Difference sets disjoint from a subgroup

Courtney Hoagland, Stephen Humphries, Seth Poulsen

Brigham Young University, Provo, Ut, USA.

Difference sets

For a group G, identify a finite subset $X \subseteq G$ with the element $\sum_{x \in X} x \in \mathbb{Q}G$ of the group algebra.
Let $X^{-1} = \{x^{-1} : x \in X\}$.

Difference sets

For a group G, identify a finite subset $X \subseteq G$ with the element $\sum_{x\in X} x \in \mathbb{Q}G$ of the group algebra.
Let $X^{-1} = \{x^{-1} : x \in X\}$.
Let G be a finite group, $|G| = v$. Then $D \subset G$ is a *difference set* with parameters (v, k, λ) if every $1 \neq g \in G$ can be written exactly λ times as $ab^{-1}, a, b \in D$. Here $k = |D|$. So

$$D^2 = \lambda(G - 1) + k.$$

Difference sets

For a group G, identify a finite subset $X \subseteq G$ with the element $\sum_{x \in X} x \in \mathbb{Q}G$ of the group algebra.
Let $X^{-1} = \{x^{-1} : x \in X\}$.
Let G be a finite group, $|G| = v$. Then $D \subset G$ is a *difference set* with parameters (v, k, λ) if every $1 \neq g \in G$ can be written exactly λ times as $ab^{-1}, a, b \in D$. Here $k = |D|$. So

$$D^2 = \lambda(G - 1) + k.$$

For $g \in G$ the set Dg is another difference set.

Difference sets

For a group G, identify a finite subset $X \subseteq G$ with the element $\sum_{x \in X} x \in \mathbb{Q}G$ of the group algebra.
Let $X^{-1} = \{x^{-1} : x \in X\}$.
Let G be a finite group, $|G| = v$. Then $D \subset G$ is a *difference set* with parameters (v, k, λ) if every $1 \neq g \in G$ can be written exactly λ times as $ab^{-1}, a, b \in D$. Here $k = |D|$. So

$$D^2 = \lambda(G - 1) + k.$$

For $g \in G$ the set Dg is another difference set.

So we assume: there is a subgroup $1 \neq H \leq G$ such that
(1) $D \cap D^{-1} = \emptyset = D \cap H$;
(2) $G = D \cup D^{-1} \cup H$.

Parameters

Let

$$h = |H|, \quad u = |G : H|.$$

Then we have $h > 1$.
A group having a difference set of the above type will be called a (v, k, λ) *relative skew Hadamard difference set group* (with difference set D and subgroup H).

Main results

Theorem

Let G be a (v, k, λ) relative skew Hadamard difference set group with subgroup H and difference set D. Then
(i) $h = u$ is even, $v = |G| = h^2$, and

$$\lambda = \frac{1}{4}h(h-2), \quad k = \frac{1}{2}h(h-1).$$

(ii) $H \triangleleft G$;
(iii) each non-trivial coset $Hg \neq H$ meets D in $h/2$ points;
(iv) H contains the subgroup generated by all the involutions in G;
(v) the subgroup $H \leq G$ does not have a complement.

Main results

Let $\Phi(G)$ be the Frattini subgroup of G

Theorem

Let G be a group that is a (v, k, λ) relative skew Hadamard difference set group with subgroup H and difference set D. Then
(a) (i) every index 2 subgroup of G contains H and D meets each such subgroup in exactly λ points.
(ii) if $N \lhd G$ has odd prime index p, then $H \leq N$. Each non-trivial coset of N meets D in $\frac{1}{2p}h^2$ elements, while $|N \cap D| = \frac{1}{2p}h(h-p)$.
(b) Now assume that G is also a 2-group. Then $H \leq \Phi(G)$. Further, D meets each maximal subgroup of G in exactly λ points.

Schur rings

Our original motivation for studying (v, k, λ) relative skew Hadamard difference set groups was to produce examples of Schur rings with a small number of principal sets.

