Paley difference sets.

Theorem 37 (Theorem 11.6.7, [11])**.** *Suppose that $\mathcal{D}$ is a difference set in an elementary abelian group of order $q \equiv 7 \mod 12$ which admits the sextic residues as multipliers. Then either $\mathcal{D}$ is equivalent to a Paley difference set, or $\mathcal{D}$ is equivalent to a HSR difference set.*

Hall's construction requires a prime power of the form $x^2 + 27 = p^\alpha$. There are many primes of this form. More generally, the Diophantine equation $x^2 + C = y^n$ has been the subject of much study [5]. The theory of linear forms in logarithms implies that there exists a constant depending only on C bounding $\max\{|x|, |y|, n\}$; thus there are at most finitely many proper prime powers of the form $x^2 + 27$. Complete sets of solutions are known for many values of C, but we are not aware of a solution in the literature for the case $C = 27$. Section 6.7 of [4] is also devoted to this equation. It would appear that the tools for the analysis of this equation are available; but lie beyond the scope of this paper. We pose this as a research problem.

Problem 38. Find all solutions of the equation $x^2 + 27 = p^\alpha$ for $\alpha > 1$.

To our knowledge the automorphism groups and full multiplier groups of the HSR-designs and HSR-Hadamard matrices have never been established. Computational evidence suggests the following. We leave its verification as a research problem, however.

Problem 39. Let q a prime power of the form $x^2 + 27$, and let $\mathcal{D}$ be the HSR difference set in $(\mathbb{F}_q, +)$. Let Δ be the underlying 2-design, and H be the associated Hadamard matrix. Then the sextic residues are multipliers of $\mathcal{D}$. We conjecture for $q > 31$ that $\mathrm{Aut}(\Delta) = (\mathbb{F}_p, +) \rtimes C_{\frac{q-1}{6}}$. Furthermore, we conjecture that $\mathrm{Aut}(H) \cong C_2 \times \mathrm{Aut}(\Delta)$.

With respect to Problem 39, the following is known. Corollary 21 of [19] shows that the automorphism group of H is not doubly transitive. Theorem 4.8 of [18] shows that $|\mathcal{A}_H : \mathrm{Aut}(\Delta)| = 1$. So to determine $\mathrm{Aut}(H)$ in terms of $\mathrm{Aut}(\Delta)$ it suffices to calculate $\mathrm{Ker}(\nu)$. Note that when q is prime, a result of Burnside implies that $\mathrm{Aut}(H)$ is solvable.

4.4 Twin prime power difference sets

By *twin prime powers*, we mean a pair of odd positive integers, q and $q + 2$, each of which is a prime power. We note that twin prime power difference sets are a generalization of twin prime difference sets, which were seemingly first discovered by Gruner in 1939. As Baumert observes, these difference sets 'seem to belong to that special class of mathematical objects which are prone to independent rediscovery'.

Definition 40. Let q and $q + 2$ be twin prime powers, and let $4t - 1 = q(q + 2)$. Denote by χ the standard quadratic residue function. Then

$$\{(g, 0) \mid g \in \mathbb{F}_q\} \bigcup \{(g, h) \mid g \in \mathbb{F}_q, h \in \mathbb{F}_{q+2}, \chi(g)\chi(h) = 1\}$$

is a $(4t-1, 2t-1, t-1)$-difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$. We refer to such a difference set as a *TPP difference set*.

Theorem VI.8.2 of [3] proves that this construction yields a difference set.

With Richard M. Stafford, the author considered these difference sets in some detail in [20]. To our knowledge the full automorphism groups of the TPP-matrices and of the

underlying 2-designs are as yet unknown. We do have the following information however, which informs the problem below.

Let $q = p^n$, and $q+2 = r^m$, where p and r are prime, and let $\mathcal{D}$ be the TPP-difference set of order $q(q+2)$. Denote an arbitrary element of $\mathbb{F}_q \times \mathbb{F}_{q+2}$ by (x, y). Then Δ has automorphisms of the following types.

