# Constructions of difference sets in nonabelian 2-groups

Taylor Applebaum[*] John Clikeman[†] James A. Davis[‡]
John F. Dillon[§] Jonathan Jedwab[¶] Tahseen Rabbani[‖]
Ken Smith[**] William Yolland[††]

March 27, 2020 (revised February 4, 2022)

*Dedicated to the memory of Robert A. Liebler, a friend and mentor, and a passionate advocate for studying the action of finite nonabelian groups on combinatorial designs.*

**Abstract**

Difference sets have been studied for more than 80 years. Techniques from algebraic number theory, group theory, finite geometry, and digital communications engineering have been used to establish constructive and nonexistence results. We provide a new theoretical approach which dramatically expands the class of 2-groups known to contain a difference set, by refining the concept of covering extended building sets introduced by Davis and Jedwab in 1997. We then describe how product constructions and other methods can be used to construct difference sets in some of the remaining 2-groups. In particular, we determine that all groups of order 256 not excluded by the two classical nonexistence criteria contain a difference set, in agreement with previous findings for groups of order 4, 16, and 64. We provide suggestions for how the existence question for difference sets in 2-groups of all orders might be resolved.

## 1 Motivation and Overview

Difference sets were introduced by Singer [33] in 1938 as regular automorphism groups of projective geometries. These examples are contained in the multiplicative group of a finite field, and hence the difference sets in those geometric settings occur in cyclic groups. In the decades following, difference sets were discovered in other abelian groups and subsequently in nonabelian groups. The central objective is to determine which groups contain at least one difference set. Researchers have developed a range of techniques in pursuit of this objective, taking advantage of connections with design theory, coding theory, cryptography, sequence design, and digital communications.

A $k$-subset $D$ of a group $G$ of order $v$ is a *difference set* with parameters $(v, k, \lambda)$ if, for all nonidentity elements $g$ in $G$, the equation

$$xy^{-1} = g$$

has exactly $\lambda$ solutions $(x, y)$ with $x, y \in D$; the related parameter $n$ is defined to be $k - \lambda$. The complement of a difference set with parameters $(v, k, \lambda)$ is itself a difference set, with parameters $(v, v-k, v-2k+\lambda)$ and the same related parameter $n$. The difference set is nontrivial if $1 < k < v - 1$. A $(v, k, \lambda)$ difference set in $G$ is equivalent to a symmetric $(v, k, \lambda)$ design with a regular automorphism group $G$ [4].

Given an element $A = \sum_{g \in G} a_g g$ in the group ring $\mathbb{Z}G$, where each $a_g \in \mathbb{Z}$, we write $A^{(-1)}$ for the element $\sum_{g \in G} a_g g^{-1}$. It is customary in the study of difference sets to abuse notation by identifying a subset $D$ of a

[*]University of Richmond VA, now at Google, applebaum.taylor@gmail.com
[†]University of Richmond VA, now at Google, jclikeman@gmail.com
[‡]University of Richmond VA, jdavis@richmond.edu; supported by NSA grant H98230-12-1-0243
[§]National Security Agency, Ft. George G. Meade, MD 20755, jfdillon@gmail.com
[¶]Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC V5A 1S6, Canada, jed@sfu.ca; supported by NSERC
[‖]Department of Computer Science, University of Maryland MD, trabbani@cs.umd.edu
[**]Department of Mathematics and Statistics, Sam Houston State University, Huntsville TX, kenwsmith54@gmail.com
[††]Simon Fraser University, now at MetaOptima Technology Inc., william@metaoptima.com
2010 Mathematics Subject Classification 05B10, 05E18 (primary)

group $G$ with the element of the group ring $\mathbb{Z}G$ which is its $\{0,1\}$-valued characteristic function. The subset $D$ of $G$ is then a difference set if and only if the $\{0,1\}$-valued characteristic function $D$ satisfies the equation

$$DD^{(-1)} = n + \lambda G \quad \text{in } \mathbb{Z}G,$$

in which $n$ represents $n1_G$. Throughout, we shall instead identify the subset $D$ of $G$ with the element of $\mathbb{Z}G$ which is its $\{\pm 1\}$-valued characteristic function (taking the value $-1$ for each element of $G$ in $D$, and $+1$ for each element of $G$ not in $D$). Under this convention, the subset $D$ of $G$ is a difference set if and only if the $\{\pm 1\}$-valued function $D$ satisfies

$$DD^{(-1)} = 4n + (v - 4n)G \quad \text{in } \mathbb{Z}G.$$

When $v = 4n$, this reduces to

$$DD^{(-1)} = |G|, \tag{1}$$

in which case the subset $D$ is called a *Hadamard* difference set because the $\{\pm 1\}$-valued $v \times v$ incidence matrix, whose rows and columns are indexed by the elements of $G$ and whose $(g, h)$ entry is the coefficient of $g^{-1}h$ in $D$, is a Hadamard matrix.

**Example 1.1** (Bruck 1955 [6]). *Let $G = C_2^4 = \langle x_1, x_2, x_3, x_4 \rangle$, where $C_2$ denotes the multiplicative cyclic group of order 2. The set*

$$D = \{1, x_1, x_2, x_3, x_4, x_1x_2x_3x_4\}$$

*is a $(16, 6, 2)$ Hadamard difference set in $G$. We identify this set with the element $D = -1 - x_1 - x_2 - x_3 - x_4 - x_1x_2x_3x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$ of the group ring $\mathbb{Z}G$, and then $DD^{(-1)} = 16$.*

We call a group containing a Hadamard difference set a *Hadamard group*, and denote the class of Hadamard groups by $\mathcal{H}$. It is an outstanding problem in combinatorics to determine which groups belong to the class $\mathcal{H}$; see [11] for a survey and [22] for a summary of subsequent results. This paper focusses on determining which 2-groups (namely groups whose order is a power of 2) belong to $\mathcal{H}$. The relation $v = 4n$ between the parameters of a difference set forces the parameters to be

$$(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N) \tag{2}$$

for some integer $N$ [23]. Here $N$ can be positive or negative, and the two values $\pm N$ give the parameters of complementary difference sets and designs. A nontrivial difference set in a 2-group must also have parameters of the form (2), where $N = 2^d$ for some positive integer $d$ [28]. We therefore restrict attention to the parameters

$$(v, k, \lambda) = (2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d),$$

where $d$ is a nonnegative integer. The groups of order $2^{2d+2}$ form a rich source of potential Hadamard difference sets: there are 2 nonisomorphic groups of order 4 (both of which contain a trivial Hadamard difference set); 14 of order 16; 267 of order 64; 56,092 of order 256; and 49,487,367,289 groups of order 1024 [3, 7, 30].

The following product construction contains, as a special case, the earlier result [23, 35] that the class $\mathcal{H}$ is closed under direct products.

**Theorem 1.2** (Dillon product construction 1985 [14]). *Suppose that $H_1, H_2 \in \mathcal{H}$, and that $G$ is a group containing subgroups $H_1$ and $H_2$ satisfying $G = H_1H_2$ and $H_1 \cap H_2 = 1$. Then $G \in \mathcal{H}$.*

*Proof.* Let $D_1$ and $D_2$ be difference sets in $H_1$ and $H_2$, respectively, and let $D = D_1D_2$. By hypothesis, every element $g$ of $G$ has a unique representation $g = h_1h_2$ for some $h_1 \in H_1$ and $h_2 \in H_2$, and so $D$ is $\{\pm 1\}$-valued. Then

$$DD^{(-1)} = (D_1D_2)(D_1D_2)^{(-1)} = D_1D_2D_2^{(-1)}D_1^{(-1)} = D_1|H_2|D_1^{(-1)} = |H_1||H_2| = |G|.$$

$\square$

In a seminal paper, Turyn used algebraic number theory to prove a first nonexistence result for Hadamard 2-groups.

**Theorem 1.3** (Turyn 1965 [35])**.** *Let $G$ be a group of order $2^{2d+2}$ containing a normal subgroup $K$ of order less than $2^d$ such that $G/K$ is cyclic. Then $G \notin \mathcal{H}$.*

**Corollary 1.4** (Turyn exponent bound)**.** *Suppose $G \in \mathcal{H}$ is an abelian group of order $2^{2d+2}$. Then $G$ has exponent at most $2^{d+2}$.*

Dillon later proved a second nonexistence result for Hadamard 2-groups.

**Theorem 1.5** (Dillon 1985 [14])**.** *Let $G$ be a group of order $2^{2d+2}$ containing a normal subgroup $K$ of order less than $2^d$ such that $G/K$ is dihedral. Then $G \notin \mathcal{H}$.*

In the ensuing 35 years since the publication of [14], no further nonexistence results for Hadamard 2-groups have been found. In this paper we shall present constructive results that identify new Hadamard 2-groups. In preparation, we introduce some further conventions that will be used throughout.

Let

$$E_r := C_2^r = \langle x_1, x_2, \dots, x_r \rangle$$

be the elementary abelian group of order $2^r$. The group $E_r$ is isomorphic to the additive group of the vector space $U_r := \mathrm{GF}(2)^r$ comprising all binary $r$-tuples $a = (a_1, a_2, \dots, a_r)$, and an explicit isomorphism is given by

$$a = (a_1, a_2, \dots, a_r) \mapsto x^a = x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}.$$

The *characters* of $E_r$ are the homomorphisms from $E_r$ into the multiplicative group $\{1, -1\}$ given by

$$\chi_u : x^a \mapsto (-1)^{u \cdot a} \quad \text{for all } a \in U_r$$

as $u$ ranges over $U_r$.

We consider integer-valued functions on $G$ to be interchangeable with elements of $\mathbb{Z}G$: we identify an integer-valued function $F$ on $G$ with the element $\sum_{g \in G} F(g)g$ of the group ring $\mathbb{Z}G$, and conversely we identify a group ring element $\sum_{g \in G} F_g g$ with the function $F$ on $G$ given by $F(g) = F_g$. The character $\chi_u$ of $E_r$ may then be written in the group ring $\mathbb{Z}E_r$ as

$$\begin{aligned}
\chi_u &= \sum_{a \in U_r} \chi_u(x^a) x^a \\
&= \sum_{a \in U_r} (-1)^{u \cdot a} x^a \\
&= \sum_{a \in U_r} \prod_{i=1}^{r} (-1)^{u_i a_i} x_i^{a_i} \\
&= \prod_{i=1}^{r} \sum_{a_i = 0}^{1} (-1)^{u_i a_i} x_i^{a_i} \\
&= \prod_{i=1}^{r} \big(1 + (-1)^{u_i} x_i\big). \qquad (3)
\end{aligned}$$

This is consistent with the common notation $\chi_0$ for the principal character, which takes the value 1 at every group element; we identify this function in $\mathbb{Z}E_r$ with the group ring element $\sum_{e \in E_r} e$, or simply $E_r$. For each nonzero $u \in U_r$, the complement of the subset of $E_r$ associated with the $\{\pm 1\}$-valued function $\chi_u$ is a subgroup of $E_r$ of index 2, and as $u$ ranges over the nonzero values of $U_r$ we obtain all $2^r - 1$ subgroups of $E_r$ of index 2 in this way.

**Example 1.6.** *Let $E_2 = C_2^2 = \langle x, y \rangle$. The four characters of $E_2$ are the functions $\chi_u$ as $u$ ranges over $U_2 = \{(0,0), (0,1), (1,0), (1,1)\}$. Expressed in the group ring $\mathbb{Z}E_2$, these functions are*

$$\chi_{00} = 1 + x + y + xy = (1 + x)(1 + y),$$

$$\chi_{01} = 1 + x - y - xy = (1+x)(1-y),$$
$$\chi_{10} = 1 - x + y - xy = (1-x)(1+y),$$
$$\chi_{11} = 1 - x - y + xy = (1-x)(1-y),$$

*(where we abbreviate $\chi_{(0,1)}$, for example, as $\chi_{01}$).*

*The subgroups of $E_2$ corresponding to $\chi_{01}$, $\chi_{10}$, $\chi_{11}$ are $\{1,x\}$, $\{1,y\}$, $\{1,xy\}$, respectively.*

The group ring interpretation of the characters of $E_2$ shown in Example 1.6 illustrates the following fundamental properties, which underlie our new constructions of difference sets. These properties can all be derived directly from (3), noting that $\chi_v^{(-1)} = \chi_v$ for all $v \in U_r$.

