Graphs and Combinatorics (2023) 39:67
https://doi.org/10.1007/s00373-023-02662-8

ORIGINAL PAPER

Difference Sets Disjoint from a Subgroup III: The Skew Relative Cases

Gradin Anderson[1] · Andrew Haviland[1] · Mckay Holmes[1] · Stephen P. Humphries[1] · Bonnie Magland[1]

Received: 25 October 2022 / Revised: 19 May 2023 / Accepted: 21 May 2023 / Published online: 13 June 2023

Abstract

We study finite groups G having a subgroup H and $D \subset G\backslash H$ such that (i) the multiset $\{xy^{-1} : x, y \in D\}$ has every element that is not in H occur the same number of times (such a D is called a *relative difference set*); (ii) $G = D \cup D^{(-1)} \cup H$; (iii) $D \cap D^{(-1)} = \emptyset$. We show that $|H| = 2$, that H is central and that G is a group with a single involution. We also show that G cannot be abelian. We give infinitely many examples of such groups, including certain dicyclic groups, by using results of Schmidt and Ito.

Keywords Difference set · Subgroup · Hadamard difference set · Schur ring · Dicyclic group

Mathematics Subject Classification Primary 05B10; Secondary 20C05

1 Introduction

Here G will always be a finite group. We identify $X \subseteq G$ with the element $\sum_{x\in X} x \in \mathbb{Q}G$, and let $X^{(-1)} = \{x^{-1} : x \in X\}$. We write $\mathcal{C}_n$ for the cyclic group of order n. Let

✉ Stephen P. Humphries
steve@mathematics.byu.edu

Gradin Anderson
gradysocool@yahoo.com

Andrew Haviland
andrewhaviland@att.net

Mckay Holmes
realitant@gmail.com

Bonnie Magland
bonnie.magland@gmail.com

1 Department of Mathematics, Brigham Young University, Provo, UT 84602, USA

$H \leq G$ and $h = |H|$. Then a (v, k, λ)-*relative difference set* (relative to H) is a subset $D \subset G \backslash H$, $|D| = k$, $v = |G|$, such that $DD^{(-1)} = \lambda(G - H) + k$, so that $g \in G \backslash H$ occurs λ times in the multiset $\{xy^{-1} : x, y \in D\}$.

We now further assume

(1) $D \cap D^{(-1)} = \emptyset$;
(2) $G = D \cup D^{(-1)} \cup H$ (disjoint union).

A group having a difference set of the above type will be called a (v, k, λ)-*skew relative Hadamard difference set group* (with difference set D and subgroup H); or a (v, k, λ)-*SRHDS group*. Recall the following related concept: a group G is 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 [1–8].

In this paper we find infinitely many examples of such SRHDS groups. We also find groups that cannot be SRHDS groups, but which satisfy certain properties of a SRHDS group, as given in:

Theorem 1.1 *For a (v, k, λ) SRHDS group G with difference set D and subgroup H we have:*

(i) $|H| = 2$*;*
(ii) $H \lhd G$*;*
(iii) *G is a group having a single involution;*
(iv) $v \equiv 0 \bmod 8$*;*
(v) *G is not abelian.*
(vi) *A Sylow 2-subgroup is a generalized quaternion group.*

For part (vi), suppose that G is a finite group with a unique involution. Then a Sylow 2-subgroup of G also has a unique involution. Now 2-groups with unique involution were determined by Burnside (see [9, Theorems 6.11, 6.12] and [10, 11]); they are cyclic or generalized quaternion groups. Corollary 4.5 shows they cannot be cyclic.

Groups with a single involution are studied in [12–14]. Dicyclic groups Dic_v are examples of such groups and we show that each Dic_{8p}, $1 \leq p < 9$ is an SRHDS group. However, we show that Dic_{72} has no SRHDS (Proposition 8.1).

We now establish a connection between SRHDS groups and Hadamard groups. Recall that a *Hadamard group* is a group G containing $H \leq Z(G)$ of order 2 such that there is an H-transversal D, $|D| = v/2$, that is a relative difference set relative to H (so that $DD^{(-1)} = \lambda(G - H) + |D|$ and $HD = G$).

We show that if $D \subset G$ is a SRHDS, then G is also a Hadamard group (where $E = D + 1$ is the relative difference set); see Proposition 2.5. Thus it is natural to try to obtain results for SRHDS groups that are similar to the results of Schmidt and Ito [15, 16] from the Hadamard group situation. For example Schmidt and Ito show that if $4p - 1$ or $2p - 1$ is a prime power, then the groups Dic_{8p} or Dic_{4p} (respectively) are Hadamard groups. For dicyclic SRHDS groups we show:

Theorem 1.2 *If $p \in \mathbb{N}$ and $4p - 1$ is a prime power, then* Dic_{8p} *is a SRHDS group.*

There is no analogous result when $2p - 1$ is prime. Now Ito [16] determines a 'doubling process' that takes a Hadamard difference set for Dic_v and produces a Hadamard difference set for Dic_{2v}. For us this doubling process gives:

Theorem 1.3 *If $p \in \mathbb{N}$ and $4p-1$ is a prime power, then* Dic_{16p} *is a SRHDS group.*

We note that this doubling process does not work in general in the context of a SRHDS, however in our next paper we will show that it does work for a SRHDS under an additional hypothesis that we call *doubly symmetric* that is satisfied in the situation of Theorem 1.2, so that in this case we obtain an SRHDS in Dic_{16p}. This will allow us to prove, in the next paper, among other things:

Theorem 1.4 *Let $G = \mathrm{Dic}_{8\cdot 2^u}$ be a generalized quaternion group for some $u \in \mathbb{Z}_{\geq 0}$. Then G contains a doubly symmetric SRHDS if and only if $2^{u+1}-1$ is either prime or* 1.

Lastly, the following is a consequence of Proposition 8.2.

Theorem 1.5 *Let $G = C_p \times \mathrm{Dic}_{8n}$ with $p > 2$ prime and n odd. Then G is not a SRHDS group.*

2 $|H| = 2$ and Normality of H

Recall that for $p \geq 2$ the *dicyclic group* of order $4p$ is

$$\mathrm{Dic}_{4p} = \langle x, y | x^{2p} = y^2, y^4 = 1, x^y = x^{-1} \rangle.$$

A *generalized quaternion group*, Q_{2^a}, is the dicyclic group Dic_{2^a}, $a \geq 3$.

Proposition 2.1 *Let G be a SRHDS group with subgroup H. Then G has a single involution t, and $H = \langle t \rangle$. In particular $h = 2$, $H \leq Z(G)$ and $H \lhd G$.*

Proof Let $D \subset G$ be a SRHDS. Now D has no involutions since $D \cap D^{(-1)} = \emptyset$. Since $G - (D + D^{(-1)}) = H$ all involutions are contained in H.

If $d_i \in D, h_i \in H, i = 1, 2$, with $h_1 d_1 = h_2 d_2 \in H d_1 \cap H d_2$, then $h_2^{-1} h_1 = d_2 d_1^{-1} \in H$, so that $h_2^{-1} h_1 = d_2 d_1^{-1} = 1$ (since $D D^{(-1)} = \lambda(G - H) + k$ implies that the only element of H of the form $d_2 d_1^{-1}$ is 1). Thus $d_1 = d_2$ and $h_1 = h_2$.

Thus the cosets Hd, $d \in D$, are disjoint and so $|\cup_{d \in D} Hd| = |H| \cdot |D| = hk$. Since $Hd \subset G - H$ for $d \in D$, we see that $hk = |\cup_{d \in D} Hd| \leq |G \backslash H| = |D + D^{(-1)}| = 2k$. Thus $h \leq 2$ and so $h = 2$ as $h > 1$. The rest of the result follows. □

This proves (i), (ii) and (iii) of Theorem 1.1. In what follows we will let $H = \langle t \rangle$, where $t \in Z(G)$ has order 2. Then:

$$G = D + D^{(-1)} + H, \qquad D \cdot D^{(-1)} = \lambda(G - H) + k \cdot 1. \tag{2.1}$$

These equations give: $v = 2k + 2$, $k^2 = k + \lambda(v - 2)$, and solving gives (i) of

Lemma 2.2 (i) $v = 2k + 2$, $\quad \lambda = (k-1)/2 = (v-4)/4$ *and* $4|v$.
(ii) $DH = HD = D^{(-1)}H = HD^{(-1)} = G - H$.
(iii) $G, D, D^{(-1)}, H$ *all commute.*

Proof From $D \subset G - H$ we have $DH \cap H = \emptyset$, and $DH \subset G - H$; but $|G - H| = 2k = |DH|$, so that

$$DH = HD = G - H = (G - H)^{(-1)} = D^{(-1)}H = HD^{(-1)},$$

giving (ii).