- $t_{a,b} : (x, y) \mapsto (x + a, y + b)$ for $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q+2}$,
- $m_{c,d} : (x, y) \mapsto (cx, dy)$ for $c \in \mathbb{F}_q^*$, $d \in \mathbb{F}_{q+2}^*$ and $\chi(c)\chi(d) = 1$,
- $\sigma_p : (x, y) \mapsto (x^p, y)$, $\sigma_r : (x, y) \to (x, y^r)$.

Problem 41. Let H be the Hadamard matrix constructed from Δ. Show that the full automorphism group of Δ is

$$\Gamma = \left\langle t_{a,b}, m_{c,d}, \sigma_p, \sigma_r : a \in \mathbb{F}_q, b \in \mathbb{F}_{q+2}, c \in \mathbb{F}_q^*, d \in \mathbb{F}_{q+2}^*, \chi(c)\chi(d) = 1 \right\rangle,$$

and that $\mathrm{Aut}(H) \cong C_2 \times \Gamma$. Show that the full multiplier group of Δ is generated by $\left\langle m_{c,d}, \sigma_p, \sigma_r : c \in \mathbb{F}_q^*, d \in \mathbb{F}_{q+2}^*, \chi(c)\chi(d) = 1 \right\rangle$.

Again, it is known that the automorphism group of H is not doubly transitive. We observe that there are only two non-trivial systems of imprimitivity preserved by Γ. So a careful analysis of the cases of the O'Nan-Scott theorem should suffice to find the full automorphism groups of the TPP-Hadamard matrices, the underlying two designs and hence the multiplier groups of the TPP-difference sets.

5 Baumert's remark

Definition 42. Let $\mathcal{D}$ be a $(4t-1, 2t-1, t-1)$-difference set. We note that all of the families discussed in Section 4 give rise to Hadamard matrices of order $4t$ where one of the following holds:

- $t = 2^n$ for some n. A difference set of this type has *classical parameters*.
- $4t - 1$ is a prime power. A difference set of this type has *prime power parameters*.
- $4t - 1 = q(q + 2)$ where q and $q + 2$ are prime powers. A difference set of this type has *TPP parameters*.

Note that a HSR difference set has prime power parameters, and that prime power and classical parameters coincide precisely at Mersenne primes. There may exist additional difference sets at these orders inequivalent to all of these families. For example there exist 6 inequivalent difference sets in C_{127}: a Singer difference set, a Paley difference set, a HSR difference set and three others. As previously observed, Hadamard difference sets have been most extensively investigated in cyclic groups. Non-existence results for difference sets and extensive computer searches have shown that for all but a handful of orders < 1000, a cyclic Hadamard difference set of order $4t - 1$ exists only if $4t - 1$ belongs to one of the families listed above. This motivates the following conjecture, perhaps first explicitly stated in [8].

Conjecture 43. There exists a cyclic Hadamard difference set in C_{4t-1} if and only if $4t-1$ is of one of the types of Definition 42.

To our knowledge the problem for general groups of order $4t-1$ has not received as much attention. Thus we pose this as a research problem.

Problem 44. Investigate whether there exists a group (not necessarily abelian) of order $4t-1 < 1000$ which contains a Hadamard difference set but does not have parameters of one of the types listed in Definition 42.

A paper of Ding and Yuan reignited interest in $(4t-1, 2t-1, t-1)$ difference sets in 2005 with the construction of *skew* difference sets which are conjectured to be inequivalent to the Paley difference sets. Every skew difference set has prime power parameters. Deciding equivalence of these difference sets requires the development of finer invariants than are discussed in this paper.

In [2, pp. 90-91], Baumert gives a discussion of cyclic Hadamard difference sets and equivalence for such difference sets. This discussion is not accompanied by a proof, but has been frequently cited. We are not aware of any proof appearing the literature. We outline Baumert's conclusions. Then we give our main result, which generalizes Baumert's results to the four families of (not necessarily cyclic) difference sets considered in Section 4. The remainder of the paper consists of a proof of this result. Baumert's book [2] contains the following points.

1. The known (as of c. 1970) families of cyclic Hadamard difference sets all have parameters of the types given in Definition 42.