**Proposition 1.7.** *Let $\{\chi_u : u \in U_r\}$ be the set of characters of $E_r$. Then for all $u, v \in U_r$, in the group ring $\mathbb{Z}E_r$ we have:*

*(i)* $\chi_u \chi_v^{(-1)} = \begin{cases} 2^r \chi_u & \text{if } u = v, \\ 0 & \text{if } u \neq v \end{cases}$

*(ii)* $\sum_{u \in U_r} \chi_u = 2^r$

*(iii)* $\sum_{e \in E_r} \chi_u(e) = \begin{cases} 2^r & \text{if } u = 0, \\ 0 & \text{if } u \neq 0. \end{cases}$

Since all characters of $E_r$ are $\{\pm 1\}$-valued, Proposition 1.7 (*iii*) implies that every nonprincipal character on $E_r$ takes the values 1 and $-1$ equally often.

McFarland gave the following difference set construction based on hyperplanes of a vector space, which produces examples in 2-groups. We prove the construction by interpreting the hyperplanes in terms of characters.

**Theorem 1.8** (McFarland hyperplane construction 1973 [29])**.** *Let $J$ be a group of order $2^{d+1}$. Then $J \times E_{d+1} \in \mathcal{H}$.*

*Proof.* (Dillon [17]). Let $\{\chi_u : u \in U_{d+1}\}$ be the set of characters of $E_{d+1}$. Label the elements of $J$ arbitrarily as $J = \{g_u : u \in U_{d+1}\}$, and let $G = J \times E_{d+1}$. We see from Proposition 1.7 (*i*) and (*ii*) that, in the group ring $\mathbb{Z}G$, the $\{\pm 1\}$-valued function

$$D = \sum_{u \in U_{d+1}} g_u \chi_u \tag{4}$$

on $G$ satisfies

$$\begin{aligned} DD^{(-1)} &= \sum_{u,v \in U_{d+1}} g_u \chi_u \chi_v^{(-1)} g_v^{-1} \\ &= 2^{d+1} \sum_{u \in U_{d+1}} g_u \chi_u g_u^{-1} \qquad (5) \\ &= 2^{d+1} \sum_{u \in U_{d+1}} \chi_u \qquad (6) \\ &= 2^{d+1} \cdot 2^{d+1} = |G|. \end{aligned}$$

Therefore $D$ corresponds to a Hadamard difference set in $G$. □

We shall show how the proof of Theorem 1.8 can be adapted so that the result still holds when $E_{d+1}$ is a normal subgroup of index $2^{d+1}$ of a group $G$, but not necessarily a direct factor. The key consideration is how to obtain (6) from (5). The following combinatorial result allows us to do so, by showing that there is a choice for coset representatives $g_u$ of $E_{d+1}$ in $G$ satisfying $\{g_u \chi_u g_u^{-1} : u \in U_{d+1}\} = \{\chi_u : u \in U_{d+1}\}$. Note that a group $H$ *acts as a group of permutations* on a set $S$ if there is a homomorphism $\phi$ (called the *action* of $H$ on $S$) from $H$ to the group of permutations of $S$.

**Theorem 1.9** (Drisko 1998 [18, Corollary 5]). *Let $p$ be a prime and let $H$ be a finite $p$-group. Suppose that $H$ acts as a group of permutations on a set $S$ of size $|H|$ according to the action $\phi$, and that $S$ contains an element that is fixed under $\phi$. Then there is a bijection $\theta$ from $S$ to $H$ satisfying*

$$\{\phi(\theta(s))(s) : s \in S\} = S.$$

The bijection $\theta$ in Theorem 1.9 selects an element $\theta(s)$ of the group $H$ for each $s \in S$, so that the resulting set of actions of $\theta(s)$ on $s$ is a permutation of the set $S$. We now explain how this result can be used to extend Theorem 1.8 as desired, proving a conjecture due to Dillon [15].

**Corollary 1.10** (Drisko 1998 [18, Corollary 9]). *Let $G$ be a group of order $2^{2d+2}$ containing a normal subgroup $E \cong C_2^{d+1}$. Then $G \in \mathcal{H}$.*

*Proof.* Let $\widehat{E} = \{\chi_u : u \in U_{d+1}\}$ be the set of characters of $E \cong C_2^{d+1}$. We wish to apply Theorem 1.9 with $S = \widehat{E}$ and $H = G/E$. Since $E$ is normal in $G$, and the complements of the subsets of $E$ associated with the characters $\chi_u$ for nonzero $u$ are exactly the subgroups of $E$ of index 2, we have

$$g\chi_u g^{-1} \in \widehat{E} \quad \text{for all } g \in G \text{ and } \chi_u \in \widehat{E}.$$

Therefore $G/E$ acts on $\widehat{E}$ as a group of permutations under the conjugation action

$$\phi(gE)(\chi_u) = g\chi_u g^{-1} \quad \text{for all } gE \in G/E \text{ and } \chi_u \in \widehat{E},$$

and the element $\chi_0 = E$ of $\widehat{E}$ is fixed under $\phi$. Theorem 1.9 then shows that there is a bijection $\theta$ from $\widehat{E}$ to $G/E$ satisfying

$$\{\phi(\theta(\chi_u))(\chi_u) : \chi_u \in \widehat{E}\} = \widehat{E}. \tag{7}$$

Writing $\theta(\chi_u) = g_u E$ for each $u \in U_{d+1}$, this gives a set $\{g_u : u \in U_{d+1}\}$ of coset representatives for $E$ in $G$ satisfying

$$\{g_u \chi_u g_u^{-1} : u \in U_{d+1}\} = \{\chi_u : u \in U_{d+1}\}. \tag{8}$$

Use the coset representatives $g_u$ to define $D$ as in (4). The proof of Theorem 1.8 now carries through unchanged, using (8) to obtain (6) from (5). □

We next illustrate the construction described in Corollary 1.10, for a specific group of order 16.

**Example 1.11.** *Let $G$ be the order 16 modular group $C_8 \rtimes_5 C_2 = \langle x, y : x^8 = y^2 = 1,\ yxy^{-1} = x^5\rangle$, and set $X = x^4$ and $Y = y$. Let $E = \langle X, Y\rangle \cong C_2^2$, which is normal but not central in $G$, and let $\widehat{E} = \{\chi_u : u \in U_2\}$ be the set of characters of $E$:*

$$\chi_{00} = (1+x^4)(1+y),\ \chi_{01} = (1+x^4)(1-y),\ \chi_{10} = (1-x^4)(1+y),\ \chi_{11} = (1-x^4)(1-y).$$

*The center of $G$ is $\langle x^2\rangle$.*

*The group $G/E = \{E, xE, x^2E, x^3E\}$ acts on $\widehat{E}$ as a group of permutations under the conjugation action $\phi$, under which $E$ and $x^2E$ map to the identity permutation on $\widehat{E}$, and $xE$ and $x^3E$ map to the permutation of $\widehat{E}$ that fixes $\chi_{00}$ and $\chi_{01}$ but swaps $\chi_{10}$ and $\chi_{11}$.*

*A bijection $\theta$ from $\widehat{E}$ to $G/E$ satisfying (7) is*

$$\theta(\chi_{00}) = E, \quad \theta(\chi_{01}) = x^2E, \quad \theta(\chi_{10}) = xE, \quad \theta(\chi_{11}) = x^3E,$$

*and therefore*

$$D = \chi_{00} + x^2\chi_{01} + x\chi_{10} + x^3\chi_{11}$$

*is a difference set in $G$.*

The Turyn exponent bound of Corollary 1.4 gives a necessary condition for an abelian 2-group to belong to $\mathcal{H}$. A series of papers, including [10] and [16], gave constructions in pursuit of a sufficient condition. Kraemer [25] eventually showed that the necessary condition is also sufficient. This result was proved again by Jedwab [21] using the alternative viewpoint of a perfect binary array: a matrix representation of the $\{\pm1\}$-valued characteristic function of a Hadamard difference set in an abelian group.

**Theorem 1.12** (Kraemer [25]). *Let $G$ be an abelian group of order $2^{2d+2}$. Then $G \in \mathcal{H}$ if and only if $G$ has exponent at most $2^{d+2}$.*

We next give an instructive example of a Hadamard difference set in an abelian 2-group, which illustrates a fundamental insight on which this paper is based. The group ring elements $A_u$ in Example 1.13 are presented for now without explanation of their origin, but will be revisited in Example 4.13. Group ring elements $A, B$ are *orthogonal* if $AB^{(-1)} = 0$.

**Example 1.13.** *Let $G = C_8^2 = \langle x, y\rangle$, and set $X = x^2$ and $Y = y^2$. Let $K = \langle X, Y\rangle \cong C_4^2$ and $E_2 = \langle X^2, Y^2\rangle \cong C_2^2$, and let $\{\chi_u : u \in U_2\}$ be the set of characters of $E_2$. Define four group ring elements in $\mathbb{Z}K$ by*

$$A_{00} = A_{01} = A_{10} = 1 + X + Y - XY \quad \textit{and} \quad A_{11} = 1 + X + Y + XY. \tag{9}$$

*Direct calculation shows that the $A_u$ satisfy the condition*

$$A_u \chi_u A_u^{(-1)} = 4\chi_u \quad \textit{for all } u \in U_2. \tag{10}$$

*Now in $\mathbb{Z}K$ let*

$$\begin{aligned} B_{00} &= A_{00}\chi_{00} = (1 + X + Y - XY)(1 + X^2)(1 + Y^2), \\ B_{01} &= A_{01}\chi_{01} = (1 + X + Y - XY)(1 + X^2)(1 - Y^2), \\ B_{10} &= A_{10}\chi_{10} = (1 + X + Y - XY)(1 - X^2)(1 + Y^2), \\ B_{11} &= A_{11}\chi_{11} = (1 + X + Y + XY)(1 - X^2)(1 - Y^2). \end{aligned}$$

*Then from Proposition 1.7 (i) and (10), the $B_u = A_u\chi_u$ have the property, for all $u, v \in U_2$, that*

$$B_u B_v^{(-1)} = \begin{cases} 16\chi_u & \textit{if } u = v, \\ 0 & \textit{if } u \neq v, \end{cases} \tag{11}$$

*and in particular the $B_u$ are pairwise orthogonal. It follows that the $\{\pm 1\}$-valued function on $G$ given by*

$$D = B_{00} + yB_{01} + xB_{10} + xyB_{11}$$

*satisfies*

$$\begin{aligned} DD^{(-1)} &= 16(\chi_{00} + \chi_{01} + \chi_{10} + \chi_{11}) \\ &= 64 \end{aligned}$$

*by Proposition 1.7 (ii), and so $D$ corresponds to a Hadamard difference set in $G$.*

We now show how the condition (10) satisfied by the group ring elements $A_u$ in Example 1.13 can be used to construct difference sets in groups of order 64 other than $C_8^2$.

**Proposition 1.14.** *Let $G$ be a group of order 64 containing a normal subgroup $K \cong C_4^2$. Then $G \in \mathcal{H}$.*

*Proof.* Let $K = \langle X, Y\rangle \cong C_4^2$. Let $E_2 = \langle X^2, Y^2\rangle$ be the unique subgroup of $K$ isomorphic to $C_2^2$, and let $\widehat{E_2} = \{\chi_u : u \in U_2\}$ be the set of characters of $E_2$. Define four group ring elements in $\mathbb{Z}K$ as in (9), and for each $u \in U_2$ let $B_u$ be the $\{\pm 1\}$-valued function $A_u\chi_u$ on $K$. The $A_u$ satisfy (10), and therefore the $B_u$ have the pairwise orthogonality property (11) for all $u, v \in U_2$.