Since $D^{(-1)} = G - D - H$ and $H \leq Z(G)$ it now follows that D and $D^{(-1)}$ commute. This shows that $G, D, D^{(-1)}, H$ all commute. □

Lemma 2.3 *Let G be a SRHDS group with difference set D and subgroup $H = \langle t \rangle$. Then $D^{(-1)} = tD$.*

Proof We have $D + Dt = (1 + t)D = HD = G - H = D + D^{(-1)}$. □

We now define Schur rings [17–20]. A subring $\mathfrak{S}$ of $\mathbb{Z}G$ is 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 $\mathfrak{S}$. Then we have:

Lemma 2.4 *$\{1\}, \{t\}, D, D^{(-1)}$ are the principal sets of a commutative Schur ring.*

Proof Now $\{1\}, \{t\}, D, D^{(-1)}$ partition G and $D^{(-1)} = tD, tD^{(-1)} = D, t^2 = 1, D^{(-1)}D = DD^{(-1)} = \lambda(G - H) + k = \lambda(D + D^{(-1)}) + k, D^2 = tDD^{(-1)} = t(\lambda(D + D^{(-1)}) + k)$. This concludes the proof. □

Proposition 2.5 *If $D \subset G$ is a SRHDS, then G is a Hadamard group.*

Proof Now $DD^{(-1)} = \lambda(G - H) + k$. Let $E = D + 1$, so that $EE^{(-1)} = DD^{(-1)} + D + D^{(-1)} + 1 = \lambda(G - H) + k + (G - H) = (\lambda + 1)(G - H) + k + 1$, as required. □

3 Intersection Numbers

Let $N \lhd G$ and let $g_1, g_2, \ldots, g_r$ be coset representatives for G/N. Then for each $1 \leq i \leq r$ there is $1 \leq i' \leq r$ such that $g_i g_{i'} \in N$ i.e. $Ng_i \cdot Ng_{i'} = N$ in G/N. If G is a SRHDS group with difference set D, then the numbers $n_i = |D \cap Ng_i|$ are called the *intersection numbers*. Standard techniques give (see Section 7.1 of [21]):

Lemma 3.1 *Let $D \subset G$ be a SRHDS with subgroup $H = \langle t \rangle$, $t^2 = 1$. Let $N \lhd G$ have order s and index r in G. Let $g_1 = 1, g_2, \ldots, g_r$ be coset representatives for G/N and let $n_i = |D \cap Ng_i|$, $1 \leq i \leq r$. Then*

$$\sum_{i=1}^{r} n_i = k, \qquad \sum_{i=1}^{r} n_i^2 = \lambda|N\backslash H| + k,$$
$$\sum_{i=1}^{r} n_i n_{i'} = \lambda|N| + (\lambda+1)\cdot|H\cap N| - k.$$

Lemma 3.2 *Let $N \lhd G$ where $D \subset G$ is a SRHDS with subgroup H and $H \cap N = \{1\}$. Let $Ng_3, \cdots, Ng_r$ be the cosets that don't meet H, and let $n_i = |D \cap Ng_i|$. Suppose that we have distinct $i, i' > 2$ where $g_i g_{i'} \in N$. Then $n_i + n_{i'} = |N|$.*

Proof We have $n_i = |D \cap Ng_i| = |D^{(-1)} \cap Ng_i^{-1}| = |D^{(-1)} \cap Ng_{i'}|$. If $i \geq 3$, then $Ng_{i'} \subset G\backslash H = D + D^{(-1)}$, so that

$$|N| = |(D + D^{(-1)}) \cap Ng_{i'}| = |D \cap Ng_{i'}| + |D^{(-1)} \cap Ng_{i'}| = n_{i'} + n_i.$$

□

The next result concerns intersection numbers for subgroups that are not necessarily normal:

Proposition 3.3 *Let G be a SRHDS group with difference set D and subgroup H. Let $K \leq G$ be any subgroup where $t \in K$. Let $b = |G : K|$ and let $g_0 = 1, g_1, \ldots, g_{b-1}$ be coset representatives for $K \leq G$. Let $k_i = |D \cap Kg_i|, 0 \leq i < b$. Then $k_0 = |K|/2 - 1$ and $k_i = |K|/2, \ 0 < i < b$.*

Let $D_i = D \cap Kg_i, i = 0, \ldots, b-1$. Then $\sum_{i=0}^{b-1} D_i D_i^{(-1)} = \lambda(K - H) + k$.

Proof We have $D^{(-1)} = tD$. Let $D_i = D \cap Kg_i$; then $tD_i = t(D \cap Kg_i) = (tD) \cap tKg_i = D^{(-1)} \cap Kg_i$, so that $D \cap tD = \emptyset$ and $i > 0$ gives

$$\begin{aligned} D_i + tD_i &= (D \cap Kg_i) + (D^{(-1)} \cap Kg_i) = (D + D^{(-1)}) \cap Kg_i \\ &= (G - H) \cap Kg_i = G \cap Kg_i = Kg_i. \end{aligned}$$

Taking cardinalities, again using $D \cap tD = \emptyset$, gives $2k_i = |K|$, for $i > 0$. Then $\sum_{i=0}^{b-1} k_i = k$ now gives

$$k_0 + (b-1)|K|/2 = k = v/2 - 1;$$

but $v = b \cdot |K|$, from which we obtain $k_0 = |K|/2 - 1$.

Now from $DD^{(-1)} = \lambda(G-H)+k$ and $D = \sum_{i=0}^{b-1} D_i g_i$ we get $\sum_{i=0}^{b-1} D_i D_i^{(-1)} + \cdots = \lambda(G - H) + k$, so that $\sum_{i=0}^{b-1} D_i D_i^{(-1)} \subseteq \lambda(K - H) + k$. The last part will follow if we can show that both sides of this equation have the same size.

From $b = v/|K|$ and the first part, the size of the left hand side is

$$\sum_{i=0}^{b-1} |D_i|^2 = (|K|/2 - 1)^2 + (b-1)|K|^2/4 = 2p|K| - |K| + 1$$

and (since $H \subset K$) the number of elements of the right hand side is $\lambda(|K|-2)+k = 2p|K| - |K| + 1$, and we are done. □

4 Direct Products and *G* is not Abelian

Let $\zeta_n = \exp 2\pi i/n, n \in \mathbb{N}$. We first show

Theorem 4.1 *Suppose that $N \trianglelefteq G$, $G/N \cong \mathcal{C}_{2^a}, a \geq 2$, and $t \notin N$. Assume that $k = |G|/2 - 1$ is not a perfect square. Then G is not a SRHDS group.*

Proof Note that $a \geq 2$ means that k is odd. Now assume that G is a SRHDS group and that $G/N = \langle rN \rangle \cong \mathcal{C}_{2^a}, r \in G$. For $g \in G$ we have $g = r^i b, 0 \leq i < 2^a, b \in N$. Then there is a linear character $\chi' : G/N \to \mathbb{C}^\times, \chi'(rN) = \zeta_{2^a}$ that induces $\chi : G \to \mathbb{C}^\times, \chi(r^i b) = \chi'(r^i N)$. Here $N = \ker \chi$. Then we can write

$$D = \sum_{j=0}^{2^a-1} r^j N_j, \text{ where } N_j \subseteq N.$$

Since $t \notin N$ we have $\chi(t) = -1$ and so $\chi(H) = 0$. We certainly have $\chi(G) = 0$. From $G = D + D^{(-1)} + H$ we get $\chi(D) + \chi(D^{(-1)}) = 0$, and from $DD^{(-1)} = \lambda(G-H)+k$ we get $\chi(D)\chi(D^{(-1)}) = k$. These give $\chi(D)^2 = -k,$ and so $\chi(D) = \pm\sqrt{-k}$. But

$$\pm i\sqrt{k} = \chi(D) = \chi\left(\sum_{j=0}^{2^a-1} r^j N_j\right) = \sum_{j=0}^{2^a-1} (\zeta_{2^a})^j |N_j|, \tag{4.1}$$

which gives $\sqrt{k} \in \mathbb{Q}(i, \zeta_{2^a}) = \mathbb{Q}(\zeta_{2^a})$, since $a \geq 2$. But the Galois group of $\mathbb{Q}(\zeta_{2^a})/\mathbb{Q}$ is $\mathcal{C}_2 \times \mathcal{C}_{2^{a-2}}$. These groups have at most three subgroups of index 2. The Galois correspondence tells us that $\mathbb{Q}(\zeta_{2^a})$ contains at most three quadratic extensions, the only possibilities being $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$. But the hypothesis says that k is not a perfect integer square, so that $\sqrt{k} \notin \mathbb{Z}$. Now $k > 1$ is also odd, and so $\sqrt{k} \notin \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})$. This contradiction gives Theorem 4.1. □

Corollary 4.2 *Suppose that $N \trianglelefteq G$, $G/N \cong \mathcal{C}_{2^a}, a \geq 3$, and $t \notin N$. Then G is not a SRHDS group.*

Proof Since $2^a \geq 8$ we see that $k = (|G|-2)/2$ satisfies $k \equiv 3 \bmod 4$, and so the result follows from Theorem 4.1. □

