DIFFERENCE SETS DISJOINT FROM A SUBGROUP

COURTNEY HOAGLAND, STEPHEN P. HUMPHRIES, NATHAN NICHOLSON, SETH POULSEN

Abstract. We study finite groups G having a 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 *difference set*). We show that H has to be normal, that $|G| = |H|^2$, and that $|D \cap Hg| = |H|/2$ for all $g \notin H$. We show that H is contained in every normal subgroup of index 2, and other properties. We give a 2-parameter family of examples of such groups. We show that such groups have Schur rings with four principal sets, and that, further, these difference sets determine DRADs.

Keywords: Difference set, subgroup, DRAD, Schur ring.
[2010]Primary 05B10. Secondary: 20C05.

§1 Introduction

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 $X^{-1} = \{x^{-1} : x \in X\}$. Also, write $\mathcal{C}_n$ for the cyclic group of order n. All groups considered herein will be assumed finite.

A (v, k, λ) *difference set* is a subset $D \subset G, |D| = k$, where G is a group such that every element $1 \neq g \in G$ occurs λ times in the multiset $\{xy^{-1} : x, y \in D\}$. Further, $|G| = v$.

It is well-known that if $D \subset G$ is a difference set, then $gD = \{gd : d \in D\}$ and $\alpha(D)$ are also difference sets, for any $g \in G, \alpha \in \mathrm{Aut}(G)$. Thus in some sense, difference sets are spread out evenly over the group G. In this paper we seek to restrict the types of difference sets considered by imposing the following conditions:

We assume that $D \subset G$ is a (v, k, λ) difference set where is a subgroup $1 \neq H \leq G$ and $m \geq 0$ such that
(1) $D \cap D^{-1} = Hg_1 \cup \cdots \cup Hg_m$;
(2) $G \setminus (D \cup D^{-1}) = H \cup Hg'_1 \cup \cdots \cup Hg'_m$.

Here $H, Hg_1, \ldots, Hg_m, Hg'_1, \ldots, Hg'_m$ are distinct cosets of H. Let

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

Then we have $h > 1$. Following Webster [23], who considers the $m = 0$ case, a group having a difference set of the above type will be called a $(v, k, \lambda)_m$ *DRAD difference set group* (with difference set D and subgroup H). See also [5, 15, 16] for more on DRADs.

Recall that a group G has a *skew Hadamard difference set* if it has a difference set D where $G = D \cup D^{-1} \cup \{1\}$ and $D \cap D^{-1} = \emptyset$. Such groups have been studied in [2, 3, 4, 5, 7, 8, 9, 10, 12].

Theorem 1.1. *Let G be a $(v, k, \lambda)_m$ DRAD difference set group with subgroup H and difference set D. Then* *(i) $m = 0, h = u$ is even, $v = |G| = h^2$, and*

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

(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.

We note that Davis and Polhill [5] consider such difference sets, however, they are mostly concerned with the abelian case, where H is always normal. They also note (iii) of Theorem 1.1.

Let $\Phi(G)$ be the Frattini subgroup of G, the intersection of all the maximal subgroups of G. We have the following result concerning maximal subgroups of G:

Theorem 1.2. *Let G be a group that is a $(v, k, \lambda)_0$ DRAD difference set group with subgroup H and difference set D. Then*
(a) If $K \leq G, |G : K| = 2$, then $H \leq K$ and $|K \cap D| = \lambda$.
(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.

Our original motivation for studying $(v, k, \lambda)_0$ DRAD difference set groups was to produce examples of Schur rings with a small number of principal sets.

We now define Schur rings [20, 21, 24, 25]. 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 the following hold:
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 $\mathfrak{S}$. Then we have:

Theorem 1.3. *Let G be a $(v, k, \lambda)_0$ DRAD 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 1.3 allows us to show

Theorem 1.4. *Let G be a $(v, k, \lambda)_0$ DRAD difference set 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

$$1, \;\; h-1, \;\; h(h-1)/2, \;\; , h(h-1)/2 \;\; \textit{(respectively)}.$$

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

Theorem 1.5. *Let G be a $(v, k, \lambda)_0$ difference set 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 the following (up to similarity):*

(i) $\rho(H) = 0I_d$ *and* $\rho(D) = \operatorname{diag}\left(\varepsilon_1 i\frac{h}{2}, \varepsilon_2 i\frac{h}{2}, \ldots, \varepsilon_d i\frac{h}{2}\right)$, *for some* $\varepsilon_i \in \{-1, 1\}$*;*
(ii) $\rho(H) = hI_d$ *and* $\rho(D) = -\frac{h}{2}I_d$*.*

We next give examples of families of $(v, k, \lambda)_0$ DRAD difference set groups. Let $n \geq 2, 0 \leq k < n-1$ and define the following bi-infinite family of groups:

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

We will show:

Theorem 1.6. *For* $n \geq 2, 0 \leq k < n-1$*, the group* $\mathfrak{G}_{n,k}$ *is a DRAD difference set group with* $H = \langle b_1, \ldots, b_n \rangle$*.*

We note that in [5, Theorem 1.6] the authors show a similar result for abelian groups containing a $\mathcal{C}_2^n$ subgroup. The main point of [5] is to construct Doubly Regular Asymmetric Digraphs (DRADs), and they show that a difference set D determines a DRAD if $1_G \notin D$; and (ii) $D \cap D^{-1} = \emptyset$. Thus any DRAD difference set group will determine a DRAD. Thus Theorem 1.6 gives examples of DRADs that come from non-abelian groups.

We also note that the only such groups that we have found are 2-groups. If G is abelian we can show:

Theorem 1.7. *(i) Any abelian group that is a DRAD difference set group is a 2-group.*

(ii) Let G be an abelian DRAD difference set group of order h^2. Then the exponent of G is at most h.

We note results of Kraemer, Jedwab, and Turyn [19, 17, 22] that says that a group of order 2^{2d+2} with a difference set must have exponent no more than 2^{d+2}. Thus the bound for DRAD difference set groups is smaller than their general bound.

Acknowledgements We are grateful to Pace Nielsen for useful conversations regarding this paper, and also to an anonymous referee for useful comments, of notifying us of reference [5] and a proof that $m = 0$. All calculations made in the preparation of this paper were accomplished using Magma [1].

§2 Results concerning the parameters

In this section we first show: $m = 0, h = u$ is even, $|G| = h^2$ and $\lambda = \frac{1}{4}h(h-2), \quad k = \frac{1}{2}h(h-1)$. Let

$$A = Hg_1 \cup \cdots \cup Hg_m, \quad B = Hg_1' \cup \cdots \cup Hg_m',$$

and $D = A + D_1, D^{-1} = A + D_1^{-1}$, where $A \cap D_1 = \emptyset$. Thus we have

$$|A| = |B| = hm, \quad |D| = k = hm + |D_1|.$$

Then from (1) and (2) of §1 we obtain $G = H + B + D_1 + A + D_1^{-1}$. Thus we have

$$v = |G| = h + hm + |D_1| + hm + |D_1^{-1}| = h + 2hm + 2|D_1| = h + 2k.$$

Solving $v = hu, k(k-1) = \lambda(v-1), v = h + 2k$ gives $\lambda = \frac{1}{4}\frac{(hu-h)(hu-h-2)}{hu-1}$. Let

$$a = \gcd(hu - h, hu - 1),\ b = \gcd(hu - h - 2, hu - 1). \tag{2.1}$$

Then one can see that $a = \gcd(h-1, u-1), \quad b = \gcd(h+1, u+1)$. Thus $\gcd(a, b)|2$ since $a|(h-1), b|(h+1)$ and $h > 1$.