Now $E_2$ is the unique subgroup of $K$ isomorphic to $C_2^2$, and $K$ is normal in $G$, so $E_2$ is normal in $G$. Therefore $G/K$ acts on $\widehat{E_2}$ as a group of permutations under the conjugation action

$$\phi(gK)(\chi_u) = g\chi_u g^{-1} \quad \text{for all } gK \in G/K \text{ and } \chi_u \in \widehat{E_2},$$

and $\chi_0 = E_2$ is fixed under $\phi$. We may therefore apply Theorem 1.9 with $S = \widehat{E_2}$ and $H = G/K$ to show that there is a set $\{g_u : u \in U_2\}$ of coset representatives for $K$ in $G$ satisfying

$$\{g_u \chi_u g_u^{-1} : u \in U_2\} = \{\chi_u : u \in U_2\}. \tag{12}$$

Let $D$ be the $\{\pm 1\}$-valued function on $G$ defined by

$$D = \sum_{u \in U_2} g_u B_u \text{ in } \mathbb{Z}G.$$

We calculate

$$\begin{aligned} DD^{(-1)} &= \sum_{u,v \in U_2} g_u B_u B_v^{(-1)} g_v^{-1} \\ &= 16 \sum_{u \in U_2} g_u \chi_u g_u^{-1} \end{aligned}$$

by (11), and then from (12) and Proposition 1.7 (*ii*) we have

$$DD^{(-1)} = 16 \sum_{u \in U_2} \chi_u = 64.$$

Therefore $D$ corresponds to a Hadamard difference set in $G$. □

We use the proof of Proposition 1.14 as a model for establishing our principal result, stated below as Theorem 1.15. The key idea is to determine group ring elements $A_u$ satisfying a condition analogous to (10), which ensures that the associated group ring elements $B_u = A_u \chi_u$ have an orthogonality property analogous to (11). Application of Theorem 1.9 then allows us to construct a group ring element $D$ corresponding to a Hadamard difference set. By taking $r = 2$ in Theorem 1.15 and restricting the group $G$ to be abelian, and combining with the Turyn exponent bound of Corollary 1.4, we recover Kraemer's Theorem 1.12.

**Theorem 1.15** (Main Result)**.** *Let $d$ and $r$ be integers satisfying $d \geq 1$ and $2 \leq r \leq d+1$. Let $G$ be a group of order $2^{2d+2}$ containing a normal abelian subgroup of index $2^r$, rank $r$, and exponent at most $2^{d-r+2}$. Then $G \in \mathcal{H}$.*

We remark that this paper develops several concepts previously used to construct difference sets. In particular, the constructed group ring elements $B_u$ can be interpreted as covering extended building sets, as introduced by Davis and Jedwab [12] in 1997 (see the discussion at the end of Section 2). The novelty here is that imposing the additional structure $B_u = A_u \chi_u$ allows us to handle dramatically more nonabelian groups than before, as illustrated in the proof of Proposition 1.14. Likewise, Proposition 1.14 itself was previously established by Dillon [15, 17] by decomposing a difference set in $C_8^2$ into four orthogonal group ring elements $B_u$ as in Example 1.13. However, the generalization of Proposition 1.14 to Theorem 1.15 relies crucially on recognizing the additional structure $B_u = A_u \chi_u$ of these group ring elements, whose importance was not previously apparent.

Each of the two groups of order 4 belongs to $\mathcal{H}$ trivially. The third column of Table 1 below shows the number of groups of order 16, 64, and 256 which are possible members of $\mathcal{H}$, after taking into account those that are excluded by the necessary conditions of Theorems 1.3 and 1.5. We now summarize the theoretical and computational efforts of many researchers over several decades to determine whether these conditions are also sufficient for groups of these orders, with reference to results to be presented in Section 4.

In the 1970s, Whitehead [37] and Kibler [24] independently showed by construction that each of the 12 non-excluded groups of order 16 belongs to $\mathcal{H}$. We can recover this result by applying Theorem 1.15 to account for the 10 groups containing a normal subgroup isomorphic to $C_2^2$, and then using Proposition 4.1 to handle the remaining 2 groups.

In 1990, a collaborative effort led by Dillon showed by a combination of construction and computer search that each of the 259 non-excluded groups of order 64 belongs to $\mathcal{H}$; Liebler and Smith [27] resolved the status of the final group at the conclusion of a sabbatical visit to Dillon by Smith. Using the GAP software package [19], we can streamline this effort by applying in sequence the following construction methods: Theorem 1.15 to account for the 237 groups containing a normal subgroup isomorphic to $C_2^3$ or $C_4^2$; the product construction of Proposition 4.7 to account for 17 further groups; the transfer methods of Section 4.3 to account for 4 further groups; and the modified signature set method of Section 4.4 to account for the final group.

In 2011, Dillon initiated a further collaborative effort to investigate the groups of order 256, whose conclusion was that each of the 56,049 non-excluded groups of order 256 belongs to $\mathcal{H}$. Major contributions were made by Applebaum [1], and the status of the final group was resolved by Yolland [38] in 2016. Using GAP, we can likewise streamline this effort by applying in sequence the following construction methods: Theorem 1.15 to account for the 54,633 groups containing a normal subgroup isomorphic to $C_2^4$ or $C_4^2 \times C_2$ or $C_8^2$; the product construction of Proposition 4.7 to account for 1,358 further groups; the transfer methods of Section 4.3 to account for 57 further groups; and the modified signature set method of Section 4.4 to account for the final group.

These theoretical and computational results are summarized in Theorem 1.16 and in Table 1.

**Theorem 1.16.** *The necessary conditions of Theorems* 1.3 *and* 1.5 *for the existence of a difference set are also sufficient in groups of order* 4, 16, 64, *and* 256.

| Group order | Total # groups | # not excluded by Theorems 1.3, 1.5 | # in $\mathcal{H}$ by | | | |
|---|---|---|---|---|---|---|
| | | | Theorem 1.15 | Sections 4.1–4.2 | Section 4.3 | Section 4.4 |
| 16 | 14 | 12 | 10 | 2 | | |
| 64 | 267 | 259 | 237 | 17 | 4 | 1 |
| 256 | 56,092 | 56,049 | 54,633 | 1,358 | 57 | 1 |

Table 1: Membership in $\mathcal{H}$ of 2-groups of order 16, 64, and 256. Figures in column 5 onwards are for groups not previously counted in column 4 onwards.

Theorem 1.16 naturally prompts the following question (about whose answer the authors of this paper have different opinions).

**Question 1.17.** *Are the necessary conditions of Theorems* 1.3 *and* 1.5 *for the existence of a difference set in a* 2*-group also sufficient? That is, does every group $G$ of order $2^{2d+2}$, not containing a normal subgroup $K$ of order less than $2^d$ such that $G/K$ is cyclic or dihedral, belong to $\mathcal{H}$?*

The answer to Question 1.17 is "yes" for $d \leq 3$, by Theorem 1.16. It seems that resolution of this question for $d > 3$ must depend only on theoretical methods: currently there is not even a database of the 49,487,367,289 groups of order 1024 [3, 7], and the authors do not know how to estimate the proportion of the non-excluded groups of order $2^{2d+2}$ that are accounted for by Theorem 1.15 as $d$ grows large.

The rest of this paper is organized in the following way. In Section 2, we identify the "signature set" property underlying the construction of Proposition 1.14. In Section 3, we prove our principal result of Theorem 1.15 by restricting attention to signature sets on abelian 2-groups. In Section 4, we describe the various other construction methods used to complete the determination of the groups of order 64 and 256 belonging to $\mathcal{H}$, involving signature sets on nonabelian groups, products of perfect ternary arrays, transfer methods, and a modification of signature sets. In Section 5, we provide implementation details of the construction methods for groups of order 256 and describe how to quickly verify on a desktop computer that all 56,049 non-excluded groups of this order belong to $\mathcal{H}$. In Section 6, we propose some directions for future research.

# 2 Signature Sets

In this section, we identify the structure underlying Proposition 1.14 and set out a framework for proving our principal result, Theorem 1.15.

**Definition 2.1.** *Let $K$ be a group containing a normal subgroup $E \cong C_2^r$, and let $\{\chi_u : u \in U_r\}$ be the set of characters of $E$. A* signature block on $K$ with respect to $\chi_u$ *is a $\{\pm 1\}$-valued function $A_u$ on a set of coset representatives for $E$ in $K$ that satisfies*

$$A_u \chi_u A_u^{(-1)} = \tfrac{|K|}{2^r} \chi_u \quad \text{in } \mathbb{Z}K.$$

*A* signature set on $K$ with respect to $E$ *is a multiset* $\{A_u : u \in U_r\}$*, where each* $A_u$ *is a signature block on* $K$ *with respect to* $\chi_u$*.*

Note that a trivial signature set on $C_2^r$ with respect to itself is given by

$$A_u = 1 \quad \text{for each } u \in U_r.$$

We state two immediate consequences of Definition 2.1.

**Lemma 2.2.** *Let* $K$ *be a group containing a normal subgroup* $E \cong C_2^r$*, and suppose* $\{A_u : u \in U_r\}$ *is a signature set on* $K$ *with respect to* $E$*. Let* $\widehat{E} = \{\chi_u : u \in U_r\}$ *be the set of characters of* $E$*, and let* $B_u = A_u\chi_u$ *for each* $u \in U_r$*. Then:*

$(i)$ *for each* $u \in U_r$*, the function* $B_u$ *is* $\{\pm 1\}$*-valued on* $K$*.*

$(ii)$ *for all* $u, v \in U_r$*, in* $\mathbb{Z}K$ *we have*

$$B_u B_v^{(-1)} = \begin{cases} |K|\chi_u & \textit{if } u = v, \\ 0 & \textit{if } u \neq v \end{cases}$$

*(and so in particular the* $B_u$ *are pairwise orthogonal).*

*Proof.* $(i)$ Each $A_u$ is a $\{\pm 1\}$-valued function on a set of coset representatives for $E$ in $K$, and each $\chi_u$ is a $\{\pm 1\}$-valued function on $E$. Therefore each $B_u = A_u\chi_u$ is a $\{\pm 1\}$-valued function on $K$.

$(ii)$ For all $u, v \in U_r$, in $\mathbb{Z}K$ we have

$$\begin{aligned} B_u B_v^{(-1)} &= A_u \chi_u \chi_v^{(-1)} A_v^{(-1)} \\ &= \begin{cases} 2^r A_u \chi_u A_u^{(-1)} & \text{if } u = v, \\ 0 & \text{if } u \neq v \end{cases} \end{aligned}$$

by Proposition 1.7 $(i)$. Since the $A_u$ form a signature set on $K$ with respect to $E$, this gives

$$B_u B_v^{(-1)} = \begin{cases} |K|\chi_u & \text{if } u = v, \\ 0 & \text{if } u \neq v. \end{cases}$$

□

The proof of the following theorem is modelled on that of Proposition 1.14. We remark that $K$ need not be a 2-group and need not be abelian.

**Theorem 2.3.** *Let* $G$ *be a group containing a normal subgroup* $E \cong C_2^r$*, and suppose* $K$ *is a normal subgroup of* $G$ *of index* $2^r$ *containing* $E$*. Suppose there exists a signature set on* $K$ *with respect to* $E$*. Then* $G \in \mathcal{H}$*.*

*Proof.* Let $\widehat{E} = \{\chi_u : u \in U_r\}$ be the set of characters of $E$. We shall apply Theorem 1.9 with $S = \widehat{E}$ and $H = G/K$. Since $E$ is normal in $G$, and the complements of the subsets of $E$ associated with the characters $\chi_u$ for nonzero $u$ are exactly the subgroups of $E$ of index 2,

$$g\chi_u g^{-1} \in \widehat{E} \quad \text{for all } g \in G \text{ and } \chi_u \in \widehat{E}.$$

Therefore $G/K$ acts on $\widehat{E}$ as a group of permutations under the conjugation action

$$\phi(gK)(\chi_u) = g\chi_u g^{-1} \quad \text{for all } gK \in G/K \text{ and } \chi_u \in \widehat{E},$$

and the element $\chi_0 = E$ of $\widehat{E}$ is fixed under $\phi$. Apply Theorem 1.9 to show that there is a set $\{g_u : u \in U_r\}$ of coset representatives for $K$ in $G$ satisfying

$$\{g_u \chi_u g_u^{-1} : u \in U_r\} = \{\chi_u : u \in U_r\}. \tag{13}$$

By assumption, there is a signature set $\{A_u : u \in U_r\}$ on $K$ with respect to $E$. Let $B_u = A_u\chi_u$ for each $u \in U_r$, and use the coset representatives $g_u$ to define

$$D = \sum_{u \in U_r} g_u B_u \quad \text{in } \mathbb{Z}G, \tag{14}$$

which is a $\{\pm 1\}$-valued function on $G$ by Lemma 2.2 $(i)$. We calculate in $\mathbb{Z}G$ that

$$\begin{aligned} DD^{(-1)} &= \sum_{u,v \in U_r} g_u B_u B_v^{(-1)} g_v^{-1} \\ &= |K| \sum_{u \in U_r} g_u \chi_u g_u^{-1} \end{aligned}$$

by Lemma 2.2 $(ii)$. Then from (13) and Proposition 1.7 $(ii)$ we have

$$DD^{(-1)} = |K| \sum_{u \in U_r} \chi_u = 2^r|K| = |G|.$$

Therefore $D$ corresponds to a Hadamard difference set in $G$. $\square$

The motivating examples of Section 1 both occur as special cases of Theorem 2.3. Corollary 1.10 arises by taking $|G| = 2^{2d+2}$ and $r = d+1$, with $E = K \cong C_2^{d+1}$ normal in $G$, and using a trivial signature set on $K$ with respect to itself. Proposition 1.14 arises by taking $|G| = 64$ and $r = 2$, with $K = \langle X, Y \rangle \cong C_4^2$ normal in $G$ and $E = \langle X^2, Y^2 \rangle$ (the unique subgroup of $K$ isomorphic to $C_2^2$), and using the nontrivial signature set $\{A_{ij} : (i,j) \in U_2\}$ on $K$ with respect to $E$ specified in (9).