Corollary 4.3 *If G is abelian with $|G| \equiv 0 \bmod 8$, then G is not a SRHDS group.*

Proof Let G be an abelian SRHDS group, and write $G = A \times N$ where A is a Sylow 2-subgroup, and N is a subgroup of odd order. Since G has a single involution, we see that A is cyclic, say of order 2^a. The results now follow from Corollary 4.2. □

Corollary 4.4 *If G is a SRHDS group, then $v = |G| \equiv 0 \bmod 8$.*

Proof Assume that G is a SRHDS group with subgroup $H = \langle t\rangle$ and difference set D. Then we know that $4|v$ by Lemma 2.2, so suppose that $|G| = 4n$ where n is odd. Then a Sylow 2-subgroup of G must be $\mathcal{C}_4 = \langle r\rangle$ and $t = r^2$. Burnside's theorem [9, Theorem 5.13] shows that $\langle r\rangle$ has a complement $N \lhd G$, $|N| = n$, $G = N \rtimes \langle r\rangle$. So we can write $D = D_0 + D_1 r + D_2 r^2 + D_3 r^3$, $D_i \subset N$. Now $D + D^{(-1)} = G - H = N + Nr + Nr^2 + Nr^3 - H$ then gives

$$D_0 + D_0^{(-1)} = N - 1,\quad D_1 + \left(D_3^{(-1)}\right)^{r^3} = N,\quad D_2 + \left(D_2^{(-1)}\right)^{r^2} = N - 1$$
$$D_3 + \left(D_1^{(-1)}\right)^{r} = N.$$

Next, $D^{(-1)} = tD$ gives

$$D_0^{(-1)} = tD_0,\ \left(D_1^{(-1)}\right)^{r} = tD_3,\ \left(D_2^{(-1)}\right)^{r^2} = tD_2,\ \left(D_3^{(-1)}\right)^{r^3} = tD_1.$$

Using $D_1 + \left(D_3^{(-1)}\right)^{r^3} = N$ and $\left(D_3^{(-1)}\right)^{r^3} = tD_1$ we get $D_1(1+t) = N$. However $D_1(1+t)$ has an even number of elements (counting multiplicities), while $|N|$ is odd. This contradiction gives the result. □

Corollaries 4.3 and 4.4 now prove Theorem 1.1 (iv) and (v).

Corollary 4.5 *If G is a SRHDS group, then a Sylow 2-subgroup of G is not cyclic.*

Proof Assume G is a SRHDS group with cyclic Sylow 2-subgroup $\langle r\rangle$. By Corollary 4.4, $|\langle r\rangle| \geq 8$. Again, Burnside's theorem [9, Theorem 5.13] shows that $\langle r\rangle$ has a complement $N \lhd G$, $G = N \rtimes \langle r\rangle$. This now contradicts Corollary 4.2. □

This concludes the proof of Theorem 1.1.

5 Construction of Some SRHDS Groups

We need the following set-up: For prime power $q = 4p - 1$, $p \in \mathbb{N}$, we let $\mathbb{F}_{q^n}$ be the finite field of order q^n. Let $tr : \mathbb{F}_{q^2} \to \mathbb{F}_q$, $\beta \mapsto \beta^q$ be the trace function. Let $\alpha \in \mathbb{F}_{q^2}$ satisfy $tr(\alpha) = 0$. Let $\mathbb{F}_{q^2}^* = \langle z\rangle$. Let $Q = \{u^2 : u \in \mathbb{F}_q, u \neq 0\}$. Then $-1 \notin Q$ since $q \equiv 3 \bmod 4$. Now choose $D \in \mathbb{F}_q \backslash (Q \cup \{0\})$. Then any $\beta \in \mathbb{F}_{q^2}$ has the form $\beta = a + b\sqrt{D}$, for some $c, d \in \mathbb{F}_q$ and $tr(c + d\sqrt{D}) = c - d\sqrt{D}$. Write $\alpha = a + b\sqrt{D}$. Then $tr(\alpha) = 0$ if and only if $a = 0$, so we can choose $\alpha = \sqrt{D}$.

Let $U \leq \mathbb{F}_{q^2}^*$ be the subgroup of order $(q-1)/2$, and let $\pi : \mathbb{F}_{q^2}^* \to W := \mathbb{F}_{q^2}^*/U$ be the natural map.

Theorem 5.1 *Suppose that* $4p - 1$ *is a prime power. Then* Dic_{8p} *contains a SRHDS.*

Proof We follow [15, Theorem 3.3].

Let $q = 4p - 1$ and assume the above set-up. Let $g := \pi(z)$ be a generator for W and note that $|W| = 2(q+1) = 8p$. Let $R = \{\pi(x) : x \in \mathbb{F}_{q^2}^*, tr(\alpha x) \in Q\}$. Then by

[22, Thm 2.2.12], R is a relative $(q+1, 2, q, (q-1)/2)$ difference set in W relative to the subgroup $H := \langle g^{4p} \rangle$ of order 2.

Define $R_1, R_2 \subset W_2 := \langle g^2 \rangle$ by $R = R_1 + R_2 g$. Since R is a relative $(q+1, 2, q, (q-1)/2)$ difference set, $RR^{(-1)} = \frac{q-1}{2}(W - H) + q$ from which we get

$$R_1 R_1^{(-1)} + R_2 R_2^{(-1)} = q + \frac{q-1}{2}(W_2 - H).$$

If $d \in \mathbb{F}_{q^2}^*$ has order dividing $q+1$, then $d^q = d^{-1}$ and so

$$tr(\alpha d) = \alpha d + \alpha^q d^q = \alpha d - \alpha d^{-1} = -tr(\alpha d^{-1}).$$

Thus if $\mathrm{tr}(\alpha d) \in Q$, then $\mathrm{tr}(\alpha d^{-1}) \in -Q$. But $q \equiv 3 \bmod 4$ tells us that $g^{4p} = -1 \notin Q$, so that $\mathrm{tr}(\alpha g^{4p} d^{-1}) \in Q$. Thus $g^{4p} d^{-1} \in R_1$. Now the order of $g^{4p} d^{-1}$ is a divisor of $2(q+1) = |W|$. This gives a bijection, $Ud \leftrightarrow U g^{4p} d^{-1}$, between the elements of $R_1 \subset W_2$, which then gives $R_1^{(-1)} = g^{4p} R_1$.

Now let $G = \mathrm{Dic}_{8p} = \langle a, b | a^{2p} = b^2, b^4 = 1, a^b = a^{-1} \rangle$ and identify $\langle a \rangle$ with W_2, so that $a \leftrightarrow g^2$. From $R_1^{(-1)} = g^{4p} R_1$ we see that if $\gamma \in R_1 \cap R_1^{(-1)}$, then $g^{4p} \in R_1 R_1^{(-1)}$, a contradiction to R being a relative difference set relative to H. It follows that $R_1 \cap R_1^{(-1)} = \emptyset$. Now $1, -1 = g^{4p} \notin R_1$ as $\mathrm{tr}(\alpha 1) = 0 \notin Q$, and so

$$R_1 + R_1^{(-1)} = W_2 - H. \tag{5.1}$$

Then (5.1) and $R_1^{(-1)} = g^{4p} R_1$ gives

$$W_2 - H = R_1(1 + g^{4p}) = R_1 H,$$

so that we have the first part of

Lemma 5.2 (i) *$R_1 + 1$ is a transversal for W_2/H.*
(ii) *R_2 is a transversal for W_2/H.*

Proof (ii) We first show that R+1 is a transversal for W/H.

If $u \in W$, then $\mathrm{tr}(\alpha u) \in Q$, and it follows that $\mathrm{tr}(\alpha g^{4p} u) = -tr(\alpha u) \notin Q$. This sets up a bijection $u \leftrightarrow g^{4p} u$ of $W - H$ where the orbits of this bijection are the non-trivial H-cosets and a transversal corresponds to the elements of Q.

Since R+1 is a transversal for W/H and $R_1 + 1$ is a transversal for W_2/H it follows that R_2 is a transversal for W_2/H. This concludes the proof. □

Now if $\alpha = \sqrt{D}$, $\beta = a + b\sqrt{D}$, then $\mathrm{tr}(\alpha\beta) = 2bD \in Q$ if and only if $2b \in \mathbb{F}_q^* \backslash Q$.

