SPECIAL SUBSETS OF DIFFERENCE SETS WITH PARTICULAR EMPHASIS ON SKEW HADAMARD DIFFERENCE SETS

ROBERT S. COULTER AND TODD GUTEKUNST

Abstract. This article introduces a new approach to studying difference sets via their additive properties. We introduce the concept of special subsets, which are interesting combinatorial objects in their own right, but also provide a mechanism for measuring additive regularity. Skew Hadamard difference sets are given special attention, and the structure of their special subsets leads to several results on multipliers, including a categorisation of the full multiplier group of an abelian skew Hadamard difference set. We also count the number of ways to write elements as a product of any number of elements of a skew Hadamard difference set.

1. Introduction

Let G be a group, written multiplicatively. Choose any subset $\mathcal{D}$ of G and generate all quotients xy^{-1} with $x, y \in \mathcal{D}$ and $x \neq y$. It is quite likely that in performing this task, some elements will be generated more often than others. However, if every non-identity element of G is generated some constant number of times, then we call $\mathcal{D}$ a *difference set*. Classically, $\mathcal{D}$ is called a (v, k, λ)-difference set in G, where $v = o(G)$, $k = |\mathcal{D}|$ and λ is the number of times each non-identity element is generated. It is clear

$$k(k-1) = \lambda(v-1). \tag{1}$$

For any integer n, we may define the set

$$\mathcal{D}^{(n)} := \{d^n \,:\, d \in \mathcal{D}\}.$$

In particular, with $n = -1$ we obtain the set $\mathcal{D}^{(-1)}$ consisting of the inverses of the elements of $\mathcal{D}$. If $\mathcal{D}$ is a difference set, it is not generally true that $\mathcal{D}^{(n)}$ is a difference set.

Let $\mathcal{D}$ be a difference set in G. For any element $g \in G$, the set

$$\mathcal{D}g := \{dg \,:\, d \in \mathcal{D}\}$$

is also a difference set with the same parameters as $\mathcal{D}$. The sets $\mathcal{D}g$ are called *translates* of $\mathcal{D}$. A *multiplier* for $\mathcal{D}$ is any automorphism of G that maps $\mathcal{D}$ onto one of its translates. If r is an integer coprime to $o(G)$ such that the automorphism $\phi_r : x \mapsto x^r$ induced by r on G is a multiplier for $\mathcal{D}$, then ϕ_r is a *numerical multiplier* for D.

Difference sets arise naturally in the study of combinatorial designs. Specifically, if a symmetric balanced incomplete block design with parameters (v, k, λ) admits a regular automorphism group G, then the points of the design can be labelled by the elements of G and any block of the design forms a (v, k, λ)-difference set in G. Conversely, any difference set $\mathcal{D}$ gives rise to such a design, called the *development* of $\mathcal{D}$. The points of the design are the elements of G and the blocks of the design are the translates of $\mathcal{D}$. Discussion of combinatorial designs leads naturally to the concept of equivalence of difference sets. Two difference sets $\mathcal{D}_1$ and $\mathcal{D}_2$ in G are *equivalent* if one can be mapped onto the other by means of a group automorphism and a translation: $\mathcal{D}_1^{\phi} g = \mathcal{D}_2$ for some $\phi \in Aut(G)$ and $g \in G$.

Adjectives attached to difference sets often describe either the group in which they live or the design they generate. For example, a difference set $\mathcal{D} \subset G$ is called *abelian* or *cyclic* if the group G is abelian or cyclic, respectively. When $\lambda = 1$, the development of a $(v, k, 1)$-difference set is a projective plane. Consequently, such difference sets are called *planar*. A difference set is called *skew* if $\mathcal{D} \cap \mathcal{D}^{(-1)} = \varnothing$, while it is called *reversible* if $\mathcal{D} = \mathcal{D}^{(-1)}$.

A classical example of a difference set is the set $\{1, 2, 4\}$ in $\langle \mathbb{Z}_7, + \rangle$. This set is cyclic, planar and skew. More generally, if q is any prime power congruent to 3 (mod 4), then the non-zero squares of the finite field $\mathbb{F}_q$ form a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-difference set in $\langle \mathbb{F}_q, + \rangle$. Known as the Paley difference sets, these skew difference sets are particularly special, as they are examples of skew difference sets with k as large as possible with respect to v. A difference set $\mathcal{D}$ in G is called a *skew Hadamard difference set (SHDS)* if $\mathcal{D} \,\dot{\cup}\, \mathcal{D}^{(-1)} \,\dot{\cup}\, \{1\} = G$.

For many years, the Paley difference sets were the only known abelian skew Hadamard difference sets. However, in 2005 Ding and Yuan [4] discovered a new class and showed them to be distinct from the Paley class in some small cases. Further examples have since been found, see Ding, Wang and Xiang [3]. It is known a skew Hadamard difference set can only exist in a group of order $q = p^m$, where p is a prime and $q \equiv 3 \bmod 4$; see Johnsen [6]. For a recent survey on difference sets, see Xiang [9].

Let $\mathcal{D}$ be a subset of G, and let a be an arbitrary element of G. We define the *special subsets* of $\mathcal{D}$ with respect to a by

$$\begin{aligned}
\mathcal{A}_{a,\mathcal{D}} &= \{x \in \mathcal{D} \,:\, a = xy^{-1} \text{ for some } y \in \mathcal{D}\},\\
\mathcal{B}_{a,\mathcal{D}} &= \{y \in \mathcal{D} \,:\, a = xy^{-1} \text{ for some } x \in \mathcal{D}\},\\
\mathcal{C}_{a,\mathcal{D}} &= \{x \in \mathcal{D} \,:\, a = xy \text{ for some } y \in \mathcal{D}\}.
\end{aligned}$$

The set $\mathcal{D}$ will usually be clear from context, so we may omit the subscript $\mathcal{D}$ when we write the special subsets. Intuitively, the cardinalities of the sets $\mathcal{A}_a$ and $\mathcal{C}_a$ measure the number of ways to write a as a quotient and product in $\mathcal{D}$, respectively. In this context, a set $\mathcal{D} \subset G$ is a difference set if and only if $|\mathcal{A}_a|$ is constant for all nonidentity elements $a \in G$.