Theorem 2.3 establishes the existence of a difference set in $G$ by reference to Theorem 1.9, whose proof as given in [18] is not constructive. To construct such a difference set explicitly, one must therefore determine suitable coset representatives for the normal subgroup $K$ in $G$ satisfying (13). This determination currently requires a computer search that can be computationally expensive, particularly for groups of order 256 (see Section 5).

We point out a connection to the study of bent functions (see [8] for a survey), which are equivalent to Hadamard difference sets in elementary abelian 2-groups. Take $G = E_{d+1}^2$ and $E = K = E_{d+1}$ in Theorem 2.3, and let $\{A_u : u \in U_r\}$ be a trivial signature set on $K$ with respect to $E$ for which each $A_u$ is chosen arbitrarily in $\{\pm 1\}$. In this case, the choice of coset representatives $\{g_u : u \in U_{d+1}\}$ for $K$ in $G$ used to construct the difference set $D$ in the proof of Theorem 2.3 is arbitrary. Let $a$ be the Boolean function on $U_{d+1}$ defined by

$$A_u = (-1)^{a(u)} \quad \text{for each } u \in U_{d+1}.$$

Then the $\{0,1\}$-valued characteristic function of $D$ is the Maiorana-McFarland bent function $f(u,v) = \pi(u) \cdot v + a(u)$, where $\pi$ is an arbitrary permutation of $U_{d+1}$.

In view of Theorem 2.3, our objective in Section 3 is to construct a signature set on a large class of groups $K$ (which we take to be abelian in Section 3, and nonabelian in Section 4). In the remainder of this section, we introduce some preparatory results about signature sets.

We firstly show that a group automorphism of $K$ fixing $E$ maps a signature block on $K$ to another signature block on $K$.

**Proposition 2.4.** *Let $K$ be a group containing a normal subgroup $E \cong C_2^r$, and let $\sigma$ be a group automorphism of $K$ which fixes $E$. Suppose that $A_u$ is a signature block on $K$ with respect to the character $\chi_u$ of $E$, for some $u \in U_r$. Then $\sigma$ induces a map on $\mathbb{Z}K$ under which $\sigma(A_u)$ is a signature block on $K$ with respect to the character $\sigma(\chi_u)$ of $E$.*

*Proof.* The signature block $A_u$ is $\{\pm 1\}$-valued on a set of coset representatives for $E$ in $K$. Since the automorphism $\sigma$ fixes $E$, the images of these coset representatives under $\sigma$ are also a set of coset representatives for $E$ in $K$ on which $\sigma(A_u)$ is $\{\pm 1\}$-valued. Furthermore

$$\begin{aligned} \sigma(A_u)\sigma(\chi_u)\sigma(A_u)^{(-1)} &= \sigma(A_u \chi_u A_u^{(-1)}) \\ &= \tfrac{|K|}{2^r}\sigma(\chi_u), \end{aligned}$$

so $\sigma(A_u)$ is a signature block on $K$ with respect to the character $\sigma(\chi_u)$ of $E$. $\square$

We next give a simple product construction for signature sets.

**Proposition 2.5.** *Suppose there exists a signature set on a group $K_r$ with respect to a normal subgroup $E_r \cong C_2^r$, and there exists a signature set on a group $K_s$ with respect to a normal subgroup $E_s \cong C_2^s$. Then there exists a signature set on $K_r \times K_s$ with respect to $E_r \times E_s$.*

*Proof.* Let $\{A_u : u \in U_r\}$ be a signature set on $K_r$ with respect to $E_r$, and let $\{\alpha_v : v \in U_s\}$ be a signature set on $K_s$ with respect to $E_s$. We claim that $\{A_u\alpha_v : u \in U_r, v \in U_s\}$ is a signature set on $K_r \times K_s$ with respect to its normal subgroup $E_r \times E_s$.

The function $A_u\alpha_v$ is $\{\pm1\}$-valued on a set of coset representatives for $E_r \times E_s$ in $K_r \times K_s$, because $A_u$ is $\{\pm1\}$-valued on a set of coset representatives for $E_r$ in $K_r$ and $\alpha_v$ is $\{\pm1\}$-valued on a set of coset representatives for $E_s$ in $K_s$.

Let $\{\chi_u : u \in U_r\}$ be the set of characters of $E_r$, and let $\{\psi_v : v \in U_s\}$ be the set of characters of $E_s$. The set of characters of $E_r \times E_s$ is $\{\chi_u\psi_v : u \in U_r, v \in U_s\}$, and for each $u \in U_r$ and $v \in U_s$ we have

$$\begin{aligned}
(A_u\alpha_v)(\chi_u\psi_v)(A_u\alpha_v)^{(-1)} &= A_u\chi_u\big(\alpha_v\psi_v\alpha_v^{(-1)}\big)A_u^{(-1)} \\
&= A_u\chi_u\tfrac{|K_s|}{2^s}\psi_v A_u^{(-1)} \\
&= \big(A_u\chi_u A_u^{(-1)}\big)\tfrac{|K_s|}{2^s}\psi_v \\
&= \tfrac{|K_r|}{2^r}\chi_u\,\tfrac{|K_s|}{2^s}\psi_v \\
&= \tfrac{|K_r\times K_s|}{2^{r+s}}(\chi_u\psi_v).
\end{aligned}$$

□

To illustrate the previously unrecognized power of the signature set approach, note that in 2013 Applebaum [1] used computer search to show that 643 of the 714 groups of order 256, whose membership in $\mathcal{H}$ was then undetermined, belong to $\mathcal{H}$. Since all 643 of these groups contain a normal subgroup isomorphic to $C_4^2 \times C_2$, this result follows directly from Theorem 2.3 simply by exhibiting a signature set on $C_4^2 \times C_2$ with respect to its unique subgroup isomorphic to $C_2^3$. This can be constructed by using Proposition 2.5 to take the product of a signature set on $C_4^2$ with respect to its unique subgroup isomorphic to $C_2^2$ (see Example 1.13) with a trivial signature set on $C_2$ with respect to itself.

Finally, we derive constraints on a signature set in terms of $|K|$ and $|E|$. We will use these constraints to show how Theorem 2.3 can be viewed as refining a construction method for difference sets introduced by Davis and Jedwab [12], by interpreting a signature set on an abelian group as a special kind of covering extended building set.

**Lemma 2.6.** *Let $K$ be a group containing a normal subgroup $E \cong C_2^r$, and suppose that $\{A_u : u \in U_r\}$ is a signature set on $K$ with respect to $E$. Let $\{\chi_u : u \in U_r\}$ be the set of characters of $E$, and let $B_u = A_u\chi_u$ for each $u \in U_r$. Then the number of times the $\{\pm1\}$-valued function $B_u$ on $K$ takes the value $-1$ is*

$$\begin{cases} \frac{1}{2}|K| & \text{if } u \neq 0, \\ \frac{1}{2}|K| \pm \sqrt{2^{r-2}|K|} & \text{if } u = 0. \end{cases}$$

*Proof.* By Lemma 2.2 $(i)$, each $B_u$ is $\{\pm1\}$-valued on $K$.

**Case 1:** $u \neq 0$**.** By Proposition 1.7 $(iii)$, the number of times the $\{\pm1\}$-valued function $\chi_u$ on $E$ takes the value $-1$ is $\frac{1}{2}|E|$. Since $A_u$ is a $\{\pm1\}$-valued function on a set of coset representatives for $E$ in $K$, the number of times $B_u = A_u\chi_u$ takes the value $-1$ is $\frac{1}{2}|E||K:E| = \frac{1}{2}|K|$.

**Case 2:** $u = 0$**.** Let $c \in \{0, 1, \ldots, |K|\}$ be the number of times that $B_0$ takes the value $-1$, and let $J$ be a group of order $2^r$. By Theorem 2.3, the group $G = J \times K$ contains a Hadamard difference set $D$ whose corresponding $\{\pm1\}$-valued function is defined in (14) as

$$D = g_0B_0 + \sum_{u\neq0} g_uB_u \tag{15}$$

for some choice of coset representatives $\{g_u : u \in U_r\}$ for $K$ in $G$. By (2), the parameters of the difference set $D$ satisfy

$$|G| = 2^r|K| = 4N^2 \quad \text{and} \quad |D| = 2N^2 - N$$

for some integer $N$, and eliminating $N$ gives

$$|D| = 2^{r-1}|K| \pm \sqrt{2^{r-2}|K|}.$$

But $|D|$ equals the number of times that the function $D$ takes the value $-1$, which from (15) and the result for Case 1 gives

$$|D| = c + (2^r - 1)\tfrac{1}{2}|K|.$$

Equate the two expressions for $|D|$ to give

$$c = \tfrac{1}{2}|K| \pm \sqrt{2^{r-2}|K|}.$$

□

Note from Example 1.13 that the number of times the function $A_u$ takes the value $-1$ is not determined for $u \neq 0$ solely from the hypotheses of Lemma 2.6. However, for $u = 0$ this number is determined as $\frac{1}{2^r}\left(\frac{|K|}{2} \pm \sqrt{2^{r-2}|K|}\right)$ by Lemma 2.6 and the relation $B_0 = A_0\chi_0$, because the $\{\pm 1\}$-valued function $\chi_0 = E$ takes the value 1 exactly $2^r$ times.

We can now interpret Theorem 2.3 in the framework of [12] for the case that $K$ is abelian. Suppose $\{A_u : u \in U_r\}$ is a signature set on an abelian group $K$ with respect to $E = \langle x_1, x_2, \ldots, x_r\rangle \cong C_2^r$, and let $B_u = A_u\chi_u$ for each $u \in U_r$. In the language of [12], we claim that the subsets $\left\{\frac{1}{2}(K - B_u) : u \in U_r\right\}$ of $K$ then form a $(\frac{|K|}{2}, \sqrt{2^{r-2}|K|}, 2^r, \pm)$ covering extended building set on $K$ (satisfying the key additional constraint that $B_u = A_u\chi_u$ for each $u$). To prove the claim, we require firstly that

$$\left|\tfrac{1}{2}(K - B_u)\right| = \begin{cases} \frac{1}{2}|K| \pm \sqrt{2^{r-2}|K|} & \text{for a single value of } u, \\ \frac{1}{2}|K| & \text{for all other values of } u. \end{cases}$$

This is given by Lemma 2.6, because $\left|\frac{1}{2}(K - B_u)\right|$ is the number of times that the $\{\pm 1\}$-valued function $B_u$ takes the value $-1$. To complete the proof of the claim, we also require that, for each nonprincipal character $\psi$ of the abelian group $K$ (namely a nontrivial homomorphism from $K$ to the complex roots of unity),

$$\left|\psi\big(\tfrac{1}{2}(K - B_u)\big)\right| = \begin{cases} \sqrt{2^{r-2}|K|} & \text{for a single value of } u \text{ that depends on } \psi, \\ 0 & \text{for all other values of } u. \end{cases}$$

This is given by applying $\psi$ to the case $u = v$ of Lemma 2.2 $(ii)$ to obtain $|\psi(B_u)|^2 = |K|\psi(\chi_u)$, and noting that $\psi$ maps each $x_i$ to $\{1, -1\}$ so that from (3) we have

$$\psi(\chi_u) = \begin{cases} 2^r & \text{for a single value of } u \text{ that depends on } \psi, \\ 0 & \text{for all other values of } u. \end{cases}$$

# 3 Proof of Main Result

In this section we prove our main result, Theorem 1.15, as a corollary of Theorem 3.1 below. For an abelian 2-group $K$ of rank $r$, we shall abbreviate "a signature set on $K$ with respect to its unique subgroup isomorphic to $C_2^r$" as "a signature set on $K$".