A subring $\mathfrak{S}$ of the group algebra $\mathbb{C}G$ is called a *Schur ring* (or S-ring) if there is a partition $\mathcal{K} = \{C_i\}_{i=1}^r$ of G such that:

1. $\{1_G\} \in \mathcal{K}$;
2. for each $C \in \mathcal{K}$, $C^{-1} \in \mathcal{K}$;
3. $C_i \cdot C_j = \sum_k \lambda_{i,j,k} C_k$; for all $i, j \leq r$.

Schur rings

Our original motivation for studying (v, k, λ) relative skew Hadamard difference set groups was to produce examples of Schur rings with a small number of principal sets.
A subring $\mathfrak{S}$ of the group algebra $\mathbb{C}G$ is called a *Schur ring* (or S-ring) if there is a partition $\mathcal{K} = \{C_i\}_{i=1}^r$ of G such that:

1. $\{1_G\} \in \mathcal{K}$;
2. for each $C \in \mathcal{K}$, $C^{-1} \in \mathcal{K}$;
3. $C_i \cdot C_j = \sum_k \lambda_{i,j,k} C_k$; for all $i, j \leq r$.

The C_i are called the *principal sets* of $\mathfrak{S}$.

Difference sets and Schur rings

Theorem

Let G be a (v, k, λ) relative skew Hadamard difference set group with difference set D and subgroup H. Then

$$\{1\},\ H \setminus \{1\},\ D,\ D^{-1},$$

are the principal sets of a commutative Schur-ring over G.

Difference sets and Schur rings

Theorem

Let G be a (v, k, λ) relative skew Hadamard difference set group with difference set D and subgroup H. Then

$$\{1\},\ H \setminus \{1\},\ D,\ D^{-1},$$

are the principal sets of a commutative Schur-ring over G.

Theorem

G is not cyclic.

Difference sets and Minimal polynomials

Theorem

Let G be a (v, k, λ) relative skew Hadamard group with difference set D and subgroup H. Then the minimal polynomial for D is

$$\mu(D) = (x-k)\left(x+\frac{h}{2}\right)\left(x^2+\frac{h^2}{4}\right).$$

Further, the eigenvalues $k, -h/2, ih/2, -ih/2$ have multiplicities

$$1, \;\; h-1, \;\; h(h-1)/2, \;\; , h(h-1)/2.$$

Irreducible representation of G

One can say something about the image of D under an irreducible representation of G:

Theorem

Let G be a (v, k, λ) relative skew Hadamard group with difference set D and subgroup H. Let ρ be a non-principal irreducible representation of G of degree d. Then $\rho(G) = 0I_d, \rho(D^{-1}) = \rho(D)^*$ and we have one of:

Irreducible representation of G

One can say something about the image of D under an irreducible representation of G:

Theorem

Let G be a (v, k, λ) relative skew Hadamard group with difference set D and subgroup H. Let ρ be a non-principal irreducible representation of G of degree d. Then $\rho(G) = 0I_d, \rho(D^{-1}) = \rho(D)^*$ and we have one of:
(i) $\rho(H) = 0I_d$ and $\rho(D) \sim \mathrm{diag}\left(\varepsilon_1 i\frac{h}{2}, \varepsilon_2 i\frac{h}{2}, \ldots, \varepsilon_d i\frac{h}{2}\right)$, for some $\varepsilon_i \in \{-1, 1\}$;

Irreducible representation of G

One can say something about the image of D under an irreducible representation of G:

Theorem

Let G be a (v, k, λ) relative skew Hadamard group with difference set D and subgroup H. Let ρ be a non-principal irreducible representation of G of degree d. Then $\rho(G) = 0I_d, \rho(D^{-1}) = \rho(D)^*$ and we have one of:
(i) $\rho(H) = 0I_d$ and $\rho(D) \sim \mathrm{diag}\left(\varepsilon_1 i\frac{h}{2}, \varepsilon_2 i\frac{h}{2}, \ldots, \varepsilon_d i\frac{h}{2}\right)$, for some $\varepsilon_i \in \{-1, 1\}$;
(ii) $\rho(H) = hI_d$ and $\rho(D) = -\frac{h}{2}I_d$.