The paper is set out as follows. In Section 2 we briefly consider special subsets for an arbitrary set. We introduce the main body of theory concerning special subsets of skew Hadamard difference sets in Section 3. In Section 4 we present several results on multipliers, including a categorisation of the full multiplier group of an abelian SHDS. We also establish that abelian SHDS satisfy the Multiplier Conjecture using an unsuspected regularity of products within abelian SHDS. In Section 5 we compute the product of all elements of an abelian skew Hadamard difference set, as well as the products of all elements within each special subset.

2. Initial observations on special subsets

Our first two results concerning special subsets are for arbitrary subsets of a group G. Both, however, have implications to difference sets; the first to skew Hadamard difference sets, and the second to reversible difference sets.

Lemma 2.1. *Let $\mathcal{D}$ be a subset of G. Then $\mathcal{A}_a \cap \mathcal{C}_a = \varnothing$ for all $a \in G$ if and only if $\mathcal{D} \cap \mathcal{D}^{(-1)} = \varnothing$.*

Proof. If $x \in \mathcal{A}_a \cap \mathcal{C}_a$ for some $a \in G$, then $a = xy^{-1}$ and $a = xz$ for some elements $y, z \in \mathcal{D}$. But then $x^{-1}a \in \mathcal{D} \cap \mathcal{D}^{(-1)}$. Conversely, if $\mathcal{A}_a \cap \mathcal{C}_a = \varnothing$ for all $a \in G$, then in particular we have $\mathcal{A}_1 \cap \mathcal{C}_1 = \varnothing$. Now $\mathcal{A}_1 = \mathcal{D}$ and $\mathcal{C}_1 \subset \mathcal{D}$, so $\mathcal{C}_1 = \varnothing$. This implies $\mathcal{D}$ is skew. □

Lemma 2.2. *Let $\mathcal{D}$ be a subset of G. Then $\mathcal{A}_a = \mathcal{C}_a$ for all $a \in G$ if and only if $\mathcal{D} = \mathcal{D}^{(-1)}$.*

Proof. Suppose $\mathcal{D} = \mathcal{D}^{(-1)}$. If $a = xy^{-1}$ is a representation for a as a quotient in $\mathcal{D}$, then $a = x(y^{-1})$ is also a representation for a as a product in $\mathcal{D}$, since $y^{-1} \in \mathcal{D}$ by hypothesis. Hence $\mathcal{A}_a = \mathcal{C}_a$ for any $a \in G$. Now suppose $\mathcal{A}_a = \mathcal{C}_a$ for all $a \in G$. In particular, $\mathcal{D} = \mathcal{A}_1 = \mathcal{C}_1$, which is equivalent to $\mathcal{D} = \mathcal{D}^{(-1)}$. □

We now consider how the values $|\mathcal{A}_a|$ and $|\mathcal{C}_a|$ are affected when we translate the set $\mathcal{D}$ to the set $\mathcal{D}g$. If $a = xy^{-1}$ is a representation for the element a as a quotient in $\mathcal{D}$, then clearly $a = (xg)(yg)^{-1}$ is a representation for a as a quotient in $\mathcal{D}g$. Conversely, any representation for a as a quotient in $\mathcal{D}g$ corresponds to a unique representation for a as a quotient in $\mathcal{D}$. Equivalently, the numbers $|\mathcal{A}_a|$ are invariant under translation. But what about the numbers $|\mathcal{C}_a|$?

If G is nonabelian, then little can be said. But if G is abelian, then whenever $a = xy$ is a representation for a as a product in $\mathcal{D}$, $(xg)(yg)$ is a representation for ag^2 as a product in $\mathcal{D}g$. Conversely, any representation for ag^2 as a product in $\mathcal{D}g$ corresponds to a unique representation for a as a product in $\mathcal{D}$. Thus

$$|\mathcal{C}_{a,\mathcal{D}}| = |\mathcal{C}_{ag^2,\mathcal{D}g}|.$$

So while the numbers $|\mathcal{C}_a|$ are in general not invariant under translation, it is clear that the multiset

$$\{\{|\mathcal{C}_a| : a \in G\}\}$$

is invariant under translation.

Now, if $\mathcal{D}$ is a subset of an abelian group G, what are the possible values $|\mathcal{C}_{a,\mathcal{D}}|$? Again if G is nonabelian, then little can be said. If G is abelian, then we have the following theorem.

Theorem 2.3. *For any subset $\mathcal{D}$ of an abelian group G,*

$$\{|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}| : g \in G\} \subseteq \{|\mathcal{C}_{a,\mathcal{D}}| : a \in G\}.$$

If $o(G)$ is odd, then these sets are necessarily equal.

Proof. Let $g \in G$ and suppose $|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}| = t$ for some integer t. Then $|\mathcal{C}_{1,\mathcal{D}g}| = t$. Whenever we can write $1 = (d_1g)(d_2g)$ as a product in $\mathcal{D}g$, then $g^{-2} = d_1d_2$ and conversely. Hence $|\mathcal{C}_{g^{-2},\mathcal{D}}| = t$. In particular, when $o(G)$ is odd, then $\{g^{-2} : g \in G\} = G$, so every value $|\mathcal{C}_{a,\mathcal{D}}|$ is also a value of $|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}|$ for some $g \in G$. □

We end this section with one final lemma concerning special subsets of a skew set $\mathcal{D}$. Clearly, for $\mathcal{D} \subset G$ to be skew, $\mathcal{D}$ cannot contain any pairs of inverses nor any element which is its own inverse. If $\mathcal{D}$ is a skew set that is not properly contained in any other skew set in G, then we call $\mathcal{D}$ a *maximal skew set.* If $v = o(G)$ is odd, any maximal skew set has size $\frac{v-1}{2}$.