**Theorem 3.1.** *Let $d$ and $r$ be integers satisfying $d \geq 1$ and $2 \leq r \leq d+1$. Let $\mathcal{K}_{d,r}$ be the set of all abelian groups of order $2^{2d-r+2}$, rank $r$, and exponent at most $2^{d-r+2}$. Then there exists a signature set on each $K_{d,r} \in \mathcal{K}_{d,r}$.*

Note in Theorem 3.1 that if $E$ is the unique subgroup of $K_{d,r} \in \mathcal{K}_{d,r}$ isomorphic to $C_2^r$, then $E$ is normal in $G$. We may therefore apply Theorem 2.3 to obtain Theorem 1.15 as a corollary of Theorem 3.1.

We shall prove Theorem 3.1 using a recursive construction for signature sets on abelian 2-groups. To illustrate the main ideas, we begin with a proof of the special case $r = 2$.

**Theorem 3.2** (Rank 2 case of Theorem 3.1)**.** *Let $d$ be a non-negative integer. Then there exists a signature set on $K_d = C_{2^d}^2$.*

*Proof.* The proof is by induction on $d \geq 1$. The case $d = 1$ is true, because there exists a trivial signature set on $C_2^2$.

Assume all cases up to $d-1 \geq 1$ are true. Let $K_{d-1} = \langle X, Y \rangle$, where $X^{2^{d-1}} = Y^{2^{d-1}} = 1$. By the inductive hypothesis, there exists a signature set $\{A_{ij} : (i,j) \in U_2\}$ on $K_{d-1}$ with respect to $\langle X^{2^{d-2}}, Y^{2^{d-2}} \rangle$. By associating the group ring $\mathbb{Z}K_{d-1}$ with the quotient ring $\mathbb{Z}[X,Y]/\langle 1-X^{2^{d-1}}, 1-Y^{2^{d-1}} \rangle$, we may regard each group ring element $A_{ij}$ as a polynomial $A_{ij}(X,Y)$ in $X$ and $Y$, and regard each character of $\langle X^{2^{d-2}}, Y^{2^{d-2}} \rangle$ as a polynomial

$$\chi_{ij}(X,Y) = \big(1 + (-1)^i X^{2^{d-2}}\big)\big(1 + (-1)^j Y^{2^{d-2}}\big) \quad \text{for } (i,j) \in U_2.$$

By assumption, in the polynomial ring $\mathbb{Z}[X,Y]/\langle 1 - X^{2^{d-1}}, 1 - Y^{2^{d-1}} \rangle$ we have

$$A_{ij}(X,Y)\chi_{ij}(X,Y)A_{ij}(X,Y)^{(-1)} = 2^{2d-4}\chi_{ij}(X,Y) \quad \text{for each } (i,j) \in U_2. \tag{16}$$

Let $K_d = \langle x, y \rangle$, where $x^{2^d} = y^{2^d} = 1$, and let $E = \langle x^{2^{d-1}}, y^{2^{d-1}} \rangle$. We wish to construct a signature set $\{\alpha_{ij} : (i,j) \in U_2\}$ on $K_d$ with respect to $E$. Define the $\alpha_{ij}$ in $\mathbb{Z}K_d$ in terms of the polynomials $A_{ij}$ via

$$\left.\begin{aligned}
\alpha_{00} &= (1 + x^{2^{d-2}})A_{00}(x,y^2) + y(1 - x^{2^{d-2}})A_{10}(x,y^2), \\
\alpha_{01} &= (1 + x^{2^{d-2}})A_{01}(x,y^2) + y(1 - x^{2^{d-2}})A_{11}(x,y^2), \\
\alpha_{10} &= (1 + y^{2^{d-2}})A_{10}(x^2,y) + x(1 - y^{2^{d-2}})A_{11}(x^2,y), \\
\alpha_{11} &= (1 + x^{2^{d-2}}y^{2^{d-2}})A_{10}(x^2,xy) + x(1 - x^{2^{d-2}}y^{2^{d-2}})A_{11}(x^2,xy),
\end{aligned}\right\} \tag{17}$$

and let the characters of $E$ be

$$\psi_{ij} = \big(1 + (-1)^i x^{2^{d-1}}\big)\big(1 + (-1)^j y^{2^{d-1}}\big) \quad \text{for each } (i,j) \in U_2.$$

We firstly use Proposition 2.4 to show it is sufficient to prove for each $(i,j) \neq (1,1)$ that $\alpha_{ij}$ is a signature block with respect to $\psi_{ij}$. Let $\sigma$ be the group automorphism of $K_d$ that maps $x$ to itself and maps $y$ to $xy$. Then $\sigma(\alpha_{10}) = \alpha_{11}$ by definition, and $\sigma$ fixes $E$, and

$$\sigma(\psi_{10}) = (1 - x^{2^{d-1}})(1 + x^{2^{d-1}}y^{2^{d-1}}) = (1 - x^{2^{d-1}})(1 - y^{2^{d-1}}) = \psi_{11}.$$

Therefore if $\alpha_{10}$ is a signature block on $K_d$ with respect to $\psi_{10}$, then $\alpha_{11}$ is a signature block on $K_d$ with respect to $\psi_{11}$ by Proposition 2.4.

We next show that $\alpha_{00}$ is a $\{\pm 1\}$-valued function on a set of coset representatives for $E$ in $K_d$, and a similar argument shows that the same holds for $\alpha_{01}$ and $\alpha_{10}$. By definition, $A_{00}(X,Y)$ is $\{\pm 1\}$-valued on exactly one of the four values $\big\{X^iY^j, X^iY^{j+2^{d-2}}, X^{i+2^{d-2}}Y^j, X^{i+2^{d-2}}Y^{j+2^{d-2}}\big\}$ for $0 \leq i < 2^{d-2}$, $0 \leq j < 2^{d-2}$. Therefore $A_{00}(x,y^2)$ is $\{\pm 1\}$-valued on exactly one of the four values $\big\{x^iy^{2j}, x^iy^{2j+2^{d-1}}, x^{i+2^{d-2}}y^{2j}, x^{i+2^{d-2}}y^{2j+2^{d-1}}\big\}$ for $0 \leq i < 2^{d-2}$, $0 \leq j < 2^{d-2}$, and so $(1 + x^{2^{d-2}})A_{00}(x,y^2)$ is $\{\pm 1\}$-valued on exactly one of the four values $\big\{x^iy^{2j}, x^iy^{2j+2^{d-1}}, x^{i+2^{d-1}}y^{2j}, x^{i+2^{d-1}}y^{2j+2^{d-1}}\big\}$ for $0 \leq i < 2^{d-1}$, $0 \leq j < 2^{d-2}$. Likewise, $y(1 - x^{2^{d-2}})A_{10}(x,y^2)$ is $\{\pm 1\}$-valued on exactly one of the four values $\big\{x^iy^{2j+1}, x^iy^{2j+2^{d-1}+1}, x^{i+2^{d-1}}y^{2j+1}, x^{i+2^{d-1}}y^{2j+2^{d-1}+1}\big\}$ for $0 \leq i < 2^{d-1}$, $0 \leq j < 2^{d-2}$. Combining, $\alpha_{00}$ is $\{\pm 1\}$-valued on exactly one of the four values $\big\{x^iy^j, x^iy^{j+2^{d-1}}, x^{i+2^{d-1}}y^j, x^{i+2^{d-1}}y^{j+2^{d-1}}\big\}$ for $0 \leq i < 2^{d-1}$, $0 \leq j < 2^{d-1}$.

It remains to show that in $\mathbb{Z}K_d$ we have

$$\alpha_{ij}\psi_{ij}\alpha_{ij}^{(-1)} = 2^{2d-2}\psi_{ij} \quad \text{for each } (i,j) \neq (1,1). \tag{18}$$

Using $x^{2^d} = 1$, for $i, k \in \{0, 1\}$ we have the identity

$$(1 + x^{2^{d-1}})(1 + (-1)^i x^{2^{d-2}})(1 + (-1)^k x^{-2^{d-2}}) = \begin{cases} 2(1 + x^{2^{d-1}})(1 + (-1)^i x^{2^{d-2}}) & \text{if } i = k, \\ 0 & \text{if } i \neq k, \end{cases}$$

and multiplication by $1 + (-1)^j y^{2^{d-1}}$ for $j \in \{0, 1\}$ then gives

$$(1 + (-1)^i x^{2^{d-2}})\psi_{0j}(1 + (-1)^k x^{-2^{d-2}}) = \begin{cases} 2(1 + x^{2^{d-1}})\chi_{ij}(x, y^2) & \text{if } i = k, \\ 0 & \text{if } i \neq k. \end{cases} \tag{19}$$

We can now establish (18) for $(i, j) = (0, 0)$. Using (17), we calculate

$$\begin{aligned} \alpha_{00}\psi_{00}\alpha_{00}^{(-1)} &= \big((1 + x^{2^{d-2}})A_{00}(x, y^2) + y(1 - x^{2^{d-2}})A_{10}(x, y^2)\big) \times \psi_{00} \times \\ &\quad \big((1 + x^{-2^{d-2}})A_{00}(x, y^2)^{(-1)} + y^{-1}(1 - x^{-2^{d-2}})A_{10}(x, y^2)^{(-1)}\big) \\ &= 2(1 + x^{2^{d-1}})A_{00}(x, y^2)\chi_{00}(x, y^2)A_{00}(x, y^2)^{(-1)} + \\ &\quad 2(1 + x^{2^{d-1}})A_{10}(x, y^2)\chi_{10}(x, y^2)A_{10}(x, y^2)^{(-1)}, \end{aligned} \tag{20}$$

using (19) with $i \neq k$ to remove the terms involving $A_{00}(x, y^2)A_{10}(x, y^2)^{(-1)}$ and $A_{10}(x, y^2)A_{00}(x, y^2)^{(-1)}$, and using (19) with $i = k$ to simplify the surviving terms. Take $X = x$ and $Y = y^2$ in (16) to show that, in the polynomial ring $\mathbb{Z}[x, y]/\langle 1 - x^{2^{d-1}}, 1 - y^{2^d}\rangle$,

$$A_{ij}(x, y^2)\chi_{ij}(x, y^2)A_{ij}(x, y^2)^{(-1)} = 2^{2d-4}\chi_{ij}(x, y^2) \quad \text{for each } (i, j) \in U_2.$$

This implies that, in the polynomial ring $\mathbb{Z}[x, y]/\langle 1 - x^{2^d}, 1 - y^{2^d}\rangle$,

$$\begin{aligned} &(1 + x^{2^{d-1}})A_{ij}(x, y^2)\chi_{ij}(x, y^2)A_{ij}(x, y^2)^{(-1)} \\ &\qquad = 2^{2d-4}(1 + x^{2^{d-1}})\chi_{ij}(x, y^2) \quad \text{for each } (i, j) \in U_2. \end{aligned}$$

Substitution in (20) then gives

$$\alpha_{00}\psi_{00}\alpha_{00}^{(-1)} = 2^{2d-3}(1 + x^{2^{d-1}})(\chi_{00}(x, y^2) + \chi_{10}(x, y^2)) = 2^{2d-2}\psi_{00},$$

so (18) holds for $(i, j) = (0, 0)$.

A similar derivation gives

$$\begin{aligned} \alpha_{01}\psi_{01}\alpha_{01}^{(-1)} &= 2^{2d-3}(1 + x^{2^{d-1}})(\chi_{01}(x, y^2) + \chi_{11}(x, y^2)) = 2^{2d-2}\psi_{01}, \\ \alpha_{10}\psi_{10}\alpha_{10}^{(-1)} &= 2^{2d-3}(1 + y^{2^{d-1}})(\chi_{10}(x^2, y) + \chi_{11}(x^2, y)) = 2^{2d-2}\psi_{10}, \end{aligned}$$

so that (18) holds for $(i, j) = (0, 1)$ and $(i, j) = (1, 0)$.

