DIFFERENCE SETS DISJOINT FROM A SUBGROUP: GROUPS OF ORDER $4p^2$

Stephen P. Humphries and **Nathan L. Nicholson**
Brigham Young University, Provo, Ut, USA

Abstract

We study finite groups G having a normal subgroup H and $D \subset G \setminus H, D \cap D^{-1} = \emptyset$, such that the multiset $\{xy^{-1} : x, y \in D\}$ has every non-identity element occur the same number of times (such a D is called a *DRAD difference set*). We show that there are no such groups of order $4p^2$, where p is an odd prime.

Definitions and background

For a group G we will identify a finite subset $X \subseteq G$ with the element $\sum_{x\in X} x \in \mathbb{Q}G$ of the group algebra. We also let $X^{-1} = \{x^{-1} : x \in X\}$. Write $\mathcal{C}_n$ for the cyclic group of order n.
A (v,k,λ) *difference set* is a subset $D \subset G, |D| = k$, such that every element $1 \neq g \in G$ occurs λ times in the multiset $\{xy^{-1} : x, y \in D\}$. Here $|G| = v$.
Then [1, 4] a (v,k,λ) difference set is a (v,k,λ) *DRAD difference set (with subgroup H and difference set D)* if it also satisfies the conditions: there is a subgroup $1 \neq H \triangleleft G$ such that
(1) $D \cap D^{-1} = \emptyset$;
(2) $G \setminus (D \cup D^{-1}) = H$.
A group G will be called a *DRAD difference set group* if there is a DRAD difference set over G. DRAD difference sets are examples of Hadamard (or Menon) difference sets Let

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

Prior result

Previous Theorem [2] Let G be a (v,k,λ) DRAD difference set group with subgroup H and difference set D. Then
(i) $u = h \geq 4$ is even, $v = |G| = h^2$, and

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

(ii) each non-trivial coset $Hg \neq H$ meets D in $h/2$ points;
(iii) H contains the subgroup generated by all the involutions in G;
(iv) any abelian (v,k,λ) DRAD difference set group is a 2-group.

Main Result

Main Theorem There are no (v,k,λ) DRAD difference set groups of order $4p^2$, for an odd prime p.

Method of proof

There are at most 16 isomorphism classes of groups of order $4p^2$.
For the the proof of the Main Theorem we make use of a result of Iiams [3], who showed that any group of order $4p^2$ (where $p > 3$ is a prime) that has $\mathcal{C}_p \times \mathcal{C}_2^2$ as a factor group, does not have a $(4p^2, 2p^2 - p, p^2 - p)$ difference set. This leaves six groups.

We then consider each group individually, showing that none of these six groups can be a DRAD group.
The techniques used are:
1. Find restrictions on the subgroup H. For example, since all involutions are in H, we check to see if the subgroup generated by the involutions has size greater than $h = 2p$. For example in some of the six groups the subgroup generated by the involutions has size $2p^2 > h$.

2. Once we have found normal subgroups H we eliminate some groups using the following result which is easy to check:

Lemma Suppose that G has a non-principal linear character χ.
If $\chi(H) = 0$ and χ takes values in a field K where $i = \sqrt{-1} \notin K$, then G is not a DRAD group with subgroup H.

3. For the remaining three groups we do the following:
Let $D = \sum_{g\in G} \varepsilon_g g$ where $\varepsilon \in \{0,1\}$. Then we know:

$$\varepsilon_g^2 = \varepsilon_g, \quad \varepsilon_g + \varepsilon_{g^{-1}} = 1, \text{ for } g \notin H, \quad \varepsilon_g = 0 \text{ for } g \in H. \tag{1}$$

Let $\mathbb{Z}[\varepsilon_g]_{g\in G}$ be the polynomial ring.
Let $\mathcal{I}$ denote the ideal of $\mathbb{Z}[\varepsilon_g]_{g\in G}$ generated by the relations in (1) and $2\mathbb{Z}$.
Let

$$E = DD^{-1} - (\lambda(G-1) + k) \in \mathbb{Z}[\varepsilon_g]_{g\in G}$$

and for $k \in G$ let E_k denote the coefficient of k in E. Then for $k \in G, k \neq 1$, we have $E_k \in \mathbb{Z}[\varepsilon_g]_{g\in G}$.

Proof ctd

We define:

$$Z_k = \sum_{i=0}^{p-1} E_{y^i k} = \sum_{i=0}^{p-1} \sum_{h\in G} \varepsilon_{y^i k h} \varepsilon_h \in \mathbb{Z}[\varepsilon_g].$$

The result then follows from showing that

$$\mathbb{Z}[\varepsilon_g]_{g\in G} / \langle \mathcal{I}, \{Z_k : k \in G \setminus H\} \rangle$$

is the trivial ring.
More specifically: we show that there are $a, b, c \in G \setminus H$ such that

$$Z_a + Z_b + Z_c \equiv 1 \mod \mathcal{I}.$$

What is a DRAD?

DRAD stands for: Doubly regular asymmetric digraph: D=(V,E):
1. D (or E) is symmetric.
2. D is regular of valency k.
3. D is doubly regular of valency λ (for distinct $v_1, v_2 \in V$ there are λ vertices $v_3 \in V$ such that $(v_i, v_3) \in E, i = 1, 2$).

References

References

[1] Davis, James A.; Polhill, John Difference set constructions of DRADs and association schemes. J. Combin. Theory Ser. A 117 (2010), no. 5, 598–605.

[2] Courtney Hoagland, Stephen P. Humphries, Nathan Nicholson, Seth Poulsen, *Difference Sets Disjoint from a Subgroup*, Graphs and Combinatorics (2019) 35, 579–597

[3] Iiams, J., *On difference sets in groups of order* $4p^2$, Journal of Comb. Theory A, (1996), 256–276.

[4] Ito, Noboru Automorphism groups of DRADs. Group theory (Singapore, 1987), 151–170, de Gruyter, Berlin, (1989).