Lemma 2.4. *Let G be a group of odd order v and let $\mathcal{D}$ be a maximal skew subset of G. Then*

$$|\mathcal{A}_a| + |\mathcal{C}_a| = \begin{cases} \frac{v-3}{2} & \textit{if } a \in \mathcal{D}, \\ \frac{v-1}{2} & \textit{if } a \notin \mathcal{D}. \end{cases}$$

Proof. Since $o(G)$ is odd, every nonidentity element a of G has an inverse distinct from itself, so precisely one of a, a^{-1} is in $\mathcal{D}$.

Let $a \in \mathcal{D}$. For each $x \in \mathcal{D}$, there is a unique $y \in G$ such that $a = xy$. If $y \in \mathcal{D}$, then $x \in \mathcal{C}_a$. If $y \notin \mathcal{D}$ and $x \neq a$, then $y^{-1} \in \mathcal{D}$, so $x \in \mathcal{A}_a$. However, when $x = a$ we have $y = 1$, and $1 \notin \mathcal{D}$. Hence $|\mathcal{A}_a| + |\mathcal{C}_a| = |\mathcal{D}| - 1 = \frac{v-3}{2}$.

Now let $a \notin \mathcal{D}$. Either $a = 1$ or $a \in \mathcal{D}^{(-1)}$. If $a = 1$, then $\mathcal{A}_a = \mathcal{D}$ while $\mathcal{C}_a = \varnothing$, so $|\mathcal{A}_a| + |\mathcal{C}_a| = \frac{v-1}{2}$. If $a \in \mathcal{D}^{(-1)}$, then by the same argument used above, every $x \in \mathcal{D}$ is either in $\mathcal{A}_a$ or $\mathcal{C}_a$. Hence $|\mathcal{A}_a| + |\mathcal{C}_a| = \frac{v-1}{2}$. □

3. Special subsets of skew Hadamard difference sets

We now turn to skew Hadamard difference sets. Specifically, we outline the fundamental role the special subsets play in their construction and behavior. The first step in this approach is to recognise we may count the number of ways to generate each group element as a product within a skew Hadamard difference set.

Theorem 3.1. *If $\mathcal{D}$ is a (v, k, λ) skew Hadamard difference set, then every element of $\mathcal{D}$ can be written in precisely λ ways as a product in $\mathcal{D}$, while every element of $\mathcal{D}^{(-1)}$ can be written in $\lambda + 1$ ways as a product in $\mathcal{D}$.*

Proof. If $\mathcal{D}$ is a (v, k, λ) skew Hadamard difference set, then $(v, k, \lambda) = (v, \frac{v-1}{2}, \frac{v-3}{4})$. Since $\mathcal{D}$ is skew and $|\mathcal{D}| = \frac{v-1}{2}$, $\mathcal{D}$ is a maximally skew set in G. Hence we may apply Lemma 2.4. Note $|\mathcal{A}_a| = \frac{v-3}{4}$ for all $a \neq 1$. If $a \in \mathcal{D}$, then

$$|\mathcal{C}_a| = \frac{v-3}{2} - \frac{v-3}{4} = \lambda,$$

while if $a \in D^{(-1)}$, then

$$|\mathcal{C}_a| = \frac{v-1}{2} - \frac{v-3}{4} = \lambda + 1.$$

□

Corollary 3.2. *If $\mathcal{D}$ is an abelian skew Hadamard difference set, then every translate $\mathcal{D}g$ of $\mathcal{D}$ satisfies $|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}| \in \{\lambda, \lambda + 1\}$.*

Proof. By Theorems 2.3 and 3.1, the quantity $|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}|$ may take one of only three values: 0, λ, or $\lambda + 1$. However, if $|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}| = 0$ then g^{-2} cannot be written as a product in $\mathcal{D}$. If $g \neq 1$, then this is impossible, and thus any nontrivial translate $\mathcal{D}g$ of D satisfies $|(\mathcal{D}g) \cap (\mathcal{D}g)^{(-1)}| \in \{\lambda, \lambda + 1\}$. □

If $\mathcal{D}$ is a (v, k, λ) skew Hadamard difference set, and if $a \in \mathcal{D}$, then $|\mathcal{A}_a| = |\mathcal{C}_a| = \lambda = \frac{k-1}{2}$. Note a is not in either $\mathcal{A}_a$ nor $\mathcal{C}_a$, since $1 \notin \mathcal{D}$. By Lemma 2.1 the sets $\mathcal{A}_a$ and $\mathcal{C}_a$ are disjoint, so by size considerations $\mathcal{D}$ must be the disjoint union of $\mathcal{A}_a$, $\mathcal{C}_a$, and $\{a\}$. Similarly, if $a \in \mathcal{D}^{(-1)}$, then $\mathcal{D}$ is the disjoint union of $\mathcal{A}_a$ and $\mathcal{C}_a$. In other words, any non-identity element $a \in G$ induces a partition of $\mathcal{D}$ by the special subsets $\mathcal{A}_a$ and $\mathcal{C}_a$ (and possibly the singleton $\{a\}$). We now show that among difference sets, this property is characteristic only of skew Hadamard difference sets.