Therefore the $\alpha_{ij}$ form a signature set on $K_d$ with respect to $E$. This shows that case $d$ is true and completes the induction. □

We next illustrate the recursive construction method used in the proof of Theorem 3.2.

**Example 3.3.** *A trivial signature set* $\{A_{ij}^1 : (i, j) \in U_2\}$ *on* $C_2^2$ *with respect to itself is given by*

$$A_{ij}^1 = 1 \quad \text{for all } (i, j) \in U_2.$$

*Apply the recursion* (17) *with* $d = 2$ *to obtain the signature set* $\{A_{ij}^2 : (i, j) \in U_2\}$ *on* $C_4^2 = \langle x, y\rangle$ *with respect to* $\langle x^2, y^2\rangle \cong C_2^2$ *given by*

$$\begin{aligned} A_{00}^2 = A_{01}^2 &= (1 + x) + y(1 - x) = 1 + x + y - xy, \\ A_{10}^2 &= (1 + y) + x(1 - y) = 1 + x + y - xy, \end{aligned}$$

$$A_{11}^2 = (1+xy) + x(1-xy) = 1 + x - x^2y + xy.$$

*Apply the recursion* (17) *again with* $d = 3$ *to obtain the signature set* $\{A_{ij}^3 : (i,j) \in U_2\}$ *on* $C_8^2 = \langle x, y\rangle$ *with respect to* $\langle x^4, y^4\rangle \cong C_2^2$ *given by*

$$\begin{aligned}
A_{00}^3 &= (1+x^2)A_{00}^2(x,y^2) + y(1-x^2)A_{10}^2(x,y^2) \\
&= (1+x^2)(1+x+y^2-xy^2) + y(1-x^2)(1+x+y^2-xy^2), \\
A_{01}^3 &= (1+x^2)A_{01}^2(x,y^2) + y(1-x^2)A_{11}^2(x,y^2) \\
&= (1+x^2)(1+x+y^2-xy^2) + y(1-x^2)(1+x-x^2y^2+xy^2), \\
A_{10}^3 &= (1+y^2)A_{10}^2(x^2,y) + x(1-y^2)A_{11}^2(x^2,y) \\
&= (1+y^2)(1+x^2+y-x^2y) + x(1-y^2)(1+x^2-x^4y+x^2y), \\
A_{11}^3 &= (1+x^2y^2)A_{10}^2(x^2,xy) + x(1-x^2y^2)A_{11}^2(x^2,xy) \\
&= (1+x^2y^2)(1+x^2+xy-x^3y) + x(1-x^2y^2)(1+x^2-x^5y+x^3y).
\end{aligned}$$

We note that the recursion (17) in the proof of Theorem 3.2 has a simpler form when expressed in terms of group ring elements $B_{ij} = A_{ij}\chi_{ij}$ and $\beta_{ij} = \alpha_{ij}\psi_{ij}$, namely

$$\begin{aligned}
\beta_{00}(x,y) &= (1+x^{2^{d-1}})\big(B_{00}(x,y^2) + yB_{10}(x,y^2)\big), \\
\beta_{01}(x,y) &= (1+x^{2^{d-1}})\big(B_{01}(x,y^2) + yB_{11}(x,y^2)\big), \\
\beta_{10}(x,y) &= (1+y^{2^{d-1}})\big(B_{10}(x^2,y) + xB_{11}(x^2,y)\big), \\
\beta_{11}(x,y) &= (1-y^{2^{d-1}})\big(B_{10}(x^2,xy) + xB_{11}(x^2,xy)\big).
\end{aligned}$$

We now prove Theorem 3.1 in full generality, using the proof of Theorem 3.2 as a model. We abbreviate some of the proof, focussing attention on the parts for which a new argument or additional care is needed.

*Proof of Theorem 3.1.* The proof is by induction on $d \ge 1$. In the case $d = 1$, we have $r = 2$ and $\mathcal{K}_{1,2} = \{C_2^2\}$. The case $d = 1$ is therefore true, because there exists a trivial signature set on $C_2^2$.

Assume all cases up to $d - 1 \ge 1$ are true. We shall write $u = (i, j, u_3, \dots, u_r) \in U_r$ as $(i, j, v)$, where $v = (u_3, \dots, u_r)$. Let

$$K_{d,r} = C_{2^{a_1}} \times \cdots \times C_{2^{a_r}} = \langle x, y, x_3, \dots, x_r\rangle \in \mathcal{K}_{d,r},$$

where $x^{2^{a_1}} = y^{2^{a_2}} = x_3^{2^{a_3}} = \cdots = x_r^{2^{a_r}} = 1$ and $d - r + 2 \ge a_1 \ge a_2 \ge \cdots \ge a_r \ge 1$ and $\sum_i a_i = 2d - r + 2$. The unique subgroup of $K_{d,r}$ isomorphic to $C_2^r$ is $E_{d,r} = \langle x^{2^{a_1-1}}, y^{2^{a_2-1}}, x_3^{2^{a_3-1}}, \dots, x_r^{2^{a_r-1}}\rangle$.

If $a_r = 1$, then by the inductive hypothesis there is a signature set on the group $\langle x, y, x_3, \dots, x_{r-1}\rangle \in \mathcal{K}_{d-1,r-1}$. In that case we may use Proposition 2.5 to combine this with a trivial signature set on $C_2$ in order to obtain the required signature set on $K_{d,r}$ with respect to $E_{d,r}$.

We may therefore take $d - r + 2 \ge a_1 \ge a_2 \ge \cdots \ge a_r \ge 2$. This implies that $r \le d$, and if $r > 2$ then $a_3 \le d - r + 1$ (otherwise $2d - r + 2 = \sum_i a_i \ge 3(d - r + 2) + (r - 3)2 = 3d - r$, giving the contradiction $r \le d \le 2$). By the inductive hypothesis, the group

$$C_{2^{a_1-1}} \times C_{2^{a_2-1}} \times C_{2^{a_3}} \times \cdots \times C_{2^{a_r}} = \langle X, Y, x_3, \dots, x_r\rangle \in \mathcal{K}_{d-1,r},$$

where $X^{2^{a_1-1}} = Y^{2^{a_2-1}} = x_3^{2^{a_3}} = \cdots = x_r^{2^{a_r}} = 1$, therefore contains a signature set $\{A_{ijv} : (i,j,v) \in U_r\}$ with respect to $E_{d-1,r} = \langle X^{2^{a_1-2}}, Y^{2^{a_2-2}}, x_3^{2^{a_3-1}}, \dots, x_r^{2^{a_r-1}}\rangle$.

Regard each group ring element $A_{ijv}$ as a polynomial in $X, Y, x_3, \dots, x_r$, but abbreviate this as $A_{ijv}(X,Y)$ because we will make variable substitutions only for $X$ and $Y$. Similarly, regard each character of $E_{d-1,r}$ as a polynomial

$$\chi_{ijv}(X,Y) = \big(1 + (-1)^i X^{2^{a_1-2}}\big)\big(1 + (-1)^j Y^{2^{a_2-2}}\big)\,\tau_v$$

where

$$\tau_v = (1 + (-1)^{u_3} x_3^{2^{a_3-1}}) \dots (1 + (-1)^{u_r} x_r^{2^{a_r-1}}).$$

By assumption, in the polynomial ring $\mathbb{Z}[X,Y,x_3,\ldots,x_r]/\langle 1-X^{2^{a_1-1}}, 1-Y^{2^{a_2-1}}, 1-x_3^{2^{a_3}},\ldots,1-x_r^{2^{a_r}}\rangle$ we have

$$A_{ijv}(X,Y)\chi_{ijv}(X,Y)A_{ijv}(X,Y)^{(-1)} = 2^{2d-2r}\chi_{ijv}(X,Y) \quad \text{for each } (i,j,v)\in U_r. \tag{21}$$

We wish to construct a signature set $\{\alpha_{ijv} : (i,j,v)\in U_r\}$ on $K_{d,r}$ with respect to $E_{d,r}$. Define the $\alpha_{ijv}$ in $\mathbb{Z}K_{d,r}$ in terms of the polynomials $A_{ijv}$ via

$$\left.\begin{aligned}
\alpha_{00v} &= (1+x^{2^{a_1-2}})A_{00v}(x,y^2) + y(1-x^{2^{a_1-2}})A_{10v}(x,y^2),\\
\alpha_{01v} &= (1+x^{2^{a_1-2}})A_{01v}(x,y^2) + y(1-x^{2^{a_1-2}})A_{11v}(x,y^2),\\
\alpha_{10v} &= (1+y^{2^{a_2-2}})A_{10v}(x^2,y) + x(1-y^{2^{a_2-2}})A_{11v}(x^2,y),\\
\alpha_{11v} &= (1+x^{2^{a_1-2}}y^{2^{a_2-2}})A_{10v}(x^2,x^{2^{a_1-a_2}}y) + x(1-x^{2^{a_1-2}}y^{2^{a_2-2}})A_{11v}(x^2,x^{2^{a_1-a_2}}y),
\end{aligned}\right\} \tag{22}$$

and let the characters of $E_{d,r}$ be

$$\psi_{ijv} = \big(1+(-1)^i x^{2^{a_1-1}}\big)\big(1+(-1)^j y^{2^{a_2-1}}\big)\,\tau_v \quad \text{for each } (i,j,v)\in U_r.$$

We firstly use Proposition 2.4 to show it is sufficient to prove for each $(i,j,v)\neq(1,1,v)$ that $\alpha_{ijv}$ is a signature block with respect to $\psi_{ijv}$. Let $\sigma$ be the group automorphism of $K_{d,r}$ that maps $x$ to itself and maps $y$ to $x^{2^{a_1-a_2}}y$ (which has order $2^{a_2}$). Then $\sigma(\alpha_{10v})=\alpha_{11v}$ by definition, and $\sigma$ fixes $E_{d,r}$, and $\sigma(\psi_{10v})=\psi_{11v}$. Therefore if $\alpha_{10v}$ is a signature block on $K_{d,r}$ with respect to $\psi_{10v}$, then $\alpha_{11v}$ is a signature block on $K_{d,r}$ with respect to $\psi_{11v}$ by Proposition 2.4.

We next show that each $\alpha_{00v}$ is a $\{\pm1\}$-valued function on a set of coset representatives for $E_{d,r}$ in $K_{d,r}$, and a similar argument shows that the same holds for each $\alpha_{01v}$ and $\alpha_{10v}$. Fix $z=x_3^{i_3}\ldots x_r^{i_r}$. By definition, $A_{00v}(X,Y)$ is $\{\pm1\}$-valued on exactly one of the four values $\{X^iY^jz, X^iY^{j+2^{a_2-2}}z, X^{i+2^{a_1-2}}Y^jz, X^{i+2^{a_1-2}}Y^{j+2^{a_2-2}}z\}$ for $0\le i<2^{a_1-2}$, $0\le j<2^{a_2-2}$. It follows that $\alpha_{00v}$ is $\{\pm1\}$-valued on exactly one of the four values $\{x^iy^jz, x^iy^{j+2^{a_2-1}}z, x^{i+2^{a_1-1}}y^jz, x^{i+2^{a_1-1}}y^{j+2^{a_2-1}}z\}$ for $0\le i<2^{a_1-1}$, $0\le j<2^{a_2-1}$.