Define $S := a^{2p} R_1 + R_2 b$. First we show that $SS^{(-1)} = \lambda(G - H) + k$ where $k = (v-2)/2, \lambda = (k-1)/2$:

$$\begin{aligned} SS^{(-1)} &= (a^{2p} R_1 + R_2 b)\big(a^{2p} R_1^{(-1)} + b^{-1} R_2^{(-1)}\big) \\ &= R_1 R_1^{(-1)} + R_2 R_2^{(-1)} + R_1 R_2 (1 + a^{2p}) b \end{aligned}$$

$$
\begin{aligned}
&= R_1 R_1^{(-1)} + R_2 R_2^{(-1)} + R_1 R_2 H b \\
&= R_1 R_1^{(-1)} + R_2 R_2^{(-1)} + R_1 W_2 b \\
&= q + \frac{q-1}{2}(W_2 - H) + |R_1| W_2 b \\
&= k + \lambda (W_2 - H) + \lambda W_2 b \\
&= k + \lambda (W_2 + W_2 b - H) = \lambda (G - H) + k, \qquad (5.2)
\end{aligned}
$$

as desired. Next we need

Lemma 5.3 *For S as above we have $S \cap S^{(-1)} = \emptyset$.*

Proof So assume that $r \in S \cap S^{(-1)}$, $S = a^{2p} R_1 + R_2 b$. Then there are two cases.

(a) First assume that $r \in \langle a \rangle$. Then there are $x^i, x^j \in R_1$ where $r = a^{2p} a^i = a^{2p} a^{-j}$ so we have $i = -j$. Since a corresponds to g^2 the elements g^{2i}, g^{-2j} satisfy $\mathrm{tr}(\alpha g^{2i})$, $\mathrm{tr}(\alpha g^{-2j}) \in Q$. Let $g^i = c + b\sqrt{D}$. Then $\mathrm{tr}(\alpha g^{2i})$, $\mathrm{tr}(\alpha g^{-2j}) \in Q$ (respectively) gives $4bcD \in Q$, $-\frac{4bcD}{(c^2-b^2D)^2} \in Q$ (respectively), which in turn gives $-1 \in Q$, a contradiction.

(b) Next assume that $r \in \langle a \rangle b$. Then there are i, j such that $r = a^i b = (a^j b)^{-1} = a^{j+2p} b$, where $a^i, a^j \in R_2$. Thus $i = j + 2p$. As in the first case this gives $\mathrm{tr}(\alpha g^{2i+1})$, $\mathrm{tr}(\alpha g^{2j+1}) = tr(\alpha g^{2i-4p+1}) \in Q$. Since $\mathrm{tr}(\alpha g^{2i-4p+1}) = -\mathrm{tr}(\alpha g^{2i+1})$, this gives $-1 \in Q$, a contradiction.

From $S \cap S^{(-1)} = \emptyset = S \cap H$ we get $G = S + S^{(-1)} + H$ and so Eq. (5.2) shows that S is a SRHDS, giving Theorem 5.1. □

We next wish to show that we can double these examples (see Sect. 6 for the definition of this doubling process), and we will need the following symmetry results: **Symmetry proof for R_1.** Now $S = a^{2p} R_1 + R_2 b$ and if $a^i \in a^{2p} R_1$, then $i = 2p + j$ where $tr(\alpha z^{2j}) \in Q$. We note that z, the generator of $\mathbb{F}_{q^2}^*$, has order $q^2 - 1$, and so $(z^q)^q = z$, showing that the non-trivial Galois automorphism is given by $z \mapsto z^q$.

So from $tr(\alpha z^{2j}) \in Q$ we get $tr(\alpha^q z^{2jq}) \in Q$. But $\alpha^q = -\alpha = \alpha z^{(q^2-1)/2}$. Thus

$$
tr(\alpha^q z^{2jq}) = tr(\alpha z^{2jq+(q^2-1)/2}) = tr(\alpha z^{2(jq+(q^2-1)/4)}) \in Q.
$$

This if $j' = (jq + (q^2 - 1)/4)$, then $a^{2p+j'} \in a^{2p} R_1$, and so $j \mapsto j'$ determines a function $R_1 \to R_1$ that one can show is an involution.

One can then check that $j = p + r$ is sent to $j' = p - r$ (recalling that j is defined mod $4p$). This gives a 'reflective' symmetry for R_1.

Symmetry proof for R_2. We now do a similar thing for R_2. So let $a^i b \in R_2 b$, so that $tr(\alpha z^{2i+1}) \in Q$. Then acting by the Galois automorphism we get

$$
tr(\alpha^q z^{(2i+1)q}) = tr(\alpha z^{(2i+1)q+(q^2-1)/2}) = tr(\alpha z^{2(iq+(q^2-1)/4+(2p-1))+1}) \in Q.
$$

This similarly gives the involutive map

$$i \mapsto iq + (q^2 - 1)/4 + (2p - 1) \equiv -i - 1 \bmod 4p. \tag{5.3}$$

□

6 The Doubling Process

Lemma 6.1 *Let $D \subset G = \mathrm{Dic}_v = \langle x, y\rangle, v = 4n, k = 2n - 1, \lambda = n - 1$. Let $K = \langle x\rangle$, $k_1 = n - 1, k_2 = n$ and let $D = D_1 + D_2 y$, $D_i \subset K, k_i = |D_i|$. Then the requirement that $D = D_1 + D_2 y$ is a SRHDS is equivalent to (a)–(d):*

$$(a)\ D_1 H = K - H,\ \ (b)\ D_1^{(-1)} = tD_1,\ \ (c)\ D_2 H = K,$$
$$(d)\ \lambda(K - H) + k = D_1 D_1^{(-1)} + D_2 D_2^{(-1)}.$$

Proof One checks that $D = D_1 + D_2 y$ is a SRHDS is equivalent to the conditions

(i) $D_1 \cup \{1\}$ and D_2 are transversals for K/H (this comes from looking at $G - H = D + D^{(-1)} = D_1 + D_2 y + (D_1^{(-1)} + (D_2 y)^{(-1)})$).
(ii) $\lambda D_1 H + k = D_1 D_1^{(-1)} + D_2 D_2^{(-1)}$;
(iii) $\lambda K y = D_2 D_1 y + D_1 D_2 y^{-1}$ (from $DD^{(-1)} = \lambda(G - H) + k$);
(iv) $D_1^{(-1)} = tD_1$ and $D_i^y = D_i^{(-1)}$.

Now (iii) is equivalent to $D_1 D_2(1 + t) = \lambda K$ or $D_1 K = \lambda K$. But $D_1 K = \lambda K$ follows directly from $D_i \subset K$, and $|D_1| = \lambda$. Thus (ii) and (iii) are equivalent to $\lambda D_1 H + k = D_1 D_1^{(-1)} + D_2 D_2^{(-1)}$. □

Write $D = D_0 + D_1 y$. We construct the set $E \subseteq \mathrm{Dic}_{16p}$ as

$$E := E_0 + E_1 y \text{ with } E_0 := D_0 + D_1 x \quad\text{and}\quad E_1 := D_1^{(-1)} x^{-1} t + D_0^{(-1)} + 1.$$

We show that if D_1 satisfies the symmetry: $x^{2i} \in D_1$ implies $x^{4p-2i-2} \in D_1$, then E is a (v_2, k_2, λ_2)-SRHDS with $v_2 = 16p$, $k_2 = 8p - 1$, and $\lambda_2 = 4p - 1$.

Theorem 6.2 *Let $\mathrm{Dic}_{16p} = \langle x, y \mid x^{4p} = y^2, y^4 = 1, x^y = x^{-1}\rangle$, $t = y^2$. We let $\mathrm{Dic}_{8p} = \langle x^2, y\rangle \le \mathrm{Dic}_{16p}$. Let D be a (v_1, k_1, λ_1)-SRHDS in Dic_{8p}, with $v_1 = 8p$, $k_1 = 4p - 1$, and $\lambda_1 = 2p - 1$. Then the unique involution t in Dic_{16p} is the same as the unique involution in Dic_{8p}.*

Write $D = D_0 + D_1 y$, $D_i \subset \langle x^2\rangle$, and let $E = E_0 + E_1 y \subseteq \mathrm{Dic}_{16p}$ where:

$$E_0 := D_0 + D_1 x \quad\textit{and}\quad E_1 := D_1^{(-1)} x^{-1} t + D_0^{(-1)} + 1.$$

Assume that D_1 satisfies the symmetry: $x^{2i} \in D_1$ implies $x^{4p-2i-2} \in D_1$. Then E is a (v_2, k_2, λ_2)-SRHDS with $v_2 = 16p$, $k_2 = 8p - 1$, and $\lambda_2 = 4p - 1$.

Proof We note that $D^{(-1)} = tD$ implies that $E^{(-1)} = tE$. We also observe that the map $x^{2i} \to x^{4p-2i-2}$ is an involution. Using Lemma 6.1, to show E is a SRHDS it suffices to show that E satisfies

(1) $E \cup E^{(-1)} = \mathrm{Dic}_{16p} - \langle t \rangle$;

(2) $E \cap E^{(-1)} = \emptyset$;

(3) $E_0 E_0^{(-1)} + E_1 E_1^{(-1)} = \lambda_2(\langle x \rangle - \langle t \rangle) + k_2$.