Theorem 3.3. *A (v, k, λ) difference set $\mathcal{D}$ is skew Hadamard if and only if the following conditions hold:*

(i) *For any $a \in \mathcal{D}$, $\mathcal{D}$ is the disjoint union of $\mathcal{A}_a$, $\mathcal{C}_a$, and $\{a\}$.*
(ii) *For any $a \notin \mathcal{D}$, $\mathcal{D}$ is the disjoint union of $\mathcal{A}_a$ and $\mathcal{C}_a$.*

Proof. A combination of Lemma 2.1 and Theorem 3.1 proves any skew Hadamard difference set satisfies the two conditions. Conversely, any difference set $\mathcal{D}$ satisfying these two conditions must be skew by Lemma 2.1, so $\mathcal{C}_1 = \varnothing$. Our task is to show $k = \frac{v-1}{2}$, as all else will then follow from Theorem 3.1. We have

$$\begin{aligned}\sum_{a \in G} |\mathcal{C}_a| &= |\mathcal{C}_1| + \sum_{a \in \mathcal{D}} |\mathcal{C}_a| + \sum_{a \notin (\mathcal{D} \cup \{1\})} |\mathcal{C}_a| \\ &= 0 + k(k-\lambda-1) + (v-k-1)(k-\lambda) \\ &= k(v-2) - \lambda(v-1) \\ &= k(v-2) - k(k-1) \\ &= k(v-k-1).\end{aligned}$$

But for any $x \in \mathcal{D}$, $x \in \mathcal{C}_{xy}$ for each $y \in \mathcal{D}$. Letting x vary over $\mathcal{D}$, we have

$$\sum_{a \in G} |\mathcal{C}_a| = k^2.$$

Hence $k = \frac{v-1}{2}$, which completes the proof. □

While the sets $\mathcal{B}_a$ appear to play less of a role in this approach, they do exhibit a predictable regularity in the abelian case: they split as evenly as possible between the sets $\mathcal{A}_a$ and $\mathcal{C}_a$.

Theorem 3.4. *Let $\mathcal{D}$ be an abelian skew Hadamard difference set in G, and let $a \in G$, $a \neq 1$. If λ is even, then $|\mathcal{A}_a \cap \mathcal{B}_a| = |\mathcal{B}_a \cap \mathcal{C}_a| = \frac{\lambda}{2}$. If λ is odd and $a \in \mathcal{D}$, then $|\mathcal{A}_a \cap \mathcal{B}_a| = |\mathcal{B}_a \cap \mathcal{C}_a| = \frac{\lambda-1}{2}$. If λ is odd and $a \notin \mathcal{D}$, then $|\mathcal{A}_a \cap \mathcal{B}_a| = \frac{\lambda-1}{2}$ and $|\mathcal{B}_a \cap \mathcal{C}_a| = \frac{\lambda+1}{2}$.*

Proof. Fix $a \neq 1$. Select any $x \in \mathcal{A}_a$ such that $a = xy^{-1}$ for some $y \in \mathcal{B}_a$. For every $x_i \in \mathcal{A}_a$ with $x_1 \neq x$ satisfying $a = x_i y_i^{-1}$ for some $y_i \in \mathcal{B}_a$, we have $(xx_i^{-1})(y_i y^{-1}) = 1$. Since $\mathcal{D}$ is skew Hadamard, precisely one of xx_i^{-1} or $y_i y^{-1}$ must be in $\mathcal{D}$. In the former case $xx_i^{-1} \in \mathcal{D}$ and $y_i y^{-1} \in \mathcal{D}^{(-1)}$, so $x_i \in \mathcal{C}_x$ and $y_i \in \mathcal{C}_y$. So, in this case, we find

$$|\mathcal{A}_a \cap \mathcal{C}_x| = |\mathcal{B}_a \cap \mathcal{C}_y|.$$

In the latter case $xx_i^{-1} \in \mathcal{D}^{(-1)}$ and $y_i y^{-1} \in \mathcal{D}$, so $x_i \in \mathcal{A}_x$ and $y_i \in \mathcal{A}_y$. Here we conclude

$$|\mathcal{A}_a \cap \mathcal{A}_x| = |\mathcal{B}_a \cap \mathcal{A}_y|.$$

The conclusions of the two cases are equivalent by Lemma 2.1. Using $a = a^2a^{-1}$, we therefore have

$$|\mathcal{A}_a \cap \mathcal{C}_{a^2}| = |\mathcal{B}_a \cap \mathcal{C}_a|$$

for any $a \neq 1$.

Select any pair $x, y \in \mathcal{C}_a$ satisfying $a = xy$. For any pair $x_i, y_i \in \mathcal{C}_a$ with $x_i \neq x$ satisfying $a = x_iy_i$ we have $(xx_i^{-1})(yy_i^{-1}) = 1$. Using a similar argument as above we find

$$|\mathcal{C}_a \cap \mathcal{C}_x| = |\mathcal{C}_a \cap \mathcal{A}_y|.$$

Setting $x = y = a$ shows

$$|\mathcal{C}_{a^2} \cap \mathcal{C}_a| = |\mathcal{C}_{a^2} \cap \mathcal{A}_a| = |\mathcal{B}_a \cap \mathcal{C}_a|. \tag{2}$$

Now

$$|\mathcal{C}_{a^2}| = \begin{cases} \lambda & \text{if } a^2 \in \mathcal{D}, \\ \lambda + 1 & \text{if } a^2 \in \mathcal{D}^{(-1)}. \end{cases} \tag{3}$$

The partition $\{\mathcal{A}_a, \mathcal{C}_a\}$ of $\mathcal{D}$ and (2) shows

$$|\mathcal{C}_{a^2}| = \begin{cases} 2|\mathcal{C}_{a^2} \cap \mathcal{C}_a| + 1 & \text{if } a \in \mathcal{D}, \\ 2|\mathcal{C}_{a^2} \cap \mathcal{C}_a| & \text{if } a \in \mathcal{D}^{(-1)}. \end{cases}$$

Solving for $|\mathcal{B}_a \cap \mathcal{C}_a| = |\mathcal{C}_{a^2} \cap \mathcal{C}_a|$ via (3) yields the corresponding claims. □

4. Multiplier results for abelian skew Hadamard difference sets

We now consider how the additive structure of skew Hadamard difference sets described in Section 3 affects the multiplier groups for abelian skew Hadamard difference sets. Throughout this section p is a prime, $p \equiv 3 \bmod 4$, and $\mathcal{D}$ is an abelian skew Hadamard difference set in G, with $exp(G) = p^s$. The strongest result known concerning the multiplier group of $\mathcal{D}$ was established by Camion and Mann [1], who showed the quadratic residues modulo p^s, $\mathcal{Q}_{p^s}$, are precisely the numerical multipliers of $\mathcal{D}$. Our first result on multipliers is a weaker, though often equivalent, version of Camion and Mann's result.