We wish to show that $h = u$. Now if we have $h < u$, then we cannot have $(u+1)|(h+1)$, so that we have $ab \leq (h-1)(u+1)/2$. This gives

$$ab \leq \frac{1}{2}(h-1)(u+1) = \frac{1}{2}(hu - 1 + h - u) < \frac{1}{2}(hu-1).$$

While if $h > u$, then we cannot have $(h+1)|(u+1)$, so that $ab \leq (u-1)(h+1)/2$, giving

$$ab \leq \frac{1}{2}(u-1)(h+1) = \frac{1}{2}(hu - 1 + u - h) < \frac{1}{2}(hu-1).$$

Thus in both cases we get $ab < \frac{1}{2}(hu-1)$. We show this gives a contradiction.
Case 1: $\gcd(a, b) = 1$. Then $a|(hu-1), b|(hu-1)$ and $\gcd(a, b) = 1$ gives $ab|(hu-1)$. So let $hu - 1 = abc, c \in \mathbb{N}$. Then from (2.1) we have

$$\gcd\left(\frac{hu-h}{a}, c\right) = \gcd\left(\frac{hu-h-2}{b}, c\right) = 1,$$

so that

$$\lambda = \frac{1}{4}\frac{(hu-h)(hu-h-2)}{hu-1} = \frac{1}{4}\frac{(hu-h)}{a}\frac{(hu-h-2)}{b}\frac{1}{c},$$

which implies that $c = 1$. But then we have $ab = hu - 1 > \frac{hu-1}{2}$, a contradiction.
Case 2: $\gcd(a, b) = 2$. Then $(ab/2)|(hu-1)$, so that $hu - 1 = \frac{ab}{2}c, c \in \mathbb{N}$, where $\gcd\left(\frac{hu-h}{a}, c\right) = \gcd\left(\frac{hu-h-2}{b}, c\right) = 1$. Then

$$\lambda = \frac{1}{4}\frac{(hu-h)(hu-h-2)}{hu-1} = \frac{1}{2}\frac{(hu-h)}{a}\frac{(hu-h-2)}{b}\frac{1}{c}.$$

Thus again $c = 1$, so that $\frac{ab}{2} = hu - 1$, a contradiction. So $h = u$ and $v = h^2$.

Now if $h = u$, then we have

$$\lambda = \frac{(h^2-h)(h^2-h-2)}{4(h^2-1)} = \frac{h(h-1)(h-2)(h+1)}{4(h-1)(h+1)} = \frac{h(h-2)}{4},$$

so that h is even.

We next show that $m = 0$. The *intersection numbers* are $|Hg_i \cap D|$, where $g_1, \dots, g_h$ are coset representatives for G/H. Let $m_i, 0 \leq i \leq h$, be the number of intersection numbers of size i. Then we have

$$\sum_{i=0}^{h} m_i = h, \quad \sum_{i=0}^{h} i m_i = k = \frac{1}{2}h(h-1), \quad \sum_{i=0}^{h} i^2 m_i = k - \lambda + \lambda h = \frac{1}{4}h^2(h-1),$$

where the last equation comes from [11, Theorem 7.1]. Using these equations one shows that

$$T := \sum_{i=0}^{h}\left(i - \frac{h}{2}\right)\left(i - \left(\frac{h}{2} - 1\right)\right) m_i = \frac{1}{4}h(h-2).$$

We note that each summand of T is non-negative. Now from (1) of §1 we see that $m_h \geq m$. Thus if $m > 0$, then $m_h > 0$. Now if $m_h > 0$, then the contribution to T for $i = h$ is

$$\frac{h}{2}\left(\frac{h}{2} + 1\right) m_h \geq \frac{h}{2}\left(\frac{h}{2} + 1\right) > \frac{1}{4}h(h-2) = T,$$

which is a contradiction. This concludes the proof of Theorem 1.1 (i).

§3 H is normal

Let D be the difference set where $G = D \cup D^{-1} \cup H, H \leq G, D \cap H = D \cap D^{-1} = \emptyset$. Order the elements of G according to the cosets $Hg_1, Hg_2, \ldots, Hg_h$.

Then thinking of D, H and G as matrices via the regular representation (relative to the above order of G) we have

$$G = D + D^{-1} + H, \qquad D \cdot D^{-1} = \lambda G + (k - \lambda) \cdot 1. \tag{3.1}$$

Note that the fact that D^{-1} is also a difference set [11, p. 57], together with the last equation of (3.1), gives $DD^{-1} = D^{-1}D$.

For $m \in \mathbb{N}$ let J_m be the all 1 matrix of size $m \times m$. Then we have ordered the elements of G so that $H = \operatorname{diag}(J_h, J_h, \ldots, J_h)$. So solving for D^{-1} from the first equation of (3.1), and using $DG = kG$, the second equation gives

$$(k - \lambda)(G - 1) = D^2 + DH. \tag{3.2}$$

However (since D^{-1} is also a difference set) we can interchange D and D^{-1} so as to obtain

$$(k - \lambda)(G - 1) = (D^{-1})^2 + D^{-1}H. \tag{3.3}$$

Now taking the inverse of equation (3.2) we have

$$(k - \lambda)(G - 1) = (D^{-1})^2 + HD^{-1}. \tag{3.4}$$

Thus from equations (3.3) and (3.4) we must have $D^{-1}H = HD^{-1}$; taking inverses gives $DH = HD$.

Thus D commutes with G, H, D^{-1}. Now multiplying $(k - \lambda)(G - 1) = D^2 + HD$ by H we obtain

$$(k - \lambda)(hG - H) = D \cdot DH + hHD.$$

Multiplying by H again we have

$$h(k - \lambda)(hG - H) = (DH)^2 + h^2(DH). \tag{3.5}$$

We now find the minimal polynomial for DH, by first finding the minimal polynomial for $hG - H$. A calculation shows that

$$(hG - H)^2 = h^2(h^2 - 2)G + hH,$$
$$(hG - H)^3 = h^3(h^4 - 3h^2 + 3)G - h^2H.$$

Thus $(hG - H), (hG - H)^2, (hG - H)^3$ are in the span of H, G and so are linearly dependent. Define

$$F(x) = x(x + h)(x - h^3 + h).$$

Then one finds that

$$F(hG - H) = 0. \tag{3.6}$$

Now let $\Delta = DH$. Then from (3.5) we have

$$hG - H = \frac{1}{h(k - \lambda)}(\Delta^2 + h^2\Delta). \tag{3.7}$$

It follows from (3.6), (3.7) that Δ satisfies the polynomial

$$x\left(x + h^2\right)\left(2x + h^2 + h^3\right)\left(2x + h^2 - h^3\right)\left(2x + h^2\right)^2.$$

For $n \in \mathbb{N}$ we let $1_n = (1, 1, \ldots, 1), 0_n = (0, 0, \ldots, 0) \in \mathbb{R}^n$. Now from equation (3.5) and the definition of the function F we see that:

(A) the matrix $hG - H$ has eigenvalue $\mu = h^3 - h$ with an eigen space containing 1_{h^2}.