This is sufficient because conditions (1) and (2) along with $E^{(-1)} = tE$ imply conditions (a) and (c) of Lemma 6.1. First we note that E does not contain t or the identity, as this would imply that D_0 contains these. We now show (2), which will imply (1). We split condition (2) into cases by considering the intersection of E with each coset of $\langle x^2 \rangle$, all of which cosets are their own inverses. There are four such cosets: $\langle x^2 \rangle$, $\langle x^2 \rangle x$, $\langle x^2 \rangle y$, and $\langle x^2 \rangle xy$.

$\langle x^2 \rangle$: For $E \cap \langle x^2 \rangle = D_0$, we know that $x^{2i} \in D_0$ implies $x^{-2i} \notin D_0$ since $D_0 \cap D_0^{(-1)} = \emptyset$.

$\langle x^2 \rangle x$: We have $E \cap \langle x^2 \rangle x = D_1 x$. We show $D_1 x \cap (D_1 x)^{(-1)} = \emptyset$.

$$\begin{aligned} x^{2i+1} \in D_1 x \iff x^{2i} \in D_1 \iff x^{4p-2i-2} \in D_1 \\ \iff x^{4p-2i-2} y \in D_1 y \iff t x^{4p-2i-2} y \notin D_1 y \\ \iff x^{-2i-2} \notin D_1 \iff x^{-2i-1} \notin D_1 x. \end{aligned} \tag{6.1}$$

Here we used the symmetry and the fact that $(D_1 y) \cap (D_1 y)^{(-1)} = \emptyset$ where $(D_1 y)^{(-1)} = t D_1 y$.

$\langle x^2 \rangle y$: Here we have $E \cap \langle x^2 \rangle y = D_0^{(-1)} y + y$. First we check that $D_0^{(-1)} y$ doesn't contain any of its inverses:

$$x^{-2i} y \in D_0^{(-1)} y \iff (x^{-2i} y)^{-1} = t x^{-2i} y \notin D_0^{(-1)} y.$$

We also check the additional y doesn't have an inverse in $D_0^{(-1)} y$:

$$t \notin D_0^{(-1)} \iff y^{-1} = ty \notin D_0^{(-1)} y.$$

$\langle x^2 \rangle xy$: Here we have $E \cap \langle x^2 \rangle xy = D_1^{(-1)} x^{-1} ty$, and

$$\begin{aligned} x^{-2i-1} ty \in D_1^{(-1)} x^{-1} ty \iff x^{2i} \in D_1 \iff t x^{2i} \notin D_1 \\ \iff t x^{-2i} \notin D_1^{(-1)} \iff x^{-2i-1} y = t x^{-2i} x^{-1} ty \notin D_1^{(-1)} x^{-1} ty. \end{aligned}$$

Thus $E \cap E^{(-1)} = \emptyset$. This concludes (2) and implies (1), since both E and $E^{(-1)}$ don't intersect $\langle t \rangle$ and $|E| = k_2 = 8p - 1$.

Now we prove (3): we have

$$\begin{aligned}E_0E_0^{(-1)} + E_1E_1^{(-1)} &= (D_0 + D_1x)\left(D_0^{(-1)} + D_1^{(-1)}x^{-1}\right)\\&\quad + \left(D_1^{(-1)}x^{-1}t + D_0^{(-1)} + 1\right)(D_1xt + D_0 + 1)\\&= 2D_0D_0^{(-1)} + 2D_1D_1^{(-1)}\\&\quad + (1+t)D_0D_1^{(-1)}x^{-1} + (1+t)D_1D_0^{(-1)}x\\&\quad + D_1xt + D_0 + D_1^{(-1)}x^{-1}t + D_0^{(-1)} + 1. \qquad (6.2)\end{aligned}$$

For E to be a SRHDS we need (6.2) to be equal to $\lambda_2(\langle x\rangle - \langle t\rangle) + k_2$. Looking at just the even powers of x, we need

$$2D_0D_0^{(-1)} + 2D_1D_1^{(-1)} + D_0 + D_0^{(-1)} + 1$$

to be equal to $\lambda_2(\langle x^2\rangle - \langle t\rangle) + k_2$. We note that $D_0 + D_0^{(-1)} = \langle x^2\rangle - \langle t\rangle$, and $D_0D_0^{(-1)} + D_1D_1^{(-1)} = \lambda_1(\langle x^2\rangle - \langle t\rangle) + k_1$ since D is a SRHDS for $\langle x^2, y\rangle$. Since $\frac{k_2-1}{2} = \lambda_2$, we have

$$\begin{aligned}&2(D_0D_0^{(-1)} + D_1D_1^{(-1)}) + (D_0 + D_0^{(-1)}) + 1\\&\quad = 2(\lambda_1(\langle x^2\rangle - \langle t\rangle) + k_1) + (\langle x^2\rangle - \langle t\rangle) + 1\\&\quad = (2\lambda_1 + 1)(\langle x^2\rangle - \langle t\rangle) + (2k_1 + 1) = \lambda_2(\langle x^2\rangle - \langle t\rangle) + k_2,\end{aligned}$$

as desired. We now look at the odd powers of x in (6.2), which must equal $\lambda_2\langle x^2\rangle x$. We see that

$$\begin{aligned}&(1+t)D_0D_1^{(-1)}x^{-1} + (1+t)D_1D_0^{(-1)}x + D_1xt + D_1^{(-1)}x^{-1}t\\&\quad = (1+t)\,(D_0+1)\,D_1^{(-1)}x^{-1} + (1+t)\,(D_0+1)^{(-1)}\,D_1x\\&\qquad - (D_1x)^{(-1)} + D_1x. \qquad (6.3)\end{aligned}$$

Looking at the first two terms of (6.3), $D_0 + 1$ is a transversal of $\langle t\rangle$ in $\langle x^2\rangle$, so $(1+t)\,(D_0+1) = \langle x^2\rangle$ and $(1+t)\,(D_0+1)^{(-1)} = \langle x^2\rangle$. So we can reduce (6.3) to

$$\langle x^2\rangle D_1^{(-1)}x^{-1} + \langle x^2\rangle D_1x - (D_1x)^{(-1)} + D_1x.$$

To evaluate the last two terms of (6.3), we note that (6.1) gives us: if $x^{2i} \in D_1$, then $x^{-2i-2} \notin D_1$. Thus D_1 and $\left(D_1x^2\right)^{(-1)}$ are disjoint, so their sum is $\langle x^2\rangle$ since $|D_1| = 4p$. Thus $(D_1x)^{(-1)} + D_1x = \left(\left(D_1x^{-2}\right)^{(-1)} + D_1\right)x = \langle x^2\rangle x$. So the sum of the odd powered terms is

$$\begin{aligned}&\langle x^2\rangle\,(D_1)^{(-1)}\,x^{-1} + \langle x^2\rangle D_1x - \langle x^2\rangle x = D_1^{(-1)}\langle x^2\rangle x^{-1} + (D_1 - 1)\langle x^2\rangle x\\&\quad = |D_1|\langle x^2\rangle x + (|D_1| - 1)\langle x^2\rangle x = \lambda_2\langle x^2\rangle x\end{aligned}$$

as desired. Therefore we have shown (3), and E is a SRHDS. □

Corollary 6.3 *The set $E = E_0 + E_1 y$ as defined above is an SRHDS in* Dic_{16p} *if $D = D_0 + D_1 y$ is an SRHDS in* Dic_{8p} *and $x^{2i} \in D_1$ implies $x^{-2i-2} \in D_1$.*

Proof This follows by applying the automorphism $\varphi(x) = x, \varphi(y) = x^{2p} y$ to Dic_{16p} in the preceding theorem. We have that D is a SRHDS for Dic_{8p} if and only if $\varphi(D)$ is, and similarly E is a SRHDS for Dic_{16p} if and only if $\varphi(E)$ is. The condition $x^{2i} \in \varphi(D_1)$ implies $x^{-2i-2} \in \varphi(D_1)$ is equivalent to the condition $x^{2i} \in D_1$ implies $x^{4p-2i-2} \in D_1$. □

Many other equivalent symmetries can be obtained by using a different automorphism that fixes $\langle x \rangle$. The one we have used is that obtained at the end of Theorem 5.1. In the SRHDS $S = a^{2p} R_1 + R_2 b$ of Dic_{8p} from Theorem 5.1, we showed that $a^i \in R_2$ implies $a^{-i-1} \in R_2$. See (5.3). As a subgroup of Dic_{16p}, this is the necessary symmetry condition for Corollary 6.3 to apply. Thus Dic_{16p} is a SRHDS group when $4p - 1$ is a prime power. This proves Theorem 1.3. □

7 *D* and Cosets of Q_8

Let G be a SRHDS group with subgroup H and difference set D. Suppose that $Q \leq G$ has even order and that $g_0 = 1, \dots, g_{p-1}$ is a transversal for $Q \leq G$. Then we can write

$$D = F_0 g_0 + F_1 g_1 + \cdots + F_{p-1} g_{p-1}, \quad F_i \subset Q. \tag{7.1}$$

Lemma 7.1 *Let $Q \leq G$ be as above. For all subsets $F \subseteq Q$ of size greater than $|Q|/2$, the multiplicity of t in $FF^{(-1)}$ is greater than zero.* □

Proof Now $t \in Q$, so $H \leq Q$ and if $|F| > |Q|/2$, then some coset of $H \leq Q$ meets F in two elements and so $t \in FF^{(-1)}$. □

Now $DD^{(-1)} = \lambda(G - H) + k$ and a part of the left hand side is $\sum_{i=0}^{p-1} F_i F_i^{(-1)}$. Thus $|F_i| \leq |Q|/2$ when D is written as in Eq. (7.1).