Theorem 4.1. *Let $\mathcal{D}$ be an abelian (v, k, λ) skew Hadamard difference set in G. If $v \equiv 3 \bmod 8$, then $\mathcal{D}^{(2)} = \mathcal{D}^{(-1)}$, and hence $\mathcal{D}^{(4)} = \mathcal{D}$. If $v \equiv 7 \bmod 8$, then $\mathcal{D}^{(2)} = \mathcal{D}$.*

Proof. Let $a \in \mathcal{D}$. If $a = xy$, then $a = yx$ since G is abelian, so the ways to write $a \in \mathcal{D}$ as a product of two distinct elements of $\mathcal{D}$ come in pairs.

If $v \equiv 3 \bmod 8$, then $\lambda = \frac{v-3}{4}$ is even. It follows from Theorem 3.1 that $a \neq x^2$ for any $x \in \mathcal{D}$, or equivalently, $\mathcal{D} \cap \mathcal{D}^{(2)} = \varnothing$. Hence $\mathcal{D}^{(2)} = \mathcal{D}^{(-1)}$, as claimed.

If $v \equiv 7 \bmod 8$, then λ is odd, so there must exist some $x \in \mathcal{D}$ such that $a = x^2$. Hence $\mathcal{D}^{(2)} = \mathcal{D}$. □

It is often true that for primes $p \equiv 3 \bmod 8$, 4 is a multiplicative generator for all quadratic residues modulo p^m. Likewise, for primes $p \equiv 7 \bmod 8$, 2 is often a multiplicative generator of the quadratic residues modulo p^m. For any such prime, Theorem 4.1 is equivalent to the stronger result of Camion and Mann. However, there are primes congruent to 3 mod 4, the smallest of which is 43, for which neither 2 nor 4 generate all quadratic residues. Thus, this result is clearly weaker. We note, however, the fundamental nature of the proof, how it follows immediately from Theorem 3.1, and how it does not rely on the assumption that G is a p-group.

In this sense, one can view our proof as providing a fundamental reason as to why the quadratic residues must be multipliers of a skew Hadamard difference set.

As the quadratic residues modulo p^s comprise the numerical multiplier group of $\mathcal{D}$, they form a subgroup of the full multiplier group of $\mathcal{D}$. Our next result is a categorisation of the full multiplier group of an abelian skew Hadamard difference set.

Theorem 4.2. *Let $\mathcal{D}$ be an abelian skew Hadamard difference set in a group G of exponent p^s. The full multiplier group of $\mathcal{D}$ is precisely the stabilizer of $\mathcal{D}$ in $Aut(G)$. Furthermore, the quadratic residues modulo p^s form a subgroup $\mathcal{Q}_{p^s}$ of the stabilizer of $\mathcal{D}$. Consequently, $\mathcal{D}$ is the union of orbits of the action of $\mathcal{Q}_{p^s}$ on G.*

Proof. By Corollary 3.2, no translate of $\mathcal{D}$ is skew. As a multiplier for $\mathcal{D}$ is firstly an automorphism, it must map skew sets to skew sets. Consequently, any multiplier of $\mathcal{D}$ must in fact fix $\mathcal{D}$ and any automorphism which does so is clearly a multiplier. The remaining claims are clear. □

Our final multiplier result, Theorem 4.5, will follow from the observation that one may easily count the number of ways to write elements as the product of any number of elements of a skew Hadamard difference set $\mathcal{D}$. The computations are most easily carried out in the group ring $\mathbb{Z}G$.

Theorem 4.3. *Let $\mathcal{D} \subset G$ be a (v, k, λ) skew Hadamard difference set. Set $t = (\lambda+1)^2 + \lambda(\lambda+1)G$. Then for any integer $j \geq 2$, we have*

$$\mathcal{D}^j = a_j\mathcal{D} + (\lambda+1)a_{j-1}\mathcal{D}^{(-1)} + a_{j-2}t, \tag{4}$$

where the sequence $\{a_i\}$ satisfies $a_0 = 0$, $a_1 = 1$, $a_2 = \lambda$ and $a_i = \lambda a_{i-1} + t a_{i-3}$ for $i \geq 3$.

Proof. We induct on j. When $j = 2$ we have

$$\mathcal{D}^2 = \lambda\mathcal{D} + (\lambda+1)\mathcal{D}^{(-1)},$$

which is correct by Theorem 3.1. Now suppose $j \geq 2$ and the formula (4) is correct for j. Then

$$\begin{aligned}
\mathcal{D}^{j+1} = \mathcal{D}\mathcal{D}^j &= \mathcal{D}(a_j\mathcal{D} + (\lambda+1)a_{j-1}\mathcal{D}^{(-1)} + a_{j-2}t)\\
&= a_j\mathcal{D}^2 + (\lambda+1)a_{j-1}\mathcal{D}\mathcal{D}^{(-1)} + a_{j-2}t\mathcal{D}\\
&= a_j(\lambda\mathcal{D} + (\lambda+1)\mathcal{D}^{(-1)}) + (\lambda+1)a_{j-1}(\lambda G + (\lambda+1)) + a_{j-2}t\mathcal{D}\\
&= (\lambda a_j + t a_{j-2})\mathcal{D} + (\lambda+1)a_j\mathcal{D}^{(-1)} + a_{j-1}[\lambda(\lambda+1)G + (\lambda+1)^2]\\
&= a_{j+1}\mathcal{D} + (\lambda+1)a_j\mathcal{D}^{(-1)} + a_{j-1}t.
\end{aligned}$$

This completes the induction. □

Introducing the sequence $\{a_j\}$ of coefficients in Theorem 4.3 allows for relatively uncomplicated expressions for higher powers of a skew Hadamard difference set $\mathcal{D}$. The next lemma provides a closed formula for these coefficients.