(B) the matrix $hG - H$ has eigenvalue $\mu = -h$ with corresponding eigenspace containing the span of

$$(1_h, 0_h, 0_h, \dots, 0_h, -1_h), (0_h, 1_h, 0_h, \dots, 0_h, -1_h), \dots, (0_h, 0_h, 0_h, \dots, 0_h, 1_h, -1_h),$$

so that this eigenspace has dimension at least $h - 1$.

(C) Lastly, $hG - H$ has eigenvalue $\mu = 0$ with corresponding eigenspace containing the span of all vectors of the form $(v_1, v_2, \dots, v_h)$, where $v_i \in \mathbb{R}^h$ satisfies $J_h v_i = 0$. Thus this eigenspace has dimension at least $h^2 - h$.

Since $1 + (h - 1) + (h^2 - h) = h^2$ we see that (A), (B), (C) describe all the eigenspaces, and we conclude that $hG - H$ is diagonalizable.

The eigenvalues for $(k - \lambda)h(hG - H)$ are thus

$$\mu' = (k - \lambda)h^2(h^2 - 1), \quad \mu' = -h^2(k - \lambda), \quad \mu' = 0,$$

with corresponding eigenspaces $E_{\mu'}$, as given in (A), (B), (C).

Let $g_1 = 1, g_2, \dots, g_h$ be coset representatives for G/H. Let $d_i = |D \cap Hg_i|$, so that $d_1 = 0$. Let $D = (D_{ij})$, where the blocks are of size $h \times h$ and are $\{0, 1\}$ matrices. Now from $DH = HD$ we see that $J_h D_{ij} = D_{ij} J_h$ for all $1 \le i, j \le h$.

Lemma 3.1. *Let A be an $h \times h$ matrix whose entries are $0, 1$, and such that $J_h A = A J_h$. Then every row and column of A has the same number of 1s in it.*

Proof Note that the kth column of $J_h A$ is $u(1, 1, \dots, 1)^T$, where u is the number of 1s in the kth column of A. Similarly, the kth row of AJ_h is $u(1, 1, \dots, 1)$, where u is the number of 1s in the kth row of A.

Let $a_i, 1 \le i \le h$, be the number of 1s in the ith row of A. Then the ith row of AJ_h is $(a_i, a_i, \dots, a_i)$. Thus

$$J_h A = \begin{pmatrix} a_1 & a_1 & \dots & a_1 \\ a_2 & a_2 & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_h & a_h & \dots & a_h \end{pmatrix}.$$

Let $b_i, 1 \le i \le h$ be the number of 1s in the ith column of A. Then the ith column of $J_h A = AJ_h$ is $(b_i, b_i, \dots, b_i)^T$, so that we have

$$AJ_h = \begin{pmatrix} b_1 & b_2 & \dots & b_h \\ b_1 & b_2 & \dots & b_h \\ \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & \dots & b_h \end{pmatrix}.$$

Since $AJ_h = J_h A$ we see from the first column and first row of these matrices that

$$b_1 = a_1 = a_2 = \cdots = a_h, \quad a_1 = b_1 = b_2 = \cdots = b_h.$$

Thus $a_i = a_j = b_r = b_s$ for all $1 \le i, j, r, s \le h$, and the result follows. □

Thus from $HD_{ij} = D_{ij}H$ we see that each row and column of D_{ij} has the same number of 1s in it. Let this number be d_{ij}, so that $d_{ii} = 0$. Thus $DH = HD = (d_{ij} J_h)$.

Now $DD^{-1} = D^{-1}D$ with $D^{-1} = D^T$ shows that D is a normal matrix. Clearly H is a normal matrix. Thus we have

Lemma 3.2. *The matrices D, H, G are commuting normal matrices and are simultaneously diagonalizable.* □

In particular DH is diagonalizable. Next: if α is an eigenvalue for $\Delta = DH$ with eigenvector v, then

$$(\Delta^2 + h^2\Delta)v = (\alpha^2 + h^2\alpha)v.$$

But $\Delta^2 + h^2\Delta = (k-\lambda)h(hG - H)$, which shows that v is also an eigenvector for $(k-\lambda)h(hG-H)$ with eigenvalue $\alpha^2 + h^2\alpha$. However we know the eigenvalues and eigenvectors for $(k-\lambda)h(hG-H)$. Thus there are three cases:

(A) Here $\alpha^2 + h^2\alpha = (k-\lambda)h^2(h^2-1)$, in which case we solve for α: $\alpha = \frac{1}{2}\left(\pm h^3 - h^2\right)$. Here the eigenvector is 1_{h^2}. Since $\Delta^2 + h^2\Delta$ is a matrix with non-negative entries it follows that $\frac{1}{2}\left(-h^3 - h^2\right)$ is not possible with this eigenvector. Thus we only have $\frac{1}{2}\left(h^3 - h^2\right)$ as an eigenvalue in this case.

(B) Here $\alpha^2 + h^2\alpha = -(k-\lambda)h^2$, so that $\alpha = -h^2/2$.

(C) Here $\alpha^2 + h^2\alpha = 0$, so that $\alpha = 0, -h^2$.

Since DH is diagonalizable the dimensions of the eigenspaces in cases (A), (B), (C) must be $1, h-1, h^2-h$ (respectively). In particular, each eigenvector for $hG-H$ as in (B) is also an eigenvector for DH. Thus we have

$$\begin{pmatrix} 0 & d_{12}J_h & d_{13}J_h & \dots & d_{1h}J_h \\ d_{21}J_h & 0 & d_{23}J_h & \dots & d_{2h}J_h \\ d_{31}J_h & d_{32}J_h & 0 & \dots & d_{3h}J_h \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{h1}J_h & d_{h2}J_h & d_{h3}J_h & \dots & 0 \end{pmatrix} \begin{pmatrix} 1_h \\ 0_h \\ 0_h \\ \vdots \\ -1_h \end{pmatrix} = -\frac{h^2}{2} \begin{pmatrix} 1_h \\ 0_h \\ 0_h \\ \vdots \\ -1_h \end{pmatrix},$$

which, since $J_h 1_h = h 1_h$, gives

$$d_{1h} = \frac{h}{2}, d_{21} = d_{2h}, d_{31} = d_{3h}, \dots, d_{h-1,1} = d_{h-1,h}, d_{h1} = \frac{h}{2}.$$

Similarly, using

$$\begin{pmatrix} 0 & d_{12}J_h & d_{13}J_h & \dots & d_{1h}J_h \\ d_{21}J_h & 0 & d_{23}J_h & \dots & d_{2h}J_h \\ d_{31}J_h & d_{32}J_h & 0 & \dots & d_{3h}J_h \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{h1}J_h & d_{h2}J_h & d_{h3}J_h & \dots & 0 \end{pmatrix} \begin{pmatrix} 0_h \\ 1_h \\ 0_h \\ \vdots \\ -1_h \end{pmatrix} = -\frac{h^2}{2} \begin{pmatrix} 0_h \\ 1_h \\ 0_h \\ \vdots \\ -1_h \end{pmatrix},$$

we obtain

$$d_{12} = d_{1h} = \frac{h}{2}, d_{2h} = \frac{h}{2} = d_{21}, d_{32} = d_{3h} = d_{31}, \dots,$$
$$d_{h-1,2} = d_{h-1,h} = d_{h-1,1}, d_{h2} = \frac{h}{2}.$$

Continuing we see that $d_{ij} = \frac{h}{2}$ for all $1 \le i \ne j \le h$.