Now let $f_i = |F_i|, 0 \leq i < p - 1$, so that

$$\sum_{i=0}^{p-1} f_i = |D| = k = \frac{(|G| - 2)}{2} = \frac{(|Q|p - 2)}{2} = \frac{|Q|}{2} p - 1.$$

Since $f_i \leq |Q|/2$ we must have $f_i = |Q|/2$ for all $0 \leq i \leq p - 1$ except one. To see that $f_0 = |Q|/2 - 1$ we just note that $Q - H$ has $|Q| - 2$ elements that come in inverse pairs. Thus $f_0 = |Q|/2 - 1$.

Next note that $DD^{(-1)} = \lambda(G - H) + k$ and $F_i F_i^{(-1)} \subseteq Q$. We want to show

$$\sum_{i=0}^{p-1} F_i F_i^{(-1)} = \lambda(Q - H) + k. \tag{7.2}$$

Now, $v = 8p, k = \frac{|Q|}{2}p - 1, \lambda = \frac{|Q|}{4}p - 1$ and so $\lambda(Q - H) + k$ has $(\frac{|Q|}{4}p - 1)(|Q| - 2) + (\frac{|Q|}{2}p - 1) = \frac{|Q|^2}{4}p - |Q| + 1$ elements, while $\sum_{i=0}^{p-1} F_i F_i^{(-1)}$ has $\left(\frac{|Q|}{2} - 1\right)^2 + (p-1)\left(\frac{|Q|}{2}\right)^2 = \frac{|Q|^2}{4}p - |Q| + 1$ elements, so we must have Eq. (7.2).

For $Q = Q_8$, considering those F_i of size $|Q|/2 = 4$ a Magma [12] calculation gives the following result by finding all those subsets $F \subset Q_8$ such that $FF^{(-1)}$ does not contain t:

Lemma 7.2 *Suppose that $Q = Q_8 \le G$. Then each F_i of size 4 is one of the following 16 sets:*

$$\begin{aligned}
&\{1, x, y, xy\};\quad \{1, x, y, x^3y\};\quad \{x, x^2, x^2y, x^3y\};\quad \{1, x, x^2y, x^3y\};\\
&\{1, x^3, x^2y, x^3y\};\quad \{1, x^3, y, xy\};\quad \{x, x^2, y, x^3y\};\quad \{x^2, x^3, y, x^3y\};\\
&\{x, x^2, xy, x^2y\};\quad \{x^2, x^3, xy, x^2y\};\quad \{x^2, x^3, y, xy\};\quad \{1, x, xy, x^2y\};\\
&\{x, x^2, y, x^2y\};\quad \{x^2, x^3, x^2y, x^3y\};\quad \{1, x, xy, x^2y\};\quad \{1, x^3, y, x^3y\}.\square
\end{aligned}$$

Each of these is a relative difference set for Q_8. Thus each $F_i, i > 0$, is a relative difference set for Q_8. It follows then from Eq. (7.2) that F_0 is a SRHDS for Q_8. Thus F_0 is determined by

Lemma 7.3 *The following sets are equal:*

(i) *The set of all SRHDS for $Q_8 = \langle i, j, k\rangle$.*
(ii) *The set of all conjugate* (by elements of Q_8)*-translates* (by elements of H) *of $\{i, j, k\}$.*
(iii) *The set of all $\{a, b, c\} \subset Q_8 \backslash H$ where $|\{a, b, c\}| = 3$ and $t \notin \{uv^{-1} : u, v \in \{a, b, c\}\}$.* □

Call this common set $\mathcal{S}$ and note that $|\mathcal{S}| = 8$.

Now any F_0 must satisfy (iii), so $F_0 \in \mathcal{S}$. Further, we can choose F_0 to be any element of $\mathcal{S}$ by applying the operations in (ii) to D, which still result in a SRHDS.

Assume that $G = \mathrm{Dic}_{8p}$ so that a transversal of $Q_8 \le G$ is $1, x, \ldots, x^{p-1}$. Now we can write $D = F_0 + F_1x + F_2x^2 + \cdots + F_{p-1}x^{p-1}$ where $F_i \subset Q_8$ and $F_0 \in \mathcal{S}$.

Here each $F_i, i > 0$, is one of the 16 subsets of Q_8 in Lemma 7.2 and $F_i = (1 + x^p)(a + by) = a + by + x^pa + x^pby,$ where $a, b \in \langle x^p\rangle$.

Now $D^{(-1)}t = D$ and so if $F_ix^i \subset D$, then $t(F_ix^i)^{(-1)} = tx^{-i}F_i^{(-1)} \subset D$. Here $F_i^{(-1)} = a^{-1} + bty + x^{-p}a^{-1} + x^pbty$, and so

$$\begin{aligned}
t(F_ix^i)^{(-1)} &= tx^{-1}F_i^{(-1)} = tx^{-i}(a^{-1} + bty + x^{-p}a^{-1} + x^pbty)\\
&= ta^{-1}x^{-i} + tx^{-p}a^{-1}x^{-i} + byx^i + x^pbyx^i.
\end{aligned}$$

Thus F_i and $t(F_ix^i)^{(-1)}$ have $byx^i + x^pbyx^i$ in common and so

$$F_ix^i \cup t(F_ix^i)^{(-1)} = ax^i + byx^i + x^pax^i + x^pbyx^i + ta^{-1}x^{-i} + tx^{-p}a^{-1}x^{-i}.$$

We denote this by $J_i(a, b)$, so that D is a union of D_0 and some of the $J_i(a, b)$.

Now $J_i(a,b)$ has four elements in Q_8x^i and has two elements in Q_8x^{-i}. Since we know that each non-trivial coset of Q_8 has to contain four elements of D we know that D has to contain some $J_{-i}(c,d)$ so that

$$(a+x^pa)x^i+(a^{-1}+x^{-p}a^{-1})tx^{-i}=(c+x^pc)x^{-i}+(b^{-1}+x^{-p}b^{-1})tx^i.$$

This is true if and only if we have $a+x^pa=b^{-1}t+x^{-p}b^{-1}t$ and $(a^{-1}+x^{-p}a^{-1})t=b+x^pb$. However these equations are equivalent and we note that for any choice of $a\in\langle x^p\rangle$ there is a $b\in\langle x^p\rangle$ that solves the first equation.

Thus we now obtain eight element sets by taking the union of these two $J's$. We denote these by $L_i(a,b,c)$:

$$\begin{aligned}&(a+x^pa)x^i+(a^{-1}+x^{-p}a^{-1})tx^{-i}+(by+x^pby)x^i+(cy+x^pcy)x^{-i}\\&\quad=(1+x^p)(a+by)x^i+(1+x^p)(x^pa^{-1}+cy)x^{-i}.\end{aligned}$$

We note that $L_i(a,b,c)=L_j(a',b',c')$ if and only if $i=j, a=a', b=b', c=c'$. For $1\le i\le p-1$ let $\mathcal{L}_i=\{L_i(a,b,c):a,b,c\in\langle x^p\rangle\}$. Then $|\mathcal{L}_i|=64$.

8 Groups that are not SRHDS Groups

Proposition 8.1 *The dicyclic group* Dic_{72} *is not a SRHDS group.*

Proof Suppose it is and that D is the SRHDS. Let $G=\mathrm{Dic}_{72}=\langle x,y|x^{36}=1,y^2=x^{18},x^y=x^{-1}\rangle$. Then by the above section there are $D_i\in\mathcal{L}_i$, $1\le i\le 4$, such that $D=D_0+\sum_{i=1}^4 D_i$. There are $64=|L_i|$ choices for each D_i, $1\le i\le 4$. Using the standard irreducible representation $\rho:\mathrm{Dic}_{72}\to\mathrm{GL}(2,\mathbb{C})$ given by $\rho(x)=\begin{bmatrix}\zeta_{36}&0\\0&\zeta_{36}^{-1}\end{bmatrix}$, $\rho(y)=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$, $\zeta_{36}=e^{2\pi i/36}$, we have $\rho(G)=\rho(H)=0$. From $D+D^{(-1)}=G-H$ we then have $\rho(D)+\rho(D^{(-1)})=0$. By $DD^{(-1)}=\lambda(G-H)+k$ we have $\rho(D)\rho(D^{(-1)})=kI_2=35I_2$. Therefore, $35I_2=\rho(D)\rho(D^{(-1)})=-\rho(D)^2$. A Magma calculation determines that of the 64^4 possibilites for D, only 648 have $\rho(D)^2=-35I_2$. Another Magma [23] calculation verifies that none of these 648 give a SRHDS, completing the proof. □

Proposition 8.2 *Let G be a group where $Q_8\le G$. Suppose that there is an epimorphism $\pi:G\to\mathcal{C}_p\times Q_8$ for p prime where $\pi(Q_8)=\{1\}\times Q_8$ and $|\ker\pi|$ is odd. Then G is not a SRHDS group.*

Proof So suppose that G is a SRHDS group with difference set D and subgroup $H=\langle t\rangle$. Let $Q_8=\langle x,y|x^4,x^2=y^2,x^y=x^{-1}\rangle\le G$, so that $t=x^2,\pi(x)=x,\pi(y)=y$. First note that p must be odd since G has a unique involution. Let $N=\ker\pi$. Put $\mathcal{C}_p=\langle\pi(r)\rangle$, $r\in G$, so that we can write

$$D=\sum_{i=0}^{p-1}\sum_{j=0}^{3}r^ix^jD_{0,i,j}+\sum_{i=0}^{p-1}\sum_{j=0}^{3}r^ix^jyD_{1,i,j},\quad D_{k,i,j}\subset N.$$

We note that $|D_{i,j,k}| \le |N|$.