Lemma 4.4. *The sequence $\{a_j\}$ defined recursively by $a_0 = 0$, $a_1 = 1$, $a_2 = \lambda$, and $a_j = \lambda a_{j-1} + t a_{j-3}$ for $i \geq 3$ satisfies*

$$a_j = \sum_{i \geq 0} \binom{j-2i-1}{i} \lambda^{j-3i-1} t^i. \tag{5}$$

Proof. Base cases $j = 0, 1, 2$ are easily confirmed. Suppose the formula (5) holds for all integers $0 \leq j \leq l$ for some integer $l \geq 2$. We must prove the formula holds for $j = l + 1$. We have

$$\begin{aligned} a_{l+1} &= \lambda a_l + t a_{l-2} \\ &= \lambda \sum_{i \geq 0} \binom{l-2i-1}{i} \lambda^{l-3i-1} t^i + t \sum_{i \geq 0} \binom{l-2i-3}{i} \lambda^{l-3i-3} t^i \\ &= \sum_{i \geq 0} \binom{l-2i-1}{i} \lambda^{l-3i} t^i + \sum_{i \geq 0} \binom{l-2i-3}{i} \lambda^{l-3i-3} t^{i+1} \\ &= \sum_{i \geq 0} \binom{l-2i-1}{i} \lambda^{l-3i} t^i + \sum_{m \geq 1} \binom{l-2m-1}{m-1} \lambda^{l-3m} t^m, \end{aligned}$$

where we have set $m = i+1$ in the second sum. Note that when $m = 0$, $\binom{l-2m-1}{m-1} = 0$, so we may let the second sum run over $m \geq 0$ rather than $m \geq 1$. Relabelling m as i in the second sum, we have

$$\begin{aligned} a^{l+1} &= \sum_{i \geq 0} \binom{l-2i-1}{i} \lambda^{l-3i} t^i + \sum_{i \geq 0} \binom{l-2i-1}{i-1} \lambda^{l-3i} t^i \\ &= \sum_{i \geq 0} \left[\binom{l-2i-1}{i} + \binom{l-2i-1}{i-1} \right] \lambda^{l-3i} t^i \\ &= \sum_{i \geq 0} \binom{l-2i}{i} \lambda^{l-3i} t^i, \end{aligned}$$

which agrees with the formula. This completes the induction. □

Theorem 4.5. *Let $\mathcal{D} \subset G$ be an abelian (v, k, λ) skew Hadamard difference set. Then any odd prime divisor of $\lambda + 1$ is a multiplier of $\mathcal{D}$.*

Proof. Suppose q is an odd prime divisor of $\lambda + 1$. Then $t \equiv 0 \bmod q$, and hence from Lemma 4.4 we see $a_j \equiv \lambda^{j-1} \bmod q$. We thus obtain

$$\begin{aligned} \mathcal{D}^q &= a_q \mathcal{D} + (\lambda + 1) a_{q-1} \mathcal{D}^{(-1)} + a_{q-2} t \\ &\equiv \lambda^{q-1} \mathcal{D} \bmod q \\ &\equiv \mathcal{D} \bmod q. \end{aligned}$$

Since $\mathcal{D}^p \equiv \mathcal{D}^{(p)} \bmod p$ for any prime p (see [7] Lemma 3.3), it follows $\mathcal{D}^{(q)} \equiv \mathcal{D} \bmod q$. This is possible only if $\mathcal{D}^{(q)} = \mathcal{D}$. Hence q is a multiplier for $\mathcal{D}$. □

Theorem 4.5 is connected to one of the well-known problems of multiplier theory. The parameters of a skew Hadamard difference set satisfy $k = 2\lambda + 1$, so $\lambda + 1 = k - \lambda$. For any (v, k, λ) difference set, the quantity $k - \lambda$ is typically called the *order* of the difference set. A famous theorem of Hall [5] on cyclic groups, generalized to abelian groups by Chowla and Ryser [2], states if $\mathcal{D}$ is an abelian difference set and $q > \lambda$ is a prime dividing $k - \lambda$ but not v, then q is a multiplier of $\mathcal{D}$. It is generally believed, however, that the hypothesis $q > \lambda$ is unnecessary. The "Multiplier Conjecture" therefore states that any prime divisor of $k - \lambda$ is a multiplier for the abelian (v, k, λ) difference set $\mathcal{D}$. Theorem 4.5 shows this conjecture is true for skew Hadamard difference sets. This was shown by Xiang in [8, Corollary 2.2.6].

5. Products of elements within special subsets

For any subset $\mathcal{D}$ of a group G, we may define a directed graph $\Gamma_{\mathcal{D}}$ as follows: the elements of $\mathcal{D}$ are the vertices, and the directed edge (x, y) is in $\Gamma_{\mathcal{D}}$ if and only if $xy^{-1} \in \mathcal{D}$.