This shows that $|D \cap gH| = \frac{h}{2}$ for all $g \notin H$, and so also gives

$$DH = HD = \frac{h}{2}(G - H). \tag{3.8}$$

Proposition 3.3. *Let $H \leq G, |H| = h, |G| = n$, and order the elements of G according to the cosets of H as in the above. Represent elements of G using the regular representation relative to this ordering. Then for $g \in G$ we write $g = (g_{ij})$, where each g_{ij} is a $0, 1$ matrix of size $h \times h$. Then $H \triangleleft G$ if and only if for all $g \in G$ and all $1 \leq i, j \leq n/h$ each g_{ij} is either the zero matrix or is a permutation matrix.*

Proof We note that $H \triangleleft G$ if and only if for all $g \in G$ we have $Hg = gH$, where $H = \mathrm{diag}(J_h, J_h, \ldots, J_h)$.

Assume that $H \triangleleft G, g \in G, g = (g_{ij})_{1 \leq i,j \leq h}$, where each g_{ij} is an $h \times h$ matrix. Then $gH = Hg$ implies that $g_{ij} J_h = J_h g_{ij}$ for all $1 \leq i, j \leq n/h$. By Lemma 3.1 this is true if and only if all the rows and columns of g_{ij} have the same number of 1s in them. Since each row and column of g has exactly one 1 in it (the rest of the entries being 0) we see that if $g_{ij} \neq 0$, then each row and column of g_{ij} has exactly one 1 in it. Thus, for fixed i, j, no other $g_{ik}, k \neq j$, or $g_{kj}, k \neq i$, can be non-zero. In particular, each g_{ij} is a permutation matrix.

Now assume that for all $g \in G$ and all $1 \leq i, j \leq n/h$ each g_{ij} is either the zero matrix or is a permutation matrix. We wish to show that $H \triangleleft G$ i.e. that $g_{ij} J_h = J_h g_{ij}$ for all $1 \leq i, j \leq n/h$. This is certainly true if $g_{ij} = 0$, while if g_{ij} is a permutation matrix, then $g_{ij} J_h = J_h = J_h g_{ij}$, and so we are done. $\square$

Let D denote a difference set where $G = D \cup D^{-1} \cup H, H \leq G, D \cap H = D \cap D^{-1} = \emptyset$. We now wish to show that $H \triangleleft G$.

From the above we know that $|G| = h^2, h = |H|$, where h is even and $D = (d_{ij})$, where either $D_{ij} = 0$ or D_{ij} is a $0, 1$ matrix that has $h/2$ 1s in each row and column. We wish to show that $gH = Hg$ for all $g \in G$. This is certainly true if $g \in H$, so assume that $g \notin H$. Write $g = (g_{ij})$ as in the above. Since $g \notin H$ we either have $g \in D$ or $g \in D^{-1}$. Without loss of generality we can assume that $g \in D$. Now either $D_{ij} = 0$ or D_{ij} is a $0, 1$ matrix that has $h/2$ 1s in each row and column, so either $g_{ij} = 0$ or g_{ij} is a $0, 1$ matrix that has one 1 in each row and column. It follows that $g_{ij} J_h = J_h g_{ij}$, and so $H \triangleleft G$. $\square$

We have thus proved Theorem 1.1 (i), (ii), (iii). For Theorem 1.1 (iv) we note that if $g \in G$ is an involution that is not in H, then $g \in D \cap D^{-1}$, a contradiction.

For Theorem 1.1 (v) we show that $H \triangleleft G$ does not have a complement. So suppose that $L \leq G$ is a complement to H. Now since L is a complement to H we have $|L| = |G|/|H| = h$, which is even. Thus L contains an involution that is not in H, a contradiction. This now concludes the proof of Theorem 1.1. $\square$

§4 H AND SUBGROUPS OF INDEX 2

We prove Theorem 1.2 (i). From Theorem 1.1 we know that $|G| = h^2, k = \frac{h(h-1)}{2}, \lambda = \frac{h(h-2)}{4}$. Let $M \leq G$ be a subgroup of index 2 and let $\pi : G \to G/M = \langle t : t^2 = 1 \rangle$ be the quotient map. Let $|D \cap M| = d_1, |H \cap M| = h_1$, so that

$$\pi(D) = d_1 \cdot 1 + (k - d_1)t, \quad \pi(H) = h_1 \cdot 1 + (h - h_1)t.$$

Let $d_2 = k - d_1, h_2 = h - h_1$. Then we have the equations

$$d_1 + d_2 = k, \quad h_1 + h_2 = h, \quad k = h(h-1)/2, \quad \lambda = h(h-2)/4. \tag{4.1}$$

Now from equations (3.2) and (3.8) we deduce that $D^2 = \lambda G + \frac{h}{2} H - (k - \lambda)1$. Taking the image of this under π, and using the fact that $\pi(D) = d_1 1 + d_2 t$, we obtain two equations (by looking at the coefficients of 1 and t):

$$d_1^2 + d_2^2 = \lambda h^2/2 + hh_1/2 + \lambda - k; \quad 2d_1 d_2 = \lambda h^2/2 + hh_2/2. \tag{4.2}$$

Now $D + D^{-1} = G - H$ gives (by acting by π)

$$2d_1 + 2d_2 t = h^2/2(1+t) - (h_1 + h_2 t),$$

which gives

$$2d_1 = h^2/2 - h_1, \quad 2d_2 = h^2/2 - h_2. \tag{4.3}$$

Solving equations (4.1), (4.2), (4.3) we find that

$$h_1 = h, \quad h_2 = 0, \quad d_1 = \lambda, \quad d_2 = k - \lambda.$$

Thus D meets M in λ points, and all of H is in M. Since this is true for any maximal subgroup M we see that H is contained in the Frattini subgroup if G is a 2-group, since every maximal subgroup of such a group has index 2. This gives Theorem 1.2 (b). □

§5 The Schur ring and minimal polynomials

We have $(G-H)^{-1} = G - H, (H-1)^{-1} = H - 1, (D^{-1})^{-1} = D$, and so we just need to show that $D, D^{-1}, H-1, 1$ commute and span the ring that they generate. We have already seen in Lemma 3.2 that they commute. We have $H \cdot G = hG, D \cdot G = kG = D^{-1} \cdot G$. Using equations (3.2) and (3.8) we get

$$D^2 = (k-\lambda)(G-1) - \frac{h}{2}(G-H).$$

We collect together the rest of the products that we need:

$$\begin{aligned} &HD = DH = \frac{h}{2}(G-H); \quad H^2 = hH, \\ &D^2 = (k-\lambda)(G-1) - \frac{h}{2}(G-H) = (k - \lambda - \frac{h}{2})(D + D^{-1}) + (k-\lambda)(H-1), \\ &D \cdot D^{-1} = D^{-1} \cdot D = \lambda G + (k-\lambda)1 = \lambda D + \lambda D^{-1} + \lambda(H-1) + k1. \end{aligned}$$

Since $k = h(h-1)/2, \lambda = h(h-2)/4, k - \lambda = h^2/4 \in \mathbb{Z}$, one can check that all the coefficients in the above sums are non-negative integers. This proves that $D, D^{-1}, H-1, 1$ commute and span the ring that they generate. Theorem 1.3 follows. □

For a matrix or an element M of an algebra we let $\mu(M)$ denote the minimal polynomial of M. To help us find $\mu(D)$ we have the equations

$$\begin{aligned} &G = D + D^{-1} + H, \quad DD^{-1} = \lambda G + (k-\lambda), \quad DH = \frac{h}{2}(G-H), \\ &D^{-1}H = \frac{h}{2}(G-H), \quad D^2 = (k-\lambda)(G-1) - \frac{h}{2}(G-H). \end{aligned}$$

Using these one can show that

$$\begin{aligned} D^3 &= \frac{h^2}{4} D^{-1} + \left(\frac{1}{8}h^4 - \frac{3}{8}h^3 + \frac{1}{4}h^2\right) G; \\ D^4 &= \left(\frac{1}{16}h^6 - \frac{1}{4}h^5 + \frac{3}{8}h^4 - \frac{1}{4}h^3\right) G + \frac{1}{16}h^4. \end{aligned}$$

Using these relations one finds that D satisfies the polynomial $(x-k)\left(x+\frac{h}{2}\right)\left(x^2+\frac{h^2}{4}\right)$. Thus $\mu(D)$ divides this polynomial.