2. These parameters can intersect: at Mersenne primes for the classical and prime power parameters, and uniquely at 15 for classical and TPP parameters. Furthermore, the only Mersenne primes of the form $x^2 + 27$ are $31, 127$ and 131071.

3. The difference sets of the families listed in Section 4 are inequivalent except for $v = 3, 7, 15, 31$, but the Singer and Paley difference sets are inequivalent for $v = 31$.

We now give our main result; note that we do not assume that difference sets are cyclic.

Theorem 45. *Suppose that $\mathcal{D}_1$ and $\mathcal{D}_2$ are $(4t-1, 2t-1, t-1)$ difference sets of Singer, Paley, TPP or HSR type. Then $\mathcal{D}_1$ and $\mathcal{D}_2$ are equivalent if and only if one of the following occur:*

1. *$v \in 3, 7$, $\mathcal{D}_1$ is Singer and $\mathcal{D}_2$ is Paley.*

2. *$v = 15$, $\mathcal{D}_1$ is Singer and $\mathcal{D}_2$ is TPP.*

3. *$v = 31$, $\mathcal{D}_1$ is Singer and $\mathcal{D}_2$ is HSR.*

6 Proof of the main result

Our proof is broken into a number of preliminary results. We begin by establishing the orders at which the parameter types of Definition 42 coincide. Then at each of these coincidences, we establish equivalence or inequivalence of the relevant difference sets.

6.1 Number theoretic preliminaries

We begin with a number of well known results from number theory, from which we derive straightforward conclusions. The material relating to TPP-parameters has previously appeared in [20], though we include it again here for completeness. Some of the material relating to HSR-difference sets has appeared in [19].

Theorem 46 (Zsigmondy, [25])**.** *Let a, b and n be positive integers such that* $\gcd(a,b) = 1$. *Then there exists a prime p with the following properties:*

- $p \mid a^n - b^n$,
- $p \nmid a^k - b^k$ *for all* $k < n$,

with the following exceptions: $a = 2, b = 1, n = 6$; and $a + b = 2^k, n = 2$.

A proof of the following result may be found in [20].

Corollary 47 (Lemma 16, [20])**.** *The number $2^{2n} - 1$ is not a product of twin prime powers, unless $n = 2$ or $n = 3$.*

Theorem 48 (Mordell, [17])**.** *The only solutions of the Diophantine equation $2^n = x^2 + 7$ are $n = 3, 4, 5, 7, 15$.*

Corollary 49. *Suppose that $p = 2^n - 1$ is a Mersenne prime satisfying $p = x^2 + 27$ for some positive integer x. Then $p \in \{31, 127, 131071\}$.*

Proof. By Theorem 48, the only solutions to the equation $2^n = 4x^2 + 28$ occur when $n \in \{5, 6, 7, 9, 17\}$. But of these, the only ones such that $p = 2^n - 1$ is prime are $n \in \{5, 7, 17\}$. □

We use these number theoretic results to determine necessary and sufficient conditions for the three parameter types described above.

Lemma 50. *The classical and prime power parameters coincide at Mersenne primes. The classical and TPP parameters coincide only for $4t - 1 \in \{15, 63\}$. The prime power and TPP parameters do not overlap.*

Proof. We deal with each proposition in turn. First we consider classical and prime power parameters. $2^n - 1$ is a prime power if and only if it is prime. For suppose n is odd: then $3 \mid 2^n - 1$, so $3^\alpha = 2^n - 1$. An application of Theorem 46 forces $n = 2$. Otherwise, $n = 2m$ is even, in which case $p^\alpha = (2^m - 1)(2^m + 1)$. Assuming that this factorization is

non-trivial leads to a contradiction. Thus, classical and prime power parameters overlap precisely at Mersenne primes.

The claim about classical and TPP parameters follows immediately from Corollary 47.

Finally, the prime power and TPP parameters do not overlap because $4t-1$ cannot be simultaneously a prime power and a product of twin prime powers.

□

6.2 Inequivalence results

We must consider the following cases.

1. Paley and HSR difference sets at prime powers of the form x^2+27.
2. Paley and Singer difference sets at Mersenne primes.
3. The HSR and Singer difference sets at $p \in \{31, 127, 131071\}$.
4. Singer and TPP difference sets at $4t-1 \in \{15, 63\}$.