It remains to show that in $\mathbb{Z}K_{d,r}$ we have

$$\alpha_{ijv}\psi_{ijv}\alpha_{ijv}^{(-1)} = 2^{2d-2r+2}\psi_{ijv} \quad \text{for each } (i,j,v)\neq(1,1,v). \tag{23}$$

For $i,j,k\in\{0,1\}$, we have the identity

$$(1+(-1)^i x^{2^{a_1-2}})\psi_{0jv}(1+(-1)^k x^{-2^{a_1-2}}) = \begin{cases} 2(1+x^{2^{a_1-1}})\chi_{ijv}(x,y^2) & \text{if } i=k,\\ 0 & \text{if } i\neq k,\end{cases} \tag{24}$$

from which we now establish (23) for $(i,j,v)=(0,0,v)$. We calculate

$$\begin{aligned}
\alpha_{00v}\psi_{00v}\alpha_{00v}^{(-1)} &= \big((1+x^{2^{a_1-2}})A_{00v}(x,y^2) + y(1-x^{2^{a_1-2}})A_{10v}(x,y^2)\big)\times\psi_{00v}\times\\
&\qquad \big((1+x^{-2^{a_1-2}})A_{00v}(x,y^2)^{(-1)} + y^{-1}(1-x^{-2^{a_1-2}})A_{10v}(x,y^2)^{(-1)}\big)\\
&= 2(1+x^{2^{a_1-1}})A_{00v}(x,y^2)\chi_{00v}(x,y^2)A_{00v}(x,y^2)^{(-1)}+\\
&\qquad 2(1+x^{2^{a_1-1}})A_{10v}(x,y^2)\chi_{10v}(x,y^2)A_{10v}(x,y^2)^{(-1)},
\end{aligned} \tag{25}$$

using (24). Take $X=x$ and $Y=y^2$ in (21) to show that, in the polynomial ring $\mathbb{Z}[x,y,x_3,\ldots,x_r]/\langle 1-x^{2^{a_1}}, 1-y^{2^{a_2}}, 1-x_3^{2^{a_3}},\ldots,1-x_r^{2^{a_r}}\rangle$,

$$\begin{aligned}
&(1+x^{2^{a_1-1}})A_{ijv}(x,y^2)\chi_{ijv}(x,y^2)A_{ijv}(x,y^2)^{(-1)}\\
&\qquad\qquad = 2^{2d-2r}(1+x^{2^{a_1-1}})\chi_{ijv}(x,y^2) \quad \text{for each } (i,j,v)\in U_r.
\end{aligned}$$

Substitution in (25) then gives

$$\alpha_{00v}\psi_{00v}\alpha_{00v}^{(-1)} = 2^{2d-2r+1}(1+x^{2^{a_1-1}})(\chi_{00v}(x,y^2)+\chi_{10v}(x,y^2)) = 2^{2d-2r+2}\psi_{00v},$$

so (23) holds for $(i,j,v) = (0,0,v)$.

A similar derivation gives

$$\alpha_{01v}\psi_{01v}\alpha_{01v}^{(-1)} = 2^{2d-2r+1}(1 + x^{2^{a_1-1}})(\chi_{01v}(x,y^2) + \chi_{11v}(x,y^2)) = 2^{2d-2r+2}\psi_{01v},$$
$$\alpha_{10v}\psi_{10v}\alpha_{10v}^{(-1)} = 2^{2d-2r+1}(1 + y^{2^{a_2-1}})(\chi_{10v}(x^2,y) + \chi_{11v}(x^2,y)) = 2^{2d-2r+2}\psi_{10v},$$

so that (23) holds for $(i,j,v) = (0,1,v)$ and $(i,j,v) = (1,0,v)$.

Therefore the $\alpha_{ijv}$ form a signature set on $K_{d,r}$ with respect to $E_{d,r}$. This shows that case $d$ is true and completes the induction. $\square$

We now illustrate the recursive construction method used in the proof of Theorem 3.1.

**Example 3.4.** *We shall construct a signature set on $C_8 \times C_4^2$. By Example 3.3, there is a signature set $\{A'_{ik} : (i,k) \in U_2\}$ on $C_4^2 = \langle x, z\rangle$ with respect to $\langle x^2, z^2\rangle$ given by*

$$A'_{00} = A'_{01} = A'_{10} = 1 + x + z - xz,$$
$$A'_{11} = 1 + x - x^2z + xz.$$

*Use the product construction of Proposition 2.5 to combine this with a trivial signature set on $C_2$, producing a signature set $\{A_{ijk} : (i,j,k) \in U_3\}$ on $C_4 \times C_2 \times C_4 = \langle x,y,z\rangle$ with respect to $\langle x^2, y, z^2\rangle \cong C_2^3$ given by*

$$A_{000} = A_{010} = A_{001} = A_{011} = A_{100} = A_{110} = 1 + x + z - xz,$$
$$A_{101} = A_{111} = 1 + x - x^2z + xz.$$

*Now apply the recursion (22) to produce a signature set $\{\alpha_{ijk} : (i,j,k) \in U_3\}$ on $C_8 \times C_4^2 = \langle x,y,z\rangle$ with respect to $\langle x^4, y^2, z^2\rangle \cong C_2^3$ given by*

$$\begin{aligned}
\alpha_{000} &= (1+x^2)(1+x+z-xz) + y(1-x^2)(1+x+z-xz),\\
\alpha_{001} &= (1+x^2)(1+x+z-xz) + y(1-x^2)(1+x-x^2z+xz),\\
\alpha_{010} &= (1+x^2)(1+x+z-xz) + y(1-x^2)(1+x+z-xz),\\
\alpha_{011} &= (1+x^2)(1+x+z-xz) + y(1-x^2)(1+x-x^2z+xz),\\
\alpha_{100} &= (1+y)(1+x^2+z-x^2z) + x(1-y)(1+x^2+z-x^2z),\\
\alpha_{101} &= (1+y)(1+x^2-x^4z+x^2z) + x(1-y)(1+x^2-x^4z+x^2z),\\
\alpha_{110} &= (1+x^2y)(1+x^2+z-x^2z) + x(1-x^2y)(1+x^2+z-x^2z),\\
\alpha_{111} &= (1+x^2y)(1+x^2-x^4z+x^2z) + x(1-x^2y)(1+x^2-x^4z+x^2z).
\end{aligned}$$

# 4 Further Construction Methods

As shown in Table 1, our main result (Theorem 1.15) uses signature sets on abelian groups to provide constructions for difference sets in the great majority of the groups of order 64 and 256 that are not excluded by Theorems 1.3 and 1.5. In this section, we describe the methods that were used to show that the 22 remaining groups of order 64, and the 1,416 remaining groups of order 256, all belong to $\mathcal{H}$.

In Section 4.1, we present a construction method arising under Theorem 2.3 from a signature set on a nonabelian group; recall that Definition 2.1 for a signature set does not require the group $K$ to be abelian. In Section 4.2, we present a product construction using perfect ternary arrays, without constraining these arrays in relation to a subgroup. In Section 4.3, we describe three non-systematic methods of transferring a difference set in one group to another. We used the methods of Sections 4.1–4.3 to establish that all but one of the 22 remaining non-excluded groups of order 64, and all but one of the 1,416 remaining non-excluded groups of order 256, belong to $\mathcal{H}$. In Section 4.4, we describe the construction of a Hadamard difference set in both of these final groups using group representations. In Section 4.5, we show that the signature set construction of Section 4.1 and the perfect ternary array product construction of Section 4.2 are closely related and can sometimes be combined, which could in future assist in determining which 2-groups of order larger than 256 belong to $\mathcal{H}$.

## 4.1 Signature Set on Nonabelian Group

Our first construction method applies Theorem 2.3 to a signature set on a nonabelian group to produce Hadamard difference sets in a variety of larger groups. We illustrate this method by exhibiting a signature set on the quaternion group of order 8.

**Proposition 4.1.** *Let $Q = \langle x, y : x^4 = y^4 = 1,\ yxy^{-1} = x^{-1},\ x^2 = y^2 \rangle$ be the quaternion group of order 8, and let $G$ be a group of order 16 containing a subgroup isomorphic to $Q$. Then $G \in \mathcal{H}$.*

*Proof.* Let $E_1 = \langle x^2 \rangle \cong C_2$, and let

$$\chi_0 = 1 + x^2, \quad \chi_1 = 1 - x^2$$

be the characters of $E_1$. Since $E_1$ is the unique subgroup of $Q$ isomorphic to $C_2$, and $Q$ has index 2 and so is normal in $G$, we have that $E_1$ is normal in $G$. Therefore by Theorem 2.3 with $r = 1$, it is sufficient to exhibit a signature set $\{A_0, A_1\}$ on $Q$ with respect to $E_1$ (and then according to (14) there is a difference set in $G$ of the form $g_0 A_0 \chi_0 + g_1 A_1 \chi_1$).

Let $A = 1 - x - y - xy$, and let $\{A_0, A_1\} = \{A, A\}$. Then $A$ is a $\{\pm 1\}$-valued function on a set of coset representatives for $E_1$ in $Q$, and direct calculation shows that $AA^{(-1)} = 4$ in $\mathbb{Z}Q$. Since $E_1$ is a central subgroup of $Q$, we therefore have in $\mathbb{Z}Q$ that

$$A_u \chi_u A_u^{(-1)} = A_u A_u^{(-1)} \chi_u = 4\chi_u = \tfrac{|Q|}{2} \chi_u \quad \text{for } u \in \{0, 1\},$$

as required. □

As noted prior to Table 1, we can use Theorem 1.15 and Proposition 4.1 to recover the classification of Hadamard groups of order 16 carried out in the 1970s: Theorem 1.15 accounts for the 10 groups containing a normal subgroup isomorphic to $C_2^2$, and Proposition 4.1 accounts for 2 further groups (the generalized quaternion group and the semidihedral group) containing a subgroup isomorphic to $Q$.

Furthermore, using Proposition 2.5 we may now take the product of a signature set on $Q$ with respect to $E_1$ given in the proof of Proposition 4.1, and a trivial signature set on $C_2$, to give a signature set on $Q \times C_2$ with respect to $E_1 \times C_2 \cong C_2^2$. Then from Theorem 2.3, every group of order 64 containing a normal subgroup isomorphic to $Q \times C_2$ belongs to $\mathcal{H}$.

We now use a Hadamard difference set to construct a signature set on certain groups of order $2^{2d+1}$.

**Proposition 4.2.** *Suppose $D$ is a Hadamard difference set in a group $H$, and let $E_1 \cong C_2$. Then $\{D, D\}$ is a signature set on $H \times E_1$ with respect to $E_1$.*

*Proof.* We are given that $D$ is a $\{\pm 1\}$-valued function on the set $H$ of coset representatives for $E_1$ in $H \times E_1$. Let $\{A_0, A_1\} = \{D, D\}$, and write $E_1 = \langle x \rangle$ so that the characters of $E_1$ are $\chi_0 = 1 + x$ and $\chi_1 = 1 - x$. Since $x$ commutes with $D$, we have in $\mathbb{Z}(H \times E_1)$ that

$$A_u \chi_u A_u^{(-1)} = DD^{(-1)} \chi_u = |H| \chi_u = \tfrac{|H \times E_1|}{2} \chi_u \quad \text{for } u \in \{0, 1\},$$

as required. □

**Corollary 4.3.** *Suppose $H \in \mathcal{H}$. Let $G$ be a group containing a normal subgroup $E_1 \cong C_2$, and containing $H \times E_1$ as a subgroup of index 2. Then $G \in \mathcal{H}$.*

*Proof.* By Proposition 4.2, there exists a signature set on $H \times E_1$ with respect to $E_1$. Since $E_1$ and $H \times E_1$ are both normal in $G$, we have $G \in \mathcal{H}$ by Theorem 2.3. □

The technique of constructing Hadamard difference sets from signature sets on nonabelian groups appears to have significant potential, but we do not currently have a method of producing such signature sets that is as powerful as the recursive construction used to prove Theorem 3.1 for abelian groups.

## 4.2 Product of Perfect Ternary Arrays

Our second construction method relies on a key feature of the proof of Proposition 4.1, namely the existence of a $\{+1, 0, -1\}$-valued function $A$ on the group $Q$ satisfying $AA^{(-1)} = 4$ in $\mathbb{Z}Q$. This function $A$ is also $\{\pm 1\}$-valued on a set of coset representatives for a subgroup of $Q$, but we do not require this additional structure in the following definition.

**Definition 4.4.** *Let $G$ be a group. A* perfect ternary array *in $G$ is a $\{+1, 0, -1\}$-valued function $T$ on $G$ satisfying $TT^{(-1)} = c$ in $\mathbb{Z}G$ for some integer $c$.*

The set of elements of a group $G$ on which a group ring element $A \in \mathbb{Z}G$ is nonzero is the *support* of $A$; the size of this set is the *weight* of $A$, written $\mathrm{wt}(A)$. We firstly show that the integer $c$ in Definition 4.4 is equal to the weight of the perfect ternary array, and that it is a square.