Let $p_2 = (p-1)/2$. We can also write $D = \sum_{i=0}^{p-1} r^i D_i$, $D_i \subset \langle x, y, N \rangle$ so that

$$D_i = \sum_{j=0}^{3} x^j D_{0,i,j} + \sum_{j=0}^{3} x^j y D_{1,i,j}$$

From $D^{(-1)} = tD$ we get $D_i^{(-1)} r^{-i} = tr^{p-i} D_{p-i}, 0 \le i < p$, so that $D_{p-i} = tr^{-p}(D_i^{(-1)})^{r^{-i}}$. Thus $D = D_0 + \sum_{i=1}^{p_2} r^i D_i + r^{-i} t (D_i^{(-1)})^{r^{-i}}$.

Now let $\rho : Q_8 \to \mathrm{GL}(2, \mathbb{Q}(i)), i = \sqrt{-1}$, be an irreducible faithful unitary representation of Q_8 where $\rho(x) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\rho(y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Then the $\mathbb{Q}$-span of the image of ρ has basis

$$B_1 = I_2, \quad B_2 = \rho(x) = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad B_3 = \rho(y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad B_4 = \rho(xy) = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

since $\rho(x^2) = -B_1$. We note from Lemma 7.3 that we may assume $D_0 = \{x, y, xy\}$, so $\rho(D_0) = \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} = B_2 + B_3 + B_4$.

Let $\omega = \exp 2\pi i/p$. Then π, ρ and $r \mapsto \omega I_2$ determine an irreducible unitary representation of G that we also call ρ. Then $\rho(r^i D_i) = \omega^i \sum_{j=1}^{4} a_{ij} B_j$, where $a_{ij} \in \mathbb{Z}$, so that

$$\rho\big(r^{-i} t \big(D_i^{(-1)}\big)^{r^{-i}}\big) = -\omega^{-i} \rho\big(D_i^{(-1)}\big)^{r^{-i}}\big) = -\omega^{-i} \rho\big(D_i^{(-1)}\big) = -\omega^{-i} \sum_{j=1}^{4} a_{ij} B_j^*.$$

Here $B_1^* = B_1$, $B_2^* = -B_2$, $B_3^* = -B_3$, $B_4^* = -B_4$.

This gives

$$\begin{aligned} \rho(D) &= \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{i=1}^{p_2} \rho\big(D_i r^i + r^{-i} t \big(D_i^{(-1)}\big)^{r^{-i}}\big) \\ &= \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{i=1}^{p_2} \sum_{j=1}^{4} \big(a_{ij} B_j \omega^i - a_{ij} B_j^* \omega^{-i}\big). \end{aligned} \tag{8.1}$$

We can write this as

$$\rho(D) = \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{u=1}^{4} a_u B_u, \text{ where } a_u \in \mathbb{Z}[\omega]. \tag{8.2}$$

From $DD^{(-1)} = \lambda(G - H) + k$ and $D^{(-1)} = tD$ we get $D^2 = \lambda(G - H) + kt$. Now if $\rho(D)^2 = (e_{ij})$, then from $(e_{ij}) = \rho(D^2) = \rho(\lambda(G - H) + tk) = -kI_2$ and

Eq. (8.2) we get

$$0 = e_{11} - e_{22} = 4ia_1(1 + a_2), \;\; 0 = e_{12} = 2a_1(i + 1 + a_3 + ia_4),$$
$$0 = e_{21} = 2a_1(-1 + i - a_3 + ia_4).$$

Solving, we must have either

$$(i)\;\; a_1 = 0; \;\text{ or } (ii)\;\; a_2 = -1, \;\; a_3 = -1, \;\; a_4 = -1.$$

Now we find $a_1, \cdots, a_4$ in terms of the a_{ij}. From (8.1) and (8.2) we have

$$\begin{aligned}\sum_{u=1}^{4} a_u B_u &= \sum_{i=1}^{p_2}\sum_{j=1}^{4} a_{ij} B_j \omega^i - a_{ij} B_j^* \omega^{-i} \\ &= \sum_{i=1}^{p_2} a_{i1} B_1 \omega^i - a_{i1} B_1 \omega^{-i} + a_{i2} B_2 \omega^i + a_{i2} B_2 \omega^{-i} \\ &\quad + a_{i3} B_3 \omega^i + a_{i3} B_3 \omega^{-i} + a_{i4} B_4 \omega^i + a_{i4} B_4 \omega^{-i}.\end{aligned}$$

From this we get

$$a_1 = \sum_{i=1}^{p_2} a_{i1}(\omega^i - \omega^{-i}); \quad a_2 = \sum_{i=1}^{p_2} a_{i2}(\omega^i + \omega^{-i});$$
$$a_3 = \sum_{i=1}^{p_2} a_{i3}(\omega^i + \omega^{-i}); \quad a_4 = \sum_{i=1}^{p_2} a_{i4}(\omega^i + \omega^{-i}).$$

Now if we have (i) $a_1 = 0$, then $p > 2$ is a prime means that the $\omega^i - \omega^{-i}, i = 1, 2, \cdots, p_2$ are linearly independent over $\mathbb{Q}$, so that we must than have $a_{i1} = 0$ for all i.

Observe from previous definitions that $a_{i1} = |D_{0,i,0}| - |D_{0,i,2}|$. From $D^{(-1)} = tD$ and $D \cup D^{(-1)} = G - \langle t \rangle$ we have $|D_{0,i,0}| + |D_{0,i,2}| = |N|$. So $|D_{0,i,0}| = |D_{0,i,2}| = |N|/2$. Thus $|N|$ is even, which contradicts our assumption on $\ker \pi$.

So now assume (ii), so that

$$\begin{aligned}\rho(D) &= \begin{bmatrix} i & -i-1 \\ 1-i & -i \end{bmatrix} + \sum_{i=1}^{4} a_i B_i \\ &= \begin{bmatrix} i & -i-1 \\ 1-1 & -i \end{bmatrix} + a_1 B_1 - B_2 - B_3 - B_4 = a_1 I_2.\end{aligned}$$

But $-\rho(D^2) = \rho(DD^{(-1)}) = kI_2$ then gives $a_1^2 = -k$. Here $a_1 \in \mathbb{Q}[\omega]$. Recall that $\omega = e^{\frac{2\pi i}{p}}$, so the Galois group of $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is cyclic of even order $p - 1$. By the Galois correspondence, $\mathbb{Q}(\omega)$ has a unique quadratic subfield. In particular, we can verify that the subfield is exactly $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$. This follows from the Gauss sum:

$$\left(\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\omega^n\right)^2 = (-1)^{\frac{p-1}{2}}p$$

Note that $k \equiv 3 \pmod 4$ so k is not an integer square. Therefore $a_1^2 = -k$ implies $k = px^2$ for some $x \in \mathbb{Z}$. However, $k = 4p|N| - 1$ so we have a contradiction, as k must be congruent to both 0 and $-1 \pmod p$. □

9 Groups of Order Less Than or Equal to 72

Here are the non-dicyclic groups (using magma notation) of order at most 72 that meet the following requirements: (i) they are not abelian; (ii) their Sylow 2-subgroups are generalized quaternion groups; (iii) they have a single involution.

$$G_{24,3},\quad G_{24,11},\quad G_{40,11},\quad G_{48,18},\quad G_{48,27},\quad G_{48,28},\quad G_{72,3},$$
$$G_{72,11},\quad G_{72,24},\quad G_{72,25},\quad G_{72,26},\quad G_{72,31},\quad G_{72,38}$$

We note that all of the dicyclic groups of order less than 72 and divisible by 8 are SRHDS groups by Theorems 1.2 and 1.3, while Dic_{72} is not by Proposition 8.1.