We deal with each case in turn.

Lemma 51. *Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be Paley and HSR difference sets in $(\mathbb{F}_q, +)$ respectively. Then $\mathcal{D}_1$ and $\mathcal{D}_2$ are inequivalent.*

Proof. With the notation of Definition 36, we have $\mathcal{D}_1 = U \cup \mu^2 U \cup \mu^4 U$ and $\mathcal{D}_2 = U \cup \mu U \cup \mu^3 U$.

We must show that there are no $a, b \in \mathbb{F}_q$ such that $\mathcal{D}_2 = a\mathcal{D}_1 - b$, or equivalently $b^{-1}\mathcal{D}_2 + 1 = ab^{-1}\mathcal{D}_1$. But observe that $ab^{-1}\mathcal{D}_1 = \pm\mathcal{D}_1$ depending on whether or not ab^{-1} is a quadratic residue. Likewise, $b^{-1}\mathcal{D}_2$ remains a union of cosets of U: $b^{-1}\mathcal{D}_2 = \mu^i U \cup \mu^{i+1} U \cup \mu^{i+3} U$ say.

Suppose that ab^{-1} is a quadratic residue. Then, denoting the cyclotomic number $(i,j)_6$ by (i,j), we need only show that $\sum_{k\in 0,1,3}\sum_{j\in 0,2,4}(i+k,j) \neq 0, \frac{p-1}{2}$. Now, applying the identities of Theorem 23, we see that

$$\frac{(q-1)}{6} \leqslant (i,1)+(i,3)+(i,5)+\sum_{j=0}^{5}(0,j) \leqslant \frac{2(q-1)}{6}.$$

If ab^{-1} is a non-residue, it suffices to replace i by $i+1$ throughout. The argument is then identical. Thus $\frac{(q-1)}{6} \leqslant |\mathcal{D}_2 \cap a\mathcal{D}_1 - b| \leqslant \frac{2(q-1)}{6}$ for any $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$. The result follows. □

We now consider Paley and Singer difference sets. The following result is well known, and could also have been derived by considering the 2-ranks of the symmetric designs underlying the difference sets, [22, p.164].

Lemma 52. *Let p be a Mersenne prime. Then the Paley and Singer difference sets in C_p are equivalent if and only if $p \in \{3, 7\}$.*

Proof. Observe that if $\mathcal{D}_1$ and $\mathcal{D}_2$ are equivalent difference sets in G then by Theorem 18 $M(\mathcal{D}_1)$ and $M(\mathcal{D}_2)$ are conjugate in $\mathrm{Aut}(G)$. We consider the orders of the multiplier groups of the Singer and Paley difference sets to establish the inequivalence result.

The multiplier group of the Singer difference set in $\mathbb{F}_{2^n}^*$ consists only of the powers of 2 by Theorem 31, and so has order n. On the other hand, the multiplier groups of the Paley difference set contains the quadratic residues. Thus the multiplier group of the Singer difference set has order at least $\frac{p-1}{2}$.

We solve $\frac{2^n-2}{2} \leqslant n$, to find that the Singer and Paley families can coincide only if $n \leqslant 3$. So the Singer and Paley families can coincide only for $2^n \leqslant 8$.

Finally, we observe that a $(4t-1, 2t-1, t-1)$ difference set with $t = 1$ is trivial; and up to equivalence consists of the identity in C_3. Thus the Singer and Paley difference sets at this order trivially coincide. Similarly, calculating the Singer and Paley difference sets in C_7 (written additively) according to the definitions both give $\{1, 2, 4\}$. □

The argument for the HSR and Singer difference sets is similar, though the proof of isomorphism in the case $p = 31$ is interesting. In the following result, note that the assumption that there exists a HSR difference set means that we may assume that both difference sets are contained in a cyclic group of prime order $p \geqslant 31$.