We note that $\frac{1}{k}D$ is a stochastic matrix, and since $D^2=(k-\lambda)(G-1)-\frac{h}{2}(G-H)$ it follows that

Lemma 5.1. *The matrix $\frac{1}{k}D$ is an irreducible doubly stochastic matrix.* □

Further, we know that $\mu(D)$ factors as a product of distinct linear factors $(x-\kappa)$, where κ is an eigenvalue (since D is diagonalizable by Lemma 3.2).

Next we note that k is an eigenvalue of D, since each row sum and column sum of D is k. Next we show that $-h/2$ is an eigenvalue of D: for $g \notin H$ we have $H-Hg \neq 0$ and

$$\begin{aligned} D\cdot(H-Hg) = DH(1-g) &= \frac{h}{2}(G-H)(1-g) \\ &= \frac{h}{2}(G-H-G+Hg) = -\frac{h}{2}(H-Hg). \end{aligned}$$

Thus $-\frac{h}{2}$ is an eigenvalue for D.

Since D is a matrix with real entries it follows that the eigenspaces for eigenvalues $\pm ih/2$ have the same dimension, and that either $\mu(D)=(x-k)(x+h/2)$ or $\mu(D)=(x-k)(x+h/2)(x^2+\frac{h^2}{4})$. If $\mu(D)=(x-k)(x+h/2)$, then, since D is diagonalizable, Lemma 5.1 and the Perron Frobenius theorem show that D has eigenvalue k with multiplicity one, and $-h/2$ with multiplicity h^2-1. Now, since $D\cap H=\emptyset$, we see that D has trace zero. Thus we must have

$$k+(h^2-1)(-h/2)=0,$$

but the lefthand side of this expression is $-h^2(h-1)$, which gives a contradiction. Thus $\mu(D)=(x-k)(x+h/2)(x^2+\frac{h^2}{4})$. In fact it easily follows from $\mathrm{Trace}(D)=0$ that the eigenvalue $-h/2$ has multiplicity $h-1$. □

This gives a proof of Theorem 1.4. □

§6 Examples of DRAD difference set groups

The groups $\mathfrak{G}_{n,k}$ have been defined in the introduction. We now show that they are DRAD difference set groups with $H=\langle b_1,b_2,\dots,b_n\rangle$. Then a transversal for H in G is the set of products $a_{i_1}a_{i_2}\cdots a_{i_u}$, where these are indexed by the sequences $i_1<i_2<\cdots<i_u$ of $1,2,\dots,n$, or in other words, indexed by the subsets $X=\{i_1,i_2,\dots,i_u\}$ of $\{1,2,\dots,n\}$. We let $a_X=a_{i_1}a_{i_2}\cdots a_{i_u}$ denote the corresponding element of G. Here $a_\emptyset=1$. We may also employ a similar notation for the elements $b_X=b_{i_1}b_{i_2}\cdots b_{i_u}$.

We note that for any $g\in G$ we have $g^2\in H$. We are interested in the hypothesis (H1): there is a set of distinct maximal subgroups $M_1,\dots,M_{2^n-1}$ of H, and an ordering $S_1,\dots,S_{2^n-1}$ of the non-empty subsets of $\{1,\dots,n\}$ so that $a_{S_i}^2\notin M_i$.

Proposition 6.1. *The groups $\mathfrak{G}_{n,k}$ satisfy (H1).*

Proof We first show that the squares of the coset representatives $a_S, S\subseteq\{1,2,\dots,n\}$, are distinct. We note that the subgroup $J=\langle a_2,a_3,\dots,a_n\rangle$ is isomorphic to $\mathcal{C}_4^{n-1}$. We also have $J\lhd\mathfrak{G}_{n,k}$, so that $\mathfrak{G}_{n,k}=J\rtimes\langle a_1\rangle=J\rtimes\mathcal{C}_4$.

If $S \subseteq \{1, 2, \ldots, n\}$ and $m \in \mathbb{Z}$ we let $S + m$ be the set $\{u + m : u \in S\}$, where we take numbers mod n so that $S + m \subseteq \{1, 2, \ldots, n\}$.

Now for a coset representative $a_S, S = \{i_1, i_2, \ldots, i_u\} \subseteq \{2, \ldots, n\}$, we have $a_S \in J$ and so from the relations in $\mathfrak{G}_{n,k}$ we have

$$a_S^2 = b_{i_1+k} b_{i_2+k} \ldots b_{i_u+k} = b_{S+k}.$$

We note that in this situation, since $1 \notin S$, we have $1 + k \notin S + k$.

Now for a coset representative a_S that is not in J we can write $S = \{1, i_1, i_2, \ldots, i_u\}$, where $a_{S \setminus \{1\}} \in J$. So if we let $K = S \setminus \{1\}$, then $a_S = a_1 a_K$.

Now write $K = K_1 \cup K_2$, where the elements $a_m, m \in K_2$, commute with a_1, and those $a_m, m \in K_1$, do not. Note that

$$K_1 \subseteq \{2, \ldots, k+1\}, \quad K_1 \cap K_2 = \emptyset, \quad S = \{1\} \cup K_1 \cup K_2.$$

Then from the relations in $\mathfrak{G}_{n,k}$ we have: $a_{K_2}^{a_1} = a_{K_2}, a_{K_1}^{a_1} = a_{K_1} b_{K_1-1}$. Thus we have

$$\begin{aligned} a_S^2 = (a_1 a_{K_1} a_{K_2})^2 &= a_1^2 a_{K_1}^{a_1} a_{K_1} a_{K_2}^2 = b_{1+k} \cdot a_{K_1} b_{K_1-1} \cdot a_{K_1} \cdot a_{K_2}^2 \\ &= b_{1+k} b_{K_1-1} b_{K_1+k} b_{K_2+k} = b_{K_1-1} b_{S+k}. \end{aligned} \tag{7.1}$$

We next show that b_{1+k} has non-zero exponent in (7.1). But from the above we know that $K_1 \subseteq \{2, 3, \ldots, k+1\}$, so that $1 + k \notin K_1 - 1$. If $1 + k \in K_i + k, i = 1, 2$, then $1 \in K_i$, a contradiction. This shows that b_{1+k} has non-zero exponent in (7.1).

Note that in the above we have also shown (i) of

Lemma 6.2. *With the above definitions we have:*
(i) the element b_{1+k} occurs with non-zero coefficient in a_S^2 if and only if $1 \in S$.
(ii) The squares $a_S^2, S \subseteq \{1, 2, \ldots, n\}$, where $1 \in S$, are distinct.