Examples

We next give examples of families of (v, k, λ) relative skew Hadamard difference set groups. Let $n \geq 2, 0 \leq k < n-1$ and define the following bi-infinite family of groups:

$$\begin{aligned}
\mathfrak{G}_{n,k} = \langle a_1, \ldots, a_n, b_1, \ldots, b_n | a_i^2 = b_{i+k}, 1 \leq i \leq n, (\text{indices taken mod } n),\\
a_2^{a_1} = a_2 b_1, a_3^{a_1} = a_3 b_2, \ldots, a_{k+1}^{a_1} = a_{k+1} b_k,\\
(a_1, a_{k+2}) = (a_1, a_{k+3}) = \cdots = (a_1, a_n) = 1,\\
(a_i, a_j) = 1, \text{ for } 1 < i, j \leq n,\\
\text{and } b_1, \ldots, b_n \text{ are central involutions}\rangle.
\end{aligned}$$

Theorem

For $n \geq 2, 0 \leq k < n-1$, the group $\mathfrak{G}_{n,k}$ is a relative skew Hadamard difference set group.

Proof for the examples

Let

$$H = \langle b_1, b_2, \ldots, b_n \rangle.$$

Then a transversal for H in G is the set of products $a_X = a_{i_1} a_{i_2} \cdots a_{i_u}$, where $X = \{i_1, i_1, \ldots, i_u\} \subseteq \{1, 2, \ldots, n\}$.

Proof for the examples

Let

$$H = \langle b_1, b_2, \ldots, b_n \rangle.$$

Then a transversal for H in G is the set of products $a_X = a_{i_1} a_{i_2} \cdots a_{i_u}$, where $X = \{i_1, i_1, \ldots, i_u\} \subseteq \{1, 2, \ldots, n\}$.

Here $a_\emptyset = 1$. We may also employ a similar notation for the elements $b_X = b_{i_1} b_{i_2} \cdots b_{i_u}$.

Proof for the examples

Let

$$H = \langle b_1, b_2, \ldots, b_n \rangle.$$

Then a transversal for H in G is the set of products $a_X = a_{i_1} a_{i_2} \cdots a_{i_u}$, where $X = \{i_1, i_1, \ldots, i_u\} \subseteq \{1, 2, \ldots, n\}$.

Here $a_\emptyset = 1$. We may also employ a similar notation for the elements $b_X = b_{i_1} b_{i_2} \cdots b_{i_u}$.

For $g \in G$ we have $g^2 \in H$. We define the hypothesis

(H1): there are distinct maximal subgroups $M_1, \ldots, M_{2^n-1}$ of H, and an ordering $S_1, \ldots, S_{2^n-1}$ of the non-empty subsets of $\{1, \ldots, n\}$ so that $a_{S_i}^2 \notin M_i$.

Proof for the examples

Last step: take

$$D = \sum_i a_{S_i} M_i.$$

Proof for the examples

Proposition

The groups $\mathfrak{G}_{n,k}$ satisfy (H1).

Proof for the examples

Proposition

The groups $\mathfrak{G}_{n,k}$ satisfy (H1).

First step: show that the squares of the coset representatives $a_S, S \subseteq \{1, 2, \ldots, n\}$, are distinct.

Proof for the examples

Proposition

The groups $\mathfrak{G}_{n,k}$ satisfy (H1).

First step: show that the squares of the coset representatives $a_S, S \subseteq \{1, 2, \ldots, n\}$, are distinct.

Second step: construct the M_S.

Proof for the examples (ctd)

Let $V = \mathbb{F}_2^n, V^\times = \mathbb{F}_2^n \setminus \{0\}$. Nonempty subsets of S correspond bijectively to elements of $V^\times$.

Proof for the examples (ctd)

Let $V = \mathbb{F}_2^n, V^\times = \mathbb{F}_2^n \setminus \{0\}$. Nonempty subsets of S correspond bijectively to elements of $V^\times$.