Lemma 5.1. *If $\mathcal{D}$ is an abelian skew Hadamard difference set, then the directed graph $\Gamma_{\mathcal{D}}$ is a λ-regular tournament.*

Proof. For distinct elements x, y of G, $xy^{-1} \in \mathcal{D}$ if and only if $yx^{-1} \notin \mathcal{D}$, since $\mathcal{D}$ is skew Hadamard. It follows that $\Gamma_{\mathcal{D}}$ is a tournament. Let $x \in \mathcal{D}$, and suppose (x, y) is an edge of $\Gamma_{\mathcal{D}}$. Then $xy^{-1} = d$ for some $d \in \mathcal{D}$, hence $y \in \mathcal{C}_x$. Conversely, any $y \in \mathcal{C}_x$ corresponds to an edge (x, y) of $\Gamma_{\mathcal{D}}$, so the outdegree of vertex x is $|\mathcal{C}_x|$, which equals λ. As x was arbitrary, we see $\Gamma_{\mathcal{D}}$ is a λ-regular tournament. □

The graph $\Gamma_{\mathcal{D}}$ provides a useful mechanism for proving results about certain "large" products within $\mathcal{D}$, which we now describe. As an edge (x, y) in $\Gamma_{\mathcal{D}}$ is naturally associated to the element xy^{-1}, we can associate the walk $x \to y \to z$ in $\Gamma_{\mathcal{D}}$ to the product $(xy^{-1})(yz^{-1}) = xz^{-1}$. In this fashion we may ascribe a value vw^{-1} to a walk of any length from the vertex v to the vertex w. Clearly the value of a walk from v to w is in $\mathcal{D}$ if and only if (v, w) is an edge of $\Gamma_{\mathcal{D}}$. Also clear is the fact that any circuit has value 1.

Any regular tournament is necessarily Eulerian, so let C be an Euler circuit in $\Gamma_{\mathcal{D}}$. Now C has value 1, but as we traverse C each element of $\mathcal{D}$ is generated precisely λ times. As G is abelian, we have

$$\prod_{d \in \mathcal{D}} d^{\lambda} = \left(\prod_{d \in \mathcal{D}} d \right)^{\lambda} = 1.$$

But then

$$\left(\prod_{d \in \mathcal{D}} d \right)^{\gcd(v, \lambda)} = 1.$$

Recall that G is a p-group for some prime $p \equiv 3 \bmod 4$. It is easy to show

$$\gcd(v, \lambda) = \begin{cases} 3 & \text{if } p = 3, \\ 1 & \text{it } p \neq 3. \end{cases}$$

We have proven the following:

Lemma 5.2. *If $\mathcal{D} \subset G$ is an abelian skew Hadamard difference set with $3 \nmid o(G)$, then*

$$\prod_{d \in \mathcal{D}} d = 1.$$

Under the hypotheses of Lemma 5.2, we may compute the product of all elements in each of the special subsets of $\mathcal{D}$. Let $a \in \mathcal{D}$ and suppose λ is even. Then $\mathcal{D}^{(2)} = \mathcal{D}^{(-1)}$, so there is no $x \in \mathcal{D}$ satisfying $x^2 = a$. It follows

$$\prod_{z \in \mathcal{C}_a} z = a^{\lambda/2} \tag{6}$$

By Lemma 5.2 we have

$$\prod_{d\in\mathcal{D}} d = a\left(\prod_{z\in\mathcal{C}_a} z\right)\left(\prod_{x\in\mathcal{A}_a} x\right) = 1,$$

hence

$$\prod_{x\in\mathcal{A}_a} x = a^{-\frac{\lambda}{2}-1}. \tag{7}$$

It then follows

$$\prod_{y\in\mathcal{B}_a} y = a^{-\lambda-\frac{\lambda}{2}-1}. \tag{8}$$

If λ is odd, then there exists $b \in \mathcal{D}$ such that $b^2 = a$. In this case, similar arguments yield

$$\prod_{z\in\mathcal{C}_a} z = a^{\frac{\lambda-1}{2}}b, \tag{9}$$

$$\prod_{x\in\mathcal{A}_a} x = a^{-\frac{\lambda-1}{2}-1}b^{-1}, \tag{10}$$

$$\prod_{y\in\mathcal{B}_a} y = a^{-\lambda-\frac{\lambda-1}{2}-1}b^{-1}. \tag{11}$$

One may easily derive similar expressions for special subsets with respect to an element of $\mathcal{D}^{(-1)}$.

In Section 3 we observed any non-identity element a induces a partition of a skew Hadamard difference set $\mathcal{D}$ into its special subsets $\mathcal{A}_a$ and $\mathcal{C}_a$ (and possibly the singleton $\{a\}$). Using the above products, we may now show that in the abelian case, no two distinct elements may induce the same partition.

Theorem 5.3. *If $\mathcal{D} \subset G$ is an abelian skew Hadamard difference set, then no two distinct elements of G induce the same partition of $\mathcal{D}$ into special subsets.*

Proof. If $a, b \in \mathcal{D}$, then the partitions with respect to a and b are the same if and only if $a = b$, as the singletons $\{a\}$ and $\{b\}$ are cells of their respective partitions. Similarly, if $a \in \mathcal{D}$ and $b \in \mathcal{D}^{(-1)}$, then their respective partitions are clearly not the same. So suppose a^{-1} and b^{-1} are elements of $\mathcal{D}^{(-1)}$ inducing the same partition of $\mathcal{D}$. Then $\mathcal{A}_{a^{-1}} = \mathcal{A}_{b^{-1}}$, which means $\mathcal{B}_a = \mathcal{B}_b$. If λ is even, then

$$a^{-\frac{3}{2}\lambda-1} = \prod_{y\in\mathcal{B}_a} y = \prod_{y\in\mathcal{B}_b} y = b^{-\frac{3}{2}\lambda-1},$$

hence $a^{\frac{3}{2}\lambda+1} = b^{\frac{3}{2}\lambda+1}$.

Note $o(G) = p^m$ for some prime p, so if we can show $\gcd\left(\frac{3}{2}\lambda+1, p\right) = 1$, then we may conclude $a = b$. To the contrary, suppose $\gcd\left(\frac{3}{2}\lambda+1, p\right) > 1$, or equivalently suppose p divides $\frac{3}{2}\lambda+1$. With $\lambda = \frac{p^m-3}{4}$ we have

$$\frac{3}{8}(p^m-3)+1 = tp$$

for some integer t. Thus $3p^m - 8tp = 1$, so $p \mid 1$, a contradiction. Hence $\gcd\left(\frac{3}{2}\lambda+1, p\right) = 1$ and we conclude $a = b$.