Proof (ii) We need to show that the map $S \mapsto b_{K_1-1} b_{S+k}$ is injective.

We represent S as a (column) vector $v_S \in V = \mathbb{F}_2^n$, where the ith coordinate of v_S is 1 if and only if $i \in S$. Then the action on V of replacing S by $S + 1$ is determined by the $n \times n$ permutation matrix

$$P = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

Thus for any $i \in \mathbb{Z}$ we have

$$v_{S+i} = P^i v_S.$$

Let $0_{k,m}$ denote the $k \times m$ zero matrix, and let $0_k = 0_{k,k}$. If $k \leq 0$ or $m \leq 0$, then $0_{k,m}$ will be the empty matrix. Then, the map $S \mapsto K_1$, is determined by the $n \times n$ matrix

$$A = \mathrm{diag}(0_1, I_k, 0_{n-k-1}),$$

so that $v_{K_1} = A v_S$.

Thus the map $S \mapsto b_{K_1-1} b_{S+k}$ is represented by the matrix $P^{-1}A + P^k$, and we will be done if we can show that $P^{-1}A + P^k$ is a non-singular matrix in $\mathrm{GL}(2, \mathbb{F}_2)$.

But this is the same as showing that $B := A + P^{k+1}$ is non-singular, where

(7.2)
$$B = \begin{pmatrix} 0_1 & 0_{1,k} & 0_{1,n-k-1} \\ 0_{k,1} & I_k & 0_{k,n-k-1} \\ 0_{n-k-1,1} & 0_{n-k-1,k} & 0_{n-k-1} \end{pmatrix} + \begin{pmatrix} 0_{1,n-k-1} & 1 & 0_{1,k} \\ 0_{k,n-k-1} & 0_{k,1} & I_k \\ I_{n-k-1} & 0_{n-k-1,1} & 0_{n-k-1,k} \end{pmatrix}.$$

We note that since $k < n-1$ the second matrix is not a diagonal matrix, and that the submatrix I_k in the second matrix of equation (7.2) occurs to the right of the diagonal. (This shows that $A + P^{k+1}$ is singular when $k = n-1$.) Thus the I_k in the second matrix of equation (7.2) can be used to column-reduce the I_k in the first matrix to zero. This shows that $A + P^{k+1}$ column-reduces to P^{k+1}, which is non-singular, and we are done. □

Let $V^\times = \mathbb{F}_2^n \setminus \{0\}$. Then non-empty subsets of S correspond bijectively to elements of $V^\times$, as explained above. Further, maximal subgroups of H correspond to subspaces of V of dimension $n-1$, which, in turn, are determined by elements of $V^\times$: a vector $v \in V^\times$ determines the subspace $M_v = \{u \in V | u \cdot v = 0\}$, where $\cdot$ is the usual dot-product on V taking values in $\mathbb{F}_2$. Since V is a vector space over $\mathbb{F}_2$ the correspondence $v \leftrightarrow M_v$ is bijective. Further, given a maximal subgroup (or subspace) M we let v_M denote the corresponding vector.

Thus the correspondence of subsets with maximal subgroups that we require is $S \leftrightarrow M_S$ 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 a function

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

Conversely, such a function determines the correspondence that we want. We now show how to construct such a function:

Lemma 6.3. *For all $n \in \mathbb{N}, V = \mathbb{F}_2^n$, there is a function $\mu : V^\times \to V^\times$ such that $u \cdot \mu(u) = 1$ for all $u \in V^\times$.*

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

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

where there are k 1s (so for $k = 0$ we have the zero vector of V).

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

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

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

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

This defines a function μ that is an involution. □

Lemma 6.3 determines the pairing for hypothesis (H1) for the groups $\mathfrak{G}_{n,k}$, and concludes the proof of Proposition 6.1. □

We will next show

Proposition 6.4. *The groups $\mathfrak{G}_{n,k}$ are DRAD difference set groups.*

Proof We first note that since $b_1, \dots, b_n$ are central involutions, all the maximal subgroups of H are normal subgroups of G.

As usual, subsets S of G will correspond to elements $\sum_{s \in S} s$, of the group algebra. We define D as follows:

$$D = \sum_{i=1}^{2^n - 1} a_{S_i} M_i.$$

Let $a_i = a_{S_i}$. We first show that $(a_i M_i)^{-1} = a_i(H - M_i)$. But this is true if and only if $a_i^{-1} M_i = a_i(H - M_i)$ if and only if $M_i = a_i^2(H - M_i)$ if and only if $M_i = H - a_i^2 M_i$. But this latter equation is true since $a_i^2 \in H$ and $a_i^2 \notin M_i$.

Thus we have:

$$D^{-1} = \sum_{i=1}^{2^n - 1} a_{S_i}(H - M_i).$$

Let $1 \leq i \neq j \leq 2^n - 1$; then, since M_i, M_j are distinct maximal subgroups of $H \cong \mathcal{C}_2^n$, we have $M_i M_j = 2^{n-2} H$, so that for $1 \leq i \neq j \leq 2^n - 1$ we have

$$M_i(H - M_j) = 2^{n-1} H - 2^{n-2} H = 2^{n-2} H.$$

We use this to obtain:

$$\begin{aligned}
D \cdot D^{-1} &= \left(\sum_{i=1}^{2^n-1} a_{S_i} M_i \right) \left(\sum_{i=1}^{2^n-1} a_{S_i}(H - M_i) \right) \\
&= \sum_{1 \leq i \neq j \leq n}^{2^n-1} a_{S_i} M_i a_{S_j}(H - M_j) + \sum_{1 \leq i \leq n}^{2^n-1} a_{S_i}^2 M_i (H - M_i) \\
&= 2^{n-2} \sum_{1 \leq i \neq j \leq n}^{2^n-1} a_{S_i} a_{S_j} H + \sum_{1 \leq i \leq n}^{2^n-1} a_{S_i}^2 (2^{n-1} H - 2^{n-1} M_i) \\
&= 2^{n-2} \sum_{1 \leq i \neq j \leq n}^{2^n-1} a_{S_i} a_{S_j} H + 2^{n-1} \sum_{1 \leq i \leq n}^{2^n-1} a_{S_i}^2 (H - M_i) \qquad (7.3)
\end{aligned}$$

Since $|\mathfrak{G}_{n,k}| = 2^{2n}, h = |H| = 2^n$ we have $k = 2^{n-1}(2^n - 1)$, $\lambda = 2^{n-1}(2^{n-1} - 1)$.

Returning to equation (7.3), in particular looking at the first sum of equation (7.3), we see that every non-trivial coset of H occurs $2^n - 2$ times in equation (7.3). Thus from equation (7.3) we see that the coefficient in DD^{-1} of each element of that coset is

$$2^{n-2}(2^n - 2) = 2^{n-1}(2^{n-1} - 1) = \lambda,$$

as we desire.

The second sum of equation (7.3) gives the contributions to the trivial H-coset. We rewrite it as

$$2^{n-1} \sum_{1 \leq i \leq n}^{2^n-1} a_{S_i}^2 (H - M_i) = 2^{n-1} \sum_{1 \leq i \leq n}^{2^n-1} (H - a_{S_i}^2 M_i). \qquad (7.4)$$

But we are assuming that $a_{S_i}^2 \notin M_i$, so we must have $H - a_{S_i}^2 M_i = M_i$. Thus equation (7.4) is

$$2^{n-1} \sum_{1 \le i \le n}^{2^n - 1} M_i. \tag{7.5}$$

Now since the M_i are distinct maximal subgroups, and there are $2^n - 1$ of them, we see that every maximal subgroup of $H \cong \mathcal{C}_2^n$ is in the list $M_1, \dots, M_{2^n - 1}$, and so one has

$$\sum_{1 \le i \le 2^n - 1} M_i = (2^n - 1) \cdot 1 + (2^{n-1} - 1)(H - 1).$$

Thus if $h' \in H, h' \neq 1$, then the coefficient of h' in equation equation (7.5) is

$$2^{n-1}(2^{n-1} - 1) = \lambda,$$

as required.