Lemma 53. *Let p be a Mersenne prime of the form $x^2 + 27$. Then the Singer and HSR difference sets in C_p coincide if and only if $p = 31$.*

Proof. Arguing as in Lemma 52, we find that the multiplier group of a HSR-difference set has order at least $\frac{p-1}{6}$. Solving the equation $\frac{2^n-2}{6} \leqslant n$, we find that $n \leqslant 5$. Thus the only possibility for equivalence here is when $p = 31$. Recall that by Theorem 31, the powers of 2 are the multipliers of the Singer difference sets. We observe a curious phenomenon: the sextic residues of $\mathbb{F}_{31}$ are precisely the powers of 2 in $\mathbb{F}_{31}$. So by Hall's Theorem 37, the Singer difference set in $\mathbb{F}_{31}$ is equivalent either to the Paley difference set or to the HSR difference set in $(\mathbb{F}_{31}, +)$. Now Lemma 52 rules out the Paley difference set, and the result follows. □

Finally, we consider the TPP and Singer difference sets.

Lemma 54. *The TPP and Singer difference sets coincide if and only if $v = 15$.*

Proof. By Lemma 47 we need consider only the cases $v = 15$ and $v = 63$. Now, if $v = 63$, then the TPP difference set is contained in a group isomorphic to $C_3^2 \times C_7$, while the Singer difference set is cyclic. Thus they are trivially inequivalent under our definition of equivalence for difference sets.

When $v = 15$, we construct an isomorphism explicitly. Observe that, relative to a primitive root of the polynomial x^4+x^3+1, the Singer difference set in C_{15} is $\{0, 1, 2, 4, 5, 8, 10\}$. The TPP difference set in $C_3 \times C_5$ is $\{(0,0), (1,0), (2,0), (1,1), (1,4), (2,2), (2,3)\}$. The required isomorphism is then $(1, 1) \mapsto 1$. □

This concludes the proof of the main theorem. We observe that we have not proved that the underlying 2-designs of the difference sets considered in Theorem 45 are necessarily inequivalent. This would imply that the Hadamard matrices generated from these difference sets are inequivalent except for the exceptional isomorphisms listed in Theorem 45. Of course this result would follow from solutions of Problems 39 and 41. Another approach to this problem is via the $\mathbb{F}_p$-ranks of the incidence matrices of the underlying 2-designs. For example some results of this type are given in Section VI.9 of [3].

Acknowledgments

This paper is partly based on material that appeared in the author's PhD thesis, which was completed in the School of Mathematics, Statistics and Applied Mathematics of the National University of Ireland, Galway. The author acknowledges their support.

Furthermore, the author wishes to express gratitude to Dane Flannery, John Dillon and the anonymous referees for helpful comments on earlier drafts of this paper.

References

[1] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

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

[3] T. Beth, D. Jungnickel, and H. Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[4] H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[5] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. *Acta Arith.*, 65(4):367–381, 1993.

[6] W. de Launey and R. 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).

[7] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields Appl.*, 10(3):342–389, 2004.

[8] S. W. Golomb and H.-Y. Song. A conjecture on the existence of cyclic Hadamard difference sets. *J. Statist. Plann. Inference*, 62(1):39–41, 1997.

[9] M. Hall, Jr. Cyclic projective planes. *Duke Math. J.*, 14:1079–1090, 1947.

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

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

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

[13] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

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

[15] T. P. Kirkman. On the perfect r-partitions of $r^2 + r + 1$. *Trans of the Hist. Soc. of Lancashire and Cheshire*, 9:127–142, 1857.

[16] M. W. Liebeck, C. E. Praeger, and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra*, 111(2):365–383, 1987.

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

[18] P. Ó Catháin. *Automorphisms of pairwise combinatorial designs*. Ph. D. thesis, National University of Ireland, Galway, 2011.

[19] P. Ó Catháin. Difference sets and doubly transitive actions on Hadamard matrices. *J. Combin. Theory Ser. A*, 119(6):1235–1249, 2012.

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

[21] R. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.

[22] A. Pott. *Finite geometry and character theory*, volume 1601 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.

[23] J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.

[24] T. Storer. *Cyclotomy and difference sets*. Lectures in Advanced Mathematics, No. 2. Markham Publishing Co., Chicago, Ill., 1967.

[25] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.