Now suppose λ is odd. Then $\mathcal{B}_a = \mathcal{B}_b$ implies $a^{\frac{\lambda+1}{2}} = b^{\frac{\lambda+1}{2}}$. As before, it suffices to show $\gcd\left(\frac{\lambda+1}{2}, p\right) = 1$. If $\gcd\left(\frac{\lambda+1}{2}, p\right) > 1$ then $p \mid (\lambda+1)$, hence $p^m + 1 = tp$ for some integer t. It follows that $p \mid 1$, a contradiction. Hence $\gcd\left(\frac{\lambda+1}{2}, p\right) = 1$, so $a = b$. □

We conclude with a strengthening of Lemma 5.2. Suppose $\mathcal{D}$ is an abelian skew Hadamard difference set in the p-group G. Denote by $\mathcal{D}_{p^i}$ the subset of all elements of $\mathcal{D}$ of order p^i.

Theorem 5.4. *Let G be an abelian group of order p^m, exponent p^s, admitting a skew Hadamard difference set $\mathcal{D}$. If $p \neq 3$ then*

$$\prod_{d \in \mathcal{D}_{p^s}} d = \prod_{d \in \mathcal{D} \setminus D_{p^s}} d = 1.$$

Proof. If $p \neq 3$, then by Lemma 5.2 we know

$$\prod_{d \in \mathcal{D}} d = \left(\prod_{d \in \mathcal{D} \setminus \mathcal{D}_{p^s}} d \right) \left(\prod_{d \in \mathcal{D}_{p^s}} d \right) = 1.$$

Set

$$\prod_{d \in \mathcal{D} \setminus \mathcal{D}_{p^s}} d = g^{-1},$$

and note $o(g) \leq p^{s-1}$. We have

$$g = \prod_{d \in \mathcal{D}_{p^s}} d.$$

Say $\mathcal{D}_{p^s} = \{d_1, \ldots, d_t\}$. Then $gd_i^{-1} = d_1 d_2 \cdots d_t d_i^{-1}$ for any $i \in \{1, \ldots, t\}$. Since $o(gd_i^{-1}) = p^s$, we have $o(d_1 \cdots d_t d_i^{-1}) = p^s$ for all $i = 1, \ldots, t$.

Suppose $g \neq 1$. Then $d_1 \cdots d_t d_i^{-1}$ is either in $\mathcal{D}_{p^s}$ or $\mathcal{D}_{p^s}^{(-1)}$. If $d_1 \cdots d_t d_i^{-1} \in \mathcal{D}_{p^s}$, then $d_1 \cdots d_t d_i^{-1} = d_j$ for some j. Then $d_i d_j = d_1 \cdots d_t = g$, so $d_i, d_j \in \mathcal{C}_g$. Note at most one d_i can satisfy $d_i^2 = g$, so the number of values i such that $d_1 \cdots d_t d_i^{-1} \in \mathcal{D}_{p^s}$ can be no greater than $\frac{\lambda+1}{2} = \frac{p^m+1}{8}$.

It is easy to show $|\mathcal{D}_{p^s}| = t \geq \frac{p^m - p^{m-1}}{2}$. As there are t products of the form $d_1 \cdots d_t d_i^{-1}$ and at most $\frac{p^m+1}{8}$ of them are in $\mathcal{D}_{p^s}$, there are at least

$$\frac{p^m - p^{m-1}}{2} - \frac{p^m + 1}{8} = \frac{3p^m - 4p^{m-1} - 1}{8}$$

such products in $\mathcal{D}_{p^s}^{(-1)}$. Now if $d_1 \cdots d_t d_i^{-1} = d_j^{-1}$, then $g = d_i d_j^{-1}$. Since we assume $g \neq 1$, we have $i \neq j$ and hence $d_j \in \mathcal{B}_g$. Thus

$$|\mathcal{A}_g| = \frac{p^m - 3}{4} \geq \frac{3p^m - 4p^{m-1} - 1}{8},$$

which implies

$$4 \geq p + \frac{5}{p^{m-1}}.$$

As $p > 3$, this is impossible. Hence $g = 1$, which proves the theorem. □

References

[1] P. Camion and H. B. Mann. Antisymmetric difference sets. *J. Number Theory*, 4:266–268, 1972.

[2] S. Chowla and H. J. Ryser. Combinatorial problems. *Canad. J. Math.*, 2:93–99, 1950.

[3] C. Ding, Z. Wang, and Q. Xiang. Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$. *J. Combin. Theory Ser. A*, 114:867–887, 2007.

[4] C. Ding and J. Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113:1526–1535, 2006.

[5] M. Hall, Jr. Cyclic projective planes. *Duke Math. J.*, 14:1079–1090, 1947.
[6] E. C. Johnsen. Skew-Hadamard abelian group difference sets. *J. Algebra*, 4:388–402, 1966.
[7] D. Jungnickel. Difference sets. In *Contemporary Design Theory*, Wiley-Intersci. Ser. Discrete Math. Optim., pages 241–324. Wiley, New York, 1992.
[8] Q. Xiang, *Difference Sets: Their multipliers and existence*, Ph.D. thesis, Ohio State University, 1995.
[9] Q. Xiang. Recent progress in algebraic design theory. *Finite Fields Appl.*, 11:622–653, 2005.

(Coulter) Department of Mathematical Sciences, University of Delaware, Newark, DE, 19716, United States of America.
E-mail address: coulter@math.udel.edu

(Gutekunst) Department of Mathematics, King's College, Wilkes-Barre, PA, 18711, United States of America.
E-mail address: toddgutekunst@kings.edu