The coefficient of 1 in $D \cdot D^{-1}$ is then

$$k^2 - \lambda(|\mathfrak{G}_{n,k}| - 1) = 2^{2n-2}(2^{n-1} - 1)^2 - 2^{n-1}(2^{n-1} - 1)(2^{2n} - 1),$$

which is equal to k, as required. Thus we have $D \cdot D^{-1} = \lambda(G - 1) + k \cdot 1$. $\square$

§7 Representations

Suppose that G is a DRAD difference set group with difference set D and subgroup $H, h = |H|$. We recall that D, D^{-1}, G, H satisfy the equations

$$(10.1)\ D^2 = \lambda G + \frac{h}{2} H - (k - \lambda); \quad (10.2)\ DD^{-1} = \lambda G + (k - \lambda);$$

$$(10.3)\ HD = \frac{h}{2}(G - H).$$

Let ρ be a non-principal irreducible representation of G with irreducible character χ and $d = \chi(1)$. We assume that ρ is unitary. Since χ is not principal we see from orthogonality of the character table that $\chi(G) = 0$.

Since ρ is unitary we see that $\rho(D^{-1}) = D^*$. Now we know from Lemma 3.2 that D, D^{-1}, G, H pairwise commute, and so $\{\rho(D), \rho(D^{-1}), \rho(H), \rho(G)\}$ is a set of commuting normal matrices. Thus they are simultaneously diagonalizable, and we may assume that in fact they are diagonal matrices.

Since $H \triangleleft G$ and ρ is irreducible it follows that $\rho(H)$ is a scalar matrix, which we write as

$$\rho(H) = h_0 \rho(1), \ \ h_0 \in \mathbb{C}.$$

Since $H^2 = hH$ we have $\rho(H)^2 = h\rho(H)$, which shows that either $\rho(H) = 0$ or $\rho(H) = h$; i.e. $h_0 \in \{0, h\}$. From (10.1) and (10.2) we see that

$$\rho(D)^2 = \frac{h(2h_0 - h)}{4} \rho(1); \quad \rho(D)\rho(D)^* = (k - \lambda)\rho(1) = \frac{h^2}{4} \rho(1).$$

CASE 1: If $h_0 = 0$, then these give (where $i^2 = -1$)

$$\rho(D) = \operatorname{diag}\left(\varepsilon_1 i \frac{h}{2}, \varepsilon_2 i \frac{h}{2}, \dots, \varepsilon_d i \frac{h}{2}\right).$$

Here $\varepsilon_i \in \{-1, 1\}$. In this case $\mu(\rho(D))$ divides $x^2 + \frac{1}{4}h^2$.

CASE 2: If $h_0 = h$, then (10.3) gives

$$h\rho(D) = -\frac{h^2}{2}\rho(1), \text{ so that } \rho(D) = -\frac{h}{2}\rho(1).$$

But then we have $\rho(D^{-1}) = D^* = D$. In this case $\mu(\rho(D)) = x + \frac{h}{2}$. This gives Theorem 1.5. □

§8 ABELIAN GROUPS

Proof of Theorem 1.7 (i) . So suppose that h is not a power of 2 and let p be an odd prime divisor of h. Let $g \in H$ be an element of order $p^u, u \geq 1$, where $\langle g \rangle \cong \mathcal{C}_{p^u}, g \in H$, is a factor of the Sylow p-subgroup of H. Then $H = \mathcal{C}_{p^u} \times U$, where U is some subgroup of H.

Let ψ be a character of H that does not kill g, but where $\chi(U) = 1$. We then note that $\psi(H) = 0$.

By [14, Cor 5.5, p. 63] we can extend ψ to an irreducible character χ of G that take values in some $\mathbb{Q}(\zeta_{p^v}), v \geq u$. Then we have $\chi(H) = \phi(H) = 0$. Also $\chi(G) = 0$. Now we have $G = D + D^{-1} + H$, so that

$$0 = \chi(G) = \chi(D) + \chi(D^{-1}) + \chi(H) = \chi(D) + \chi(D^{-1}).$$

Thus $\chi(D) = -\chi(D^{-1})$. We also have $\chi(D)\chi(D^{-1}) = \lambda G + (k - \lambda)$, so that

$$-\chi(D)^2 = k - \lambda = h^2/4.$$

Thus $\chi(D) = \pm ih/2 \in \mathbb{Q}(i)$. But $\chi(D) \in \mathbb{Q}(\zeta_{p^v})$, and it is well-known that $\mathbb{Q}(\zeta_{p^v}) \cap \mathbb{Q}(i) = \mathbb{Q}$, since p is an odd prime, so that $\pm ih/2 \in \mathbb{Q}$, a contradiction. □

Proposition 8.1. *(i) If G is a semi-direct product, $G = N \rtimes \mathcal{C}_2, \mathcal{C}_2 = \langle t \rangle$, then G is not a DRAD difference set group.*

(ii) Suppose that $G = K \rtimes \mathcal{C}_{2r}$ with subgroup H where $\overline{C}_{2r} \leq H$. Then G is not a DRAD difference set group with subgroup H.

(iIi) Let p be an odd prime. Let G be a DRAD difference set group with subgroup H and diff set D. Then G is not a semi-direct product, $G = N \rtimes \mathcal{C}_p, \mathcal{C}_p = \langle t \rangle \leq H$.

Proof (i) Suppose it is, with subgroup H and difference set D. Let $\chi : G \to \mathbb{C}$ be the linear character where $\chi(t) = -1, \chi(N) = 1$.

Since $t^2 = 1$ we see that $t \in H$, which then shows that $\chi(H) = 0 = \chi(G)$. Since $D + D^{-1} = G - H$ we get $\chi(D) + \chi(D^{-1}) = 0$, so that $\chi(D^{-1}) = -\chi(D)$. Thus $DD^{-1} = \lambda G + k - \lambda$ gives $\chi(D)\chi(D^{-1}) = k - \lambda = h^2/4$. Thus $\chi(D) = \pm ih/2$. But $\chi(D) \in \mathbb{Q}$, since $D \in \mathbb{Z}G$ and χ takes values in $\{\pm 1\}$. This contradiction concludes the proof of (i) and (ii), (iii) follow similarly. □

Proof of Theorem 1.7 (ii). Let the abelian DRAD difference set group G have difference set D and subgroup $H, |H| = h$. We know from Theorem 1.7 (i) that G has to be a 2-group. So assume that the exponent of G is $h2^u$, where $u \geq 1$. Since G is abelian we may write $G = \mathcal{C}_{h2^u} \times L$, where $\mathcal{C}_{h2^u} = \langle t \rangle$. Then we have $|L| = h/2^u \leq h/2$.

If $|H \cap L| = h/2$, then we would have $L \leq H$, and so a generator of one of the maximal cyclic subgroups of L would be in H. This would contradict Proposition 8.1 (ii). Thus we see that $|H \cap L| \leq h/4$.