Maximal subgroups of H correspond to subspaces of V of dimension $n-1$,

Proof for the examples (ctd)

Let $V = \mathbb{F}_2^n, V^\times = \mathbb{F}_2^n \setminus \{0\}$. Nonempty subsets of S correspond bijectively to elements of $V^\times$.

Maximal subgroups of H correspond to subspaces of V of dimension $n-1$, which, in turn, are determined by elements of $V^\times$.

Proof for the examples (ctd)

Let $V = \mathbb{F}_2^n, V^\times = \mathbb{F}_2^n \setminus \{0\}$. Nonempty subsets of S correspond bijectively to elements of $V^\times$.
Maximal subgroups of H correspond to subspaces of V of dimension $n-1$, which, in turn, are determined by elements of $V^\times$.
Given a maximal subgroup (or subspace) M we let v_M denote the corresponding vector.

Proof for the examples (ctd)

Let $V = \mathbb{F}_2^n, V^\times = \mathbb{F}_2^n \setminus \{0\}$. Nonempty subsets of S correspond bijectively to elements of $V^\times$.
Maximal subgroups of H correspond to subspaces of V of dimension $n-1$, which, in turn, are determined by elements of $V^\times$.
Given a maximal subgroup (or subspace) M we let v_M denote the corresponding vector.

Thus for (H1) we require $S \leftrightarrow M_S$ where $v_S \leftrightarrow v_{M_S}$, with $v_S \notin M_S$ i.e. $v_S \cdot v_{M_S} = 1$. But this correspondence determines, and is determined by, a function

$$\mu : V^\times \to V^\times, \text{ where } v_u \cdot v_{\mu(u)} = 1 \text{ for all } u \in V^\times.$$

We now show how to construct such a function:

Proof for the examples (ctd)

We will show there is such a function μ that is an involution i.e. $\mu(\mu(v)) = v$ for all $v \in V^\times$.

Proof for the examples (ctd)

We will show there is such a function μ that is an involution i.e. $\mu(\mu(v)) = v$ for all $v \in V^\times$.
For $0 \le k \le n$ we let

$$(\underline{1}_k, 0) = (1, 1, 1, \dots, 1, 0, \dots, 0) \in V,$$

where there are k 1s.

Proof for the examples (ctd)

We will show there is such a function μ that is an involution i.e. $\mu(\mu(v)) = v$ for all $v \in V^\times$.
For $0 \leq k \leq n$ we let

$$(\underline{1}_k, 0) = (1, 1, 1, \ldots, 1, 0, \ldots, 0) \in V,$$

where there are k 1s.
Write $v \in V^\times$ as $v = (v_1, v_2, \ldots, v_n), v_i \in \mathbb{F}_2$. If $1 \leq k \leq n$ where $v_k = 1$ and $v_m = 0$ for $k + 1 \leq m \leq n$, then we let

$$\mu(v) = (\underline{1}_{k-1}, 0) - v,$$

Proof for the examples (ctd)

We will show there is such a function μ that is an involution i.e. $\mu(\mu(v)) = v$ for all $v \in V^\times$.
For $0 \leq k \leq n$ we let

$$(\underline{1}_k, 0) = (1, 1, 1, \ldots, 1, 0, \ldots, 0) \in V,$$

where there are k 1s.
Write $v \in V^\times$ as $v = (v_1, v_2, \ldots, v_n), v_i \in \mathbb{F}_2$. If $1 \leq k \leq n$ where $v_k = 1$ and $v_m = 0$ for $k + 1 \leq m \leq n$, then we let

$$\mu(v) = (\underline{1}_{k-1}, 0) - v,$$

This satisfies $\mu(v) \cdot v = 1$. Since the same k works for $\mu(v)$, we have

$$\mu(\mu(v)) = (1_{k-1}, 0) - ((1_{k-1}, 0) - v) = v.$$

Proof for the examples (ctd)

Last step: take

$$D = \sum_{S \neq \emptyset} a_S M_S.$$

The end

THE END