We will determine whether the remaining groups have a SRHDS. If they have a SRHDS then we give a SRHDS explicitly. If not, then we give a proof that the group is not a SRHDS group.

In the cases of $G_{72,3}$, $G_{72,11}$, $G_{72,24}$, $G_{72,25}$, and $G_{72,31}$, we use the following process to show they are not SRHDS groups: Given one of the four groups G, we take a right transversal $g_0 = 1, \ldots, g_8$ for $Q_8 \leq G$. Assuming there is an SRHDS D, we write D as in (7.1). We can assume $F_0 = \{x, y, xy\}$ by Lemma 7.3. By Lemma 7.2, there are 16 possibilities for each F_i, and a Magma [23] calculation verifies that none of these combinations give a SRHDS.

(1) $G_{24,3} = \mathrm{SL}(2,3) = \langle a, b, c, d | a^3 = 1, b^2 = d, c^2 = d, d^2, b^a = c, c^a = b c, c^b = cd\rangle$. Here $D = \{a^2cd, abcd, acd, cd, a^2bd, a^2d, a^2bc, a, bc, ab, b\}$.
(2) $G_{24,11} = \mathcal{C}_3 \times Q_8$. This is not a SRHDS group by Proposition 8.2.
(3) $G_{40,11} = \mathcal{C}_5 \times Q_8$. This is not a SRHDS group by Proposition 8.2.
(4) $G_{48,18} = \mathcal{C}_3 \rtimes \mathrm{Dic}_{16} = \langle a, b, c, d, e | d^2 = e^3 = 1, a^2 = b^2 = c^2 = d, b^a = bc, c^a = c^b = cd, d^a = d^b = d^c = d, e^a = e^2, e^b = e^c = e^d = e\rangle$ and let D be

$$\{ade^2, de^2, ae, e, abce^2, abc, bce^2, abde^2, bde^2, bce, acd, acde^2, abd,$$
$$cde^2, cd, acde, cde, bde, bcd, a, abcde, b, abe\}.$$

(5) $G_{48,27} = \mathcal{C}_3 \times \mathrm{Dic}_{16}$. We show $G_{48,27}$ is not a SRHDS group. Let $\mathcal{C}_3 = \langle r\rangle$. Then $D = D_0 + D_1 r + D_2 r^2$, $D_i \subset \mathrm{Dic}_{16}$. Now $D^{(-1)} = tD$ gives $D_0^{(-1)} = tD_0$ and

$D_2 = tD_1^{(-1)}$. Also Lemma 3.1 shows that the sizes of D_0, D_1, D_2 are 7, 8, 8 (in some order). By replacing D by $r^i D$ if necessary we may assume that $|D_0| = 7$ and that D_0+1, D_1, D_2 are transversals for G/H. Using $D_0^{(-1)} = tD_0$ one sees that there are 64 possible D_0s and 256 possible D_1s. Further, D_2 is determined by $D_2 = tD_1^{(-1)}$. There are thus $64 \cdot 256$ possibilities for D and one checks that none of these give a SRHDS.

(6) Let $G_{48,28} = \langle a, b, c, d, e | b^3 = e^2 = 1, a^2 = c^2 = d^2 = e, b^a = b^2, c^a = d, c^b = de, d^a = c, d^b = cd, d^c = de, e^a = e^b = e^c = e^d = e\rangle$. Here one D is

$$\{ab^2de, ab^2cde, b^2cde, ce, abc, b^2c, bc, d, ade, ab^2ce, ac, ab^2, acd, cd, b^2d, b^2e, abde, bde, bcd, a, ab, abcde, b\}.$$

(7) $G_{72,3} = Q_8 \rtimes \mathcal{C}_9 = \langle i, j, b | i^4 = j^4 = b^9 = 1, i^j = i^{-1}, i^2 = j^2, i^b = j, j^b = ij\rangle$. The Magma search described at the beginning of this section shows this is not an SRHDS group.

(8) $G_{72,11} = \mathcal{C}_9 \times Q_8$. The Magma search described at the beginning of this section shows this is not an SRHDS group.

(9) $G_{72,24} = \mathcal{C}_3^2 \rtimes Q_8 = \langle a, b, i, j | a^3 = b^3 = i^4 = j^4 = 1, ab = ba, i^j = i^{-1}, i^2 = j^2, a^i = a, b^i = b^2, a^j = a^2, b^j = b\rangle$. The Magma search described at the beginning of this section shows this is not an SRHDS group.

(10) $G_{72,25} = \mathcal{C}_3 \times SL(2, 3)$. The Magma search described at the beginning of this section shows this is not an SRHDS group.

(11) $G_{72,26} = \mathcal{C}_3 \times Dic_{24}$. This is not an SRHDS group by Proposition 8.2.

(12) $G_{72,31} = \mathcal{C}_3^2 \rtimes Q_8 = \langle a, b, i, j | a^3 = b^3 = i^4 = j^4 = 1, ab = ba, i^j = i^{-1}, i^2 = j^2, a^i = a^2, b^i = b^2, a^j = a, b^j = b\rangle$. The Magma search described at the beginning of this section shows this is not an SRHDS group.

(13) $G_{72,38} = \mathcal{C}_3^2 \times Q_8$. This is not an SRHDS group by Proposition 8.2.

Acknowledgements All computations made in the preparation of this paper were accomplished using Magma [23]. The first, second, third, and fifth authors thank Brigham Young University Department of Mathematics for funding during the writing of this paper. We are also grateful for useful suggestions from a referee.

Funding The first, second, third, and fifth authors thank Brigham Young University Department of Mathematics for funding during the writing of this paper.

Data Availibility All data generated or analysed during this study are included in this published article.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

1. Chen, Y.Q., Feng, T.: Abelian and non-abelian Paley type group schemes. Preprint
2. Cohen, H.: A Course in Computational Algebraic Number Theory, GTM, vol. 138. Springer, Berlin (1996)
3. Ding, C., Yuan, J.: A family of skew Hadamard difference sets. J. Combin. Theory Ser. A **113**, 1526–1535 (2006)
4. Ding, C., Wang, Z., Xiang, Q.: Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in PG(3,32h+1). J. Combin. Theory Ser. A **114**, 867–887 (2007)
5. Evans, R.J.: Nonexistence of twentieth power residue difference sets. Acta Arith. **84**, 397–402 (1999)
6. Feng, T., Xiang, Q.: Strongly regular graphs from union of cyclotomic classes. arXiv:1010.4107v2. MR2927417
7. Ikuta, T., Munemasa, A.: Pseudocyclic association schemes and strongly regular graphs. Eur. J. Combin. **31**, 1513–1519 (2010)
8. Coulter, R.S., Gutekunst, T.: Special subsets of difference sets with particular emphasis on skew Hadamard difference sets. Des. Codes Cryptogr. **53**(1), 1–12 (2009)
9. Isaacs, I.: Martin finite group theory. In: Graduate Studies in Mathematics, vol. 92. American Mathematical Society, Providence, pp. xii+350 (2008)
10. Babai, L., Cameron, P.J.: Automorphisms and enumeration of switching classes of tournaments. Electron. J. Combin. **7**, Research Paper 38 (2000)
11. https://cameroncounts.wordpress.com/2011/06/22/groups-with-unique-involution
12. Malzan, J.: On groups with a single involution. Pac. J. Math. **57**(2), 481–489 (1975)
13. Malzan, J.: Corrections to: "On groups with a single involution" (Pacific J. Math. 57 (1975), no. 2, 481–489). Pac. J. Math. **67**(2), 555 (1976)
14. Isaacs, I.M.: Real representations of groups with a single involution. Pac. J. Math. **71**(2), 463–464 (1977)
15. Schmidt, B.: Williamson matrices and a conjecture of Ito's. Des. Codes Cryptogr. **17**(1–3), 61–68 (1999)
16. Ito, N.: On Hadamard groups. III. Kyushu J. Math. **51**(2), 369–379 (1997)
17. Muzychuk, M., Ponomarenko, I.: Schur rings. Eur. J. Combin. **30**(6), 1526–1539 (2009)
18. Schur, I.: Zur Theorie der einfach transitiven Permutationsgruppen, pp. 598–623. Sitz. Preuss. Akad. Wiss, Berlin, Phys-math Klasse (1933)
19. Wielandt, H.: Finite Permutation Groups. Academic Press, New York–London, pp. x+114 (1964)
20. Wielandt, H.: Zur theorie der einfach transitiven permutationsgruppen II. Math. Z. **52**, 384–393 (1949)
21. Moore, E.H., Pollatsek, H.S.: Difference sets. Connecting algebra, combinatorics, and geometry. In: Student Mathematical Library, vol. 67, pp. xiv+298. American Mathematical Society, Providence (2013)
22. Pott, A.: Finite geometry and character theory. In: Lecture Notes in Mathematics, vol. 1601. Springer, Berlin (1995)
23. Bosma, W., Cannon, J.: MAGMA. University of Sydney, Sydney (1994)