Let $K = \langle t^{h2^u/2} \rangle$, a subgroup of order 2. Then $K \leq H$ and if $H \subset KL$, then $|H \cap L| = h/2$, which is a contradiction. Thus $H \not\subseteq KL$. Let $\alpha = t^s g_0 \in H \setminus KL$, where $g_0 \in L$. Then t^s has order $2^v \geq 4$. Let $\alpha' := \alpha^{2^v/4} = t^{s2^v/4} g_0^{2^v/4}$, where $t^{s2^v/4}$ has order 4. Further, since $\alpha \in H$ we have $\alpha' = \alpha^{2^v/4} \in H$, but since $t^{s2^v/4}$ has order 4 we also see that $\alpha^{2^v/4} \notin KL$. Thus we have $\alpha' = t^{s2^v/4} g_0'$ where $g_0' \in L$ and $t^{s2^v/4}$ has order 4. It follows that $s2^v/4 = h2^u/4$ or $s2^v/4 = 3h2^u/4$. By replacing α' by its inverse we can assume that $\alpha' = t^{h2^u/4} g_0'$.

Define $\zeta = \exp \frac{2\pi i}{h2^u}$ and define the character χ by

$$\chi(t) = \zeta, \qquad \chi(L) = 1.$$

Since $\alpha' \in H$ and is not in the kernel of χ we see that $\chi(H) = 0$. Since $G - H = D + D^{-1}$ it follows that $\chi(D) = -\chi(D^{-1})$, and so from $DD^{-1} = \lambda G + (k - \lambda)$ we obtain $\chi(D)^2 = -h^2/4$, so that $\chi(D) = \pm ih/2$. Replacing D with D^{-1} as necessary we may assume $\chi(D) = ih/2$.

Now define

$$X_j = |t^j L \cap D|, \quad 0 \leq j \leq 2^{h2^u} - 1.$$

Then we clearly have $X_j \leq |L| \leq \frac{h}{2}$. Also $\chi(D) = \sum_{j=0}^{h2^u-1} X_j \zeta^j$.

Now from $\chi(D) = ih/2$ we have

$$\begin{aligned} X_0 + & X_1\zeta^1 + X_2\zeta^2 + \cdots + X_{h2^u/4-1}\zeta^{h2^u/4-1} + X_{h2^u/4} i + X_{h2^u/4+1}\zeta^{h2^u/4+1} + \\ & \cdots + X_{h2^u/2-1}\zeta^{h2^u/2-1} - X_{h2^u/2} - X_{h2^u/2+1}\zeta^1 - X_{h2^u/2+2}\zeta^2 \\ & - \cdots - X_{3h2^u/4-1}\zeta^{h2^u/4-1} - X_{3h2^u/4} i - X_{3h2^u/4+1}\zeta^{h2^u/4+1} - \\ & \cdots - X_{h2^u-1}\zeta^{h2^u/2-1} = ih/2. \end{aligned}$$

Using the fact that $1, \zeta, \zeta^2, \ldots, \zeta^{h2^u/2-1}$ is a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$, and by looking at the coefficient of i in the above, we see that $X_{h2^u/4} - X_{3h2^u/4} = h/2$. Thus

$$X_{h2^u/4} = X_{3h2^u/4} + h/2 \geq h/2. \tag{8.1}$$

Recall that $X_{h2^u/4} = |t^{h2^u/4} L \cap D|$. Here we note that $\alpha' = t^{h2^u/4} g_0' \in H$, and since $H \cap D = \emptyset$ we thus have $\alpha' \notin t^{h2^u/4} L \cap D$ and so does not contribute to the sum that gives $X_{h2^u/4}$. It follows that $X_{h2^u/4} < h/2$ contradicting equation (8.1). This contradiction gives the result. □

Examples from [23, Theorem 9.3] show that the bound on the exponent given in Theorem 1.7 is strict.

References

[1] W. Bosma and J. Cannon, MAGMA (University of Sydney, Sydney, 1994).

[2] Y.Q. Chen, T. Feng, *Abelian and non-abelian Paley type group schemes*, preprint.

[3] Coulter, Robert S., Gutekunst, Todd, *Special subsets of difference sets with particular emphasis on skew Hadamard difference sets.* Des. Codes Cryptogr. 53 (2009), no. 1, 1–12.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM, vol. 138, Springer, 1996.

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

[6] Davis, P.J., *Circulant matrices*, Chelsea, New York, (1994).

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

[8] C. Ding, Z. Wang, Q. Xiang, *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in PG(3,32h+1)*, J. Combin. Theory Ser. A 114 (2007) 867–887.

[9] R.J. Evans, *Nonexistence of twentieth power residue difference sets*, Acta Arith. 84 (1999) 397–402.

[10] T. Feng, Q. Xiang, *Strongly regular graphs from union of cyclotomic classes*, arXiv:1010.4107v2. MR2927417
[11] Moore, Emily H.; Pollatsek, Harriet S. *Difference sets. Connecting algebra, combinatorics, and geometry.* Student Mathematical Library, 67. American Mathematical Society, Providence, RI, 2013. xiv+298 pp.
[12] T. Ikuta, A. Munemasa, *Pseudocyclic association schemes and strongly regular graphs*, European J. Combin. 31 (2010) 1513–1519.
[13] Isaacs, I. Martin *Finite group theory.* Graduate Studies in Mathematics, 92. American Mathematical Society, Providence, RI, 2008. xii+350.
[14] Isaacs, I. Martin *Character theory of finite groups.* Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. AMS Chelsea Publishing, Providence, RI, 2006. xii+310 pp.
[15] Ito, Noboru; Raposa, Blessilda P. *Nearly triply regular DRADs of RH type.* Graphs Combin. 8 (1992), no. 2, 143–153.
[16] Ito, Noboru *Automorphism groups of DRADs.* Group theory (Singapore, 1987), 151–170, de Gruyter, Berlin, (1989).
[17] J. Jedwab, *Perfect Arrays, Barker Arrays, and Difference Sets*, Ph.D. thesis, University of London, London, England (1991).
[18] Kesava Menon, P. *On difference sets whose parameters satisfy a certain relation.* Proc. Amer. Math. Soc. 13, (1962) 739–745.
[19] R. Kraemer, *A result on Hadamard difference sets*, J. Combin. Theory (A), Vol. 63 (1993) pp. 1–10.
[20] Muzychuk, Mikhail; Ponomarenko, Ilia, *Schur rings.* European J. Combin. 30 (2009), no. 6, 1526-1539.
[21] Schur I., *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitz. Preuss. Akad. Wiss. Berlin, Phys-math Klasse, (1933), 598–623.
[22] R. J. Turyn, *Character sums and difference sets.* Pacific J. Math., Vol. 15 (1965) pp. 319–346.
[23] Webster, Jordan D. *Reversible difference sets with rational idempotents.* Arab. J. Math. (Springer) 2 (2013), no. 1, 103–114.
[24] Wielandt, Helmut, *Finite permutation groups*, Academic Press, New York-London, (1964), x+114 pages.
[25] ______. *Zur theorie der einfach transitiven permutationsgruppen II.* Math. Z., 52:384–393, (1949).

Department of Mathematics, Brigham Young University, Provo, UT 84602, U.S.A. E-mail: courtneyh24601@gmail.com, steve@mathematics.byu.edu, nlnicholson24@gmail.com, poulsenseth@yahoo.com