Note

Hadamard Difference Sets in Groups of Order 64

DAVID GLUCK

Department of Mathematics, Wayne State University, Detroit, Michigan 48202

Communicated by William M. Kantor

Received April 8, 1985

A difference set in a group $G$ is a subset $D$ of $G$ such that every nonidentity element of $G$ has exactly $\lambda$ representations of the form $xy^{-1}$ with $x, y \in D$. The parameters $(v, k, \lambda, n)$ of $D$ are defined by $v = |G|$, $k = |D|$, $n = k - \lambda$. When $v = 4n$, we say that $D$ is Hadamard. A Hadamard difference set gives rise to a Hadamard matrix of order $v$; see [3, p. 71].

If $G$ is any group of order $4N^2$ which contains $N$ pairwise disjoint subgroups of order $2N$, then the nonidentity elements in those $N$ subgroups constitute a Hadamard difference set by [1, Theorem 1.1]. For $N > 3$, however, the only such groups of order $4N^2$ heretofore known to exist were elementary abelian 2-groups.

In this note we determine the groups $G$ of order 64 which contain 4 pairwise disjoint subgroups of order 8. We show that $G$ must be either elementary abelian or isomorphic to a group $G_0$ of nilpotence class two, $G_0$ is the semidirect product $\langle r \rangle \cdot V$, where $V$ is elementary abelian of order 32 and $r$ is an involution which acts on $V$ with two nontrivial Jordan blocks.

After submitting this paper for publication, I learned that an incomplete proof of the same result had been given by A. P. Sprague in [6]. Only the part of the proof not given in [6] will appear here. After my paper was written, D. Frohardt [3] showed that when $N > 4$, every group of order $4N^2$ containing $N$ pairwise disjoint subgroups of order $2N$ is an elementary abelian 2-group.

The difference set in $G_0$ does not appear to belong to any known family of difference sets in nonabelian groups. A general construction for Hadamard difference sets in nonabelian 2-groups is given in [2], but one can check that our difference set is not of that type.

Before proving our main result, we formally state our basic hypothesis.
and record two easy lemmas. Our group theory notation in this paper follows that of [4]. Basic facts about commutators in [4, Section 2.21] will be used without further reference.

**BASIC HYPOTHESIS.** Let $G$ be a group of order 64. Let $H_i$ be a subgroup of $G$ of order 8 for $1 \leq i \leq 4$. Suppose that $H_i \cap H_j = 1$ for $i \neq j$.

**LEMMA 1.** Suppose the basic hypothesis holds. Then $H_iH_j = G$ for $i \neq j$. If $i \neq j$ and $x, y \in G$, then $H_i^x \cap H_j^y = 1$.

*Proof.* The first statement is obvious. To prove the second, write $xy^{-1} = hk$, with $h \in H_i$ and $k \in H_j$. Then

$$H_i^x \cap H_j^y = (H_i^x)^y \cap H_j^y = (H_i \cap H_j)^y = (H_i \cap H_j)^{xy} = 1.$$ 

**LEMMA 2.** Let $u_1 = (12)$, $s_1 = (13)(24)$, and $t = (15)(26)(37)(48)$ be permutations in the symmetric group $S_8$. Let $z_1 = (12)(34)$ and let $u_2, s_2, z_2$ denote $u_1, s_1, z_1$. Let $D_1 = \langle u_1, s_1 \rangle$ and $D_2 = \langle u_2, s_2 \rangle = D_1'$. Then

(a) $u_1, s_1,$ and $t$ generate a 2-Sylow subgroup $T$ of $S_8$.

(b) $D_1$ and $D_2$ are dihedral of order 8 and $|T: D_1 \times D_2| = 2$.

(c) $Z(D_1) = \langle z_1 \rangle$ and $Z(D_2) = \langle z_2 \rangle$.

(d) Let $f = (1324)(5867)$. Then $f \in T'$.

*Proof.* Parts $a, b,$ and $c$ are straightforward. For $(d)$, note that $f = [u_1s_1, t]$.

**THEOREM.** Let $G$ satisfy the basic hypothesis. Then $G$ is elementary abelian or $G \cong G_0$.

**Step 1.** $|\Omega_1(Z(G))| \geq 8$.

*Proof.* If each $H_i$ meets $Z(G)$ then $Z(G)$ contains four distinct involutions, so that $|\Omega_1(Z(G))| \geq 8$. Hence we assume that $H_1$, say, does not meet $Z(G)$. Since $G$ is nilpotent, this implies that $H_1$ contains no nontrivial normal subgroup of $G$, and so $G$ is faithfully represented as a permutation group on the 8 cosets of $H_1$ in $G$. Using the notation of Lemma 2, we view $G$ as a subgroup of $T$. Then $|T: G| = 2$ and Lemma 1 implies that $H_2, H_3,$ and $H_4$ are transitive on $\{1, 2, \ldots , 8\}$. Thus the nonidentity elements of $H_2, H_3,$ and $H_4$ fix no points in $\{1, 2, \ldots , 8\}$. Let $J_i = H_i \cap (D_1 \times D_2)$ for $2 \leq i \leq 4$. The preceding sentences imply that $|J_i| = 4$ for $2 \leq i \leq 4$.

Let $s$ be a fixed point free permutation in $D_1 \times D_2$. Write $s = s_1s_2$ with $s_1 \in D_1, s_2 \in D_2$. If $|s_1| = 2$ and $|s_2| = 4$, then $s^2$ is not fixed point free. Hence $s \notin J_2 \cup J_3 \cup J_4$. A similar conclusion holds when $|s_1| = 4$ and $|s_2| = 2$. If
$|s_1| = |s_2| = 4$, then $s^2 = z_1 z_2$. We may assume $z_1 z_2 \notin J_3 \cup J_4$. Let $\mathcal{S}$ denote the set of quadruple transpositions in $D_1 \times D_2$. Then $|\mathcal{S}| = 9$ and $J_3 \cup J_4 \subseteq \mathcal{S} \cup \{1\}$.

Since $|T: G| = 2$, Lemma 2(d) implies that $f \in G$. For $s \in \mathcal{S} - \{z_1 z_2\}$, we have $[s, f] \in \{z_1, z_2, z_1 z_2\}$. Since the last set does not meet $J_3 \cup J_4$, it follows that $f$ normalizes neither $J_3$ nor $J_4$. Hence $J_3 \cup J'_4$ contains at least 5 elements of $\mathcal{S}$, and so does $J_4 \cup J'_4$. By Lemma 1, $J_3 \cup J'_4$ does not meet $J_4 \cup J'_4$. The last two sentences imply that $|\mathcal{S}| \geq 10$, which is absurd.

Thus $\Omega_1(Z(G)) \geq 8$. The rest of the proof is covered by [6], and is omitted.

REFERENCES