**Lemma 4.5.** *Let $G$ be a group, and suppose $T = \sum_{g \in G} t_g g$ is a perfect ternary array where each $t_g \in \{+1, 0, -1\}$. Then $TT^{(-1)} = \mathrm{wt}(T) = \Big(\sum_{g \in G} t_g\Big)^2$.*

*Proof.* For some integer $c$, we have

$$c = TT^{(-1)} = \Big(\sum_{h \in G} t_h h\Big)\Big(\sum_{g \in G} t_g g^{-1}\Big) = \sum_{k \in G}\Big(\sum_{g \in G} t_{kg} t_g\Big)k$$

by writing $k = hg^{-1}$. Comparison of the coefficients of $1_G$ and $k \neq 1_G$ gives

$$\begin{aligned} c &= \sum_{g \in G} t_g^2, \\ 0 &= \sum_{g \in G} t_{kg} t_g \quad \text{for } k \neq 1_G. \end{aligned} \tag{26}$$

These relations together give

$$c = \sum_{k \in G}\sum_{g \in G} t_{kg} t_g = \sum_{g \in G}\Big(\sum_{h \in G} t_h\Big)t_g = \Big(\sum_{g \in G} t_g\Big)^2.$$

The result follows by combining with (26), noting that $\sum_{g \in G} t_g^2 = \mathrm{wt}(T)$ because $T$ is $\{+1, 0, -1\}$-valued. $\square$

By Lemma 4.5 and (1), we may regard a Hadamard difference set in a group $G$ as a perfect ternary array $T$ in $G$ for which $TT^{(-1)} = |G|$. A survey of results on the matrix representation of a perfect ternary array in an abelian group is given in [2]. We next give two examples of perfect ternary arrays of weight 4, whose properties can be verified by direct calculation. The second example appears in the proof of Proposition 4.1.

**Example 4.6** (Dillon 1990 (unpublished))**.** (*i*) *Suppose $G$ is a group containing a nonidentity element $x$ and an involution (element of order 2) $y$ that commutes with $x$. Then $T = 1 - x - y - xy$ is a perfect ternary array of weight 4 in $G$.*

(*ii*) *Let $Q = \langle x, y : x^4 = y^4 = 1, yxy^{-1} = x^{-1}, x^2 = y^2\rangle$ be the quaternion group of order 8. Then $T = 1 - x - y - xy$ is a perfect ternary array of weight 4 in $Q$.*

Every perfect ternary array of weight 4 in a group of even order is equivalent to Example 4.6 (*i*) or (*ii*) [5, Lemma 2].

We now construct a Hadamard difference set as a product of perfect ternary arrays.

**Proposition 4.7** (Dillon 1990 (unpublished), Bhattacharya and Smith [5])**.** *Let $T_1, T_2, \ldots, T_s$ be subsets of a group $G$, and let $D = \prod_{i=1}^{s} T_i$. Suppose that*

(*i*) *each $T_i$ is a perfect ternary array in $G$,* (*ii*) $\mathrm{wt}(D) = \prod_{i=1}^{s} \mathrm{wt}(T_i)$,

(*iii*) $\mathrm{wt}(D) = |G|$.

*Then $D$ corresponds to a Hadamard difference set in $G$.*

*Proof.* By condition (*ii*), $D$ is a $\{+1, 0, -1\}$-valued function on $G$. Now $DD^{(-1)} = \prod_{i=1}^{s} \mathrm{wt}(T_i)$ by Lemma 4.5, and then by conditions (*ii*) and (*iii*) we have $DD^{(-1)} = |G|$. □

Since a Hadamard difference set is a special case of a perfect ternary array, we may regard Theorem 1.2 as constructing a Hadamard difference set in $G$ as the product $D_1D_2$ of two perfect ternary arrays $D_1$ and $D_2$ contained in subgroups $H_1$ and $H_2$ of $G$. In contrast, Proposition 4.7 constructs Hadamard difference sets as the product of $s$ perfect ternary arrays $T_i$, with the important relaxation that each $T_i$ need not be structurally constrained in relation to a subgroup of $G$.

This generality gives Proposition 4.7 considerable power. We take each $T_i$ to be either a perfect ternary array of weight 4 (having one of the two forms of Example 4.6), or else a Hadamard difference set in a subgroup of $G$. This allows us to construct all 27 inequivalent difference sets in the 12 groups of order 16 contained in $\mathcal{H}$ [5]; a difference set in 17 of the 22 remaining non-excluded groups of order 64; and a difference set in 1,358 of the 1,416 remaining non-excluded groups of order 256 (see Table 1). However, the same generality means that testing whether a group $G$ lies in $\mathcal{H}$ because of Proposition 4.7 (involving a computer search over all suitable perfect ternary arrays) is significantly slower than testing whether $G$ lies in $\mathcal{H}$ because of Theorem 1.15 (involving simply testing whether $G$ contains a suitable normal abelian subgroup); see Section 5 for further details.

## 4.3 Transfer Methods

The construction methods of previous sections are collectively sufficient to demonstrate that the great majority of the groups of order 64 and 256 that are not excluded by Theorems 1.3 and 1.5 belong to $\mathcal{H}$. The key in almost all of these demonstrations is the existence of a signature set on a normal subgroup, from which a difference set arises using Theorem 2.3. Nonetheless, while the signature set concept is very powerful, it does not appear to be sufficient to determine $\mathcal{H}$ completely. The reason is that some groups (2 of order 64, and 10 of order 256) have the property that each of their normal subgroups also occurs as a normal subgroup of a group that is not in $\mathcal{H}$. We therefore require construction methods that do not rely on a signature set. We now describe three such methods, each of which uses a difference set in one group to discover a difference set in another (and so "transfers" a difference set between the two groups).

The first transfer method makes use of the equivalence between a difference set in a group $G$ and a symmetric design on whose points $G$ acts as a regular (sharply transitive) automorphism group. If the full automorphism group of the design is sufficiently large, it may well contain other subgroups which also act regularly on the points of the design; in this case, each of these subgroups also contains a difference set. For example, the group $C_2^4$ contains a difference set giving a $(16, 6, 2)$ symmetric design whose 2-rank is 6, and the automorphism group of this design contains 12 nonisomorphic subgroups of order 16 acting regularly on the points of the design. We thereby transfer a single difference set in $C_2^4$ to a difference set in all 11 of the other Hadamard groups of order 16. Similarly, the group $C_2^6$ contains a difference set giving a $(64, 28, 12)$ symmetric design whose 2-rank is 8, and the automorphism group of this design contains 171 nonisomorphic subgroups of order 64 acting regularly on the points of the design. We thereby transfer a single difference set in $C_2^6$ to 170 of the other 258 Hadamard groups of order 64.

The second transfer method applies when a difference set gives an algebraic structure in the group ring that also exists in other group rings. An example is Dillon's proof [14] of Theorem 1.5, which transfers a putative difference set in a group with a large dihedral quotient to a difference set in a group with a large cyclic quotient in order to apply the nonexistence result of Theorem 1.3. A second example is Theorem 2.3, which can be viewed as using Theorem 1.9 to transfer a difference set in an abelian group that contains $K$ to a difference set in a variety of nonabelian groups containing $K$. A third example is [16, Thm. 2], which transfers a difference set among groups sharing a subgroup $H$ of index 2 and a central element $g$ not in $H$. In general, suppose that a group $G$ is known to contain a difference set $D$, and that $G$ contains a large normal subgroup $K$. Let $\{g_u\}$ be a set of coset representatives for $K$ in $G$, and partition the elements of $D$ according to their membership of the cosets of $K$ to write $D = \sum_u g_u D_u$, where each $D_u \in \mathbb{Z}K$. Now let $G'$

be a group having the same order as $G$ and containing a normal subgroup $K'$ isomorphic to $K$. Let $\phi$ be an isomorphism from $K$ to $K'$. To transfer the difference set $D$ from $G$ to $G'$ we seek, by hand or by computer search, a set of coset representatives $\{g'_u\}$ for $K'$ in $G'$ for which $\sum_u g'_u \phi(D_u)$ is a difference set in $G'$.

The third transfer method takes advantage of the structure created by the GAP method for labelling group elements. A difference set $D$ with parameters $(v, k, \lambda)$ in a group $G$ of order $v$ can be represented in GAP as a $k$-subset $S$ of the element labels $\{1, 2, \ldots, v\}$. Given such a subset $S$ representing a difference set in $G$, we test in GAP whether the same subset $S$ also represents a difference set in another group $G'$ of order $v$. This method appears to have a greater chance of success when the GAP numbering for $G'$ is close to that of $G$, which often occurs when $G'$ has similar structure to $G$.

None of these three transfer methods is systematic, and it is not yet clear when they can be expected to succeed. Nonetheless, we were able to apply them to show that all but one of the remaining 5 non-excluded groups of order 64, and all but one of the remaining 58 non-excluded groups of order 256, belong to $\mathcal{H}$ (see Table 1). We construct a difference set in the final group of order 64 and of order 256 in Section 4.4.

## 4.4 The Final Group of Order 64 and of Order 256

The final two groups whose membership in $\mathcal{H}$ we wish to demonstrate are the order 64 modular group

$$M_{64} = C_{32} \rtimes_{17} C_2 = \langle x, y : x^{32} = y^2 = 1,\, yxy^{-1} = x^{17} \rangle,$$

and the order 256 group

$$C_{64} \rtimes_{47} C_4 = \langle x, y : x^{64} = y^4 = 1,\, yxy^{-1} = x^{47} \rangle$$

that is referenced in [19] as SmallGroup(256, 536). These nonabelian groups are each a cyclic extension of a cyclic group, and have small center and high exponent. Historically, they were the last groups of their order whose membership in $\mathcal{H}$ was determined: $M_{64}$ in 1991 [27], and SmallGroup(256, 536) in 2016 [38].

We firstly describe the original construction method used in [27] and [38], which strengthens the representation theory approach used in [13, Sect. 5] to construct a difference set in the order 256 group $C_{64} \rtimes_{33} C_4 = \langle x, y : x^{64} = y^4 = 1,\, yxy^{-1} = x^{33} \rangle$. We shall then reinterpret these constructions as arising from a modification of a signature set.

**Proposition 4.8.** *Let $G$ be a 2-group, let $g$ be a central involution in $G$, and let $\natural$ be the natural map from $G$ onto $G/\langle g \rangle$. Suppose there are $\{+1, 0, -1\}$-valued functions $D_0, D_1$ on $G$ for which $D_0(1+g)$ and $D_1(1-g)$ have disjoint supports whose union is $G$, and for which*

$$\natural(D_0)\natural(D_0)^{(-1)} = \tfrac{|G|}{4} \quad \text{in } \mathbb{Z}(G/\langle g \rangle), \tag{27}$$

$$D_1(1-g)D_1^{(-1)} = \tfrac{|G|}{4}(1-g) \quad \text{in } \mathbb{Z}G. \tag{28}$$

*Then $G \in \mathcal{H}$.*

*Proof.* We note that the existence of a central involution $g$ in the 2-group $G$ follows from the class equation for finite groups. Let

$$D = D_0(1+g) + D_1(1-g) \quad \text{in } \mathbb{Z}G, \tag{29}$$

which is a $\{\pm 1\}$-valued function on $G$ by the assumption on the supports of $D_0(1+g)$ and $D_1(1-g)$.

We now calculate

$$DD^{(-1)} = 2D_0(1+g)D_0^{(-1)} + 2D_1(1-g)D_1^{(-1)} \quad \text{in } \mathbb{Z}G. \tag{30}$$

By (27), in $\mathbb{Z}(G/\langle g \rangle)$ we have

$$\tfrac{|G|}{4} 1_{G/\langle g \rangle} = \natural(D_0)\natural(D_0)^{(-1)} = (D_0\langle g \rangle)(D_0^{(-1)}\langle g \rangle) = D_0 D_0^{(-1)} \langle g \rangle,$$

so that in $\mathbb{Z}G$ we have

$$\tfrac{|G|}{4}(1+g) = D_0 D_0^{(-1)}(1+g) = D_0(1+g)D_0^{(-1)}$$

because $g$ is central in $G$. Substitute this and (28) into (30) to obtain

$$DD^{(-1)} = \tfrac{|G|}{2}(1+g) + \tfrac{|G|}{2}(1-g) = |G|.$$

Therefore $D$ corresponds to a Hadamard difference set in $G$. □

When applying Proposition 4.8, we firstly seek a $\{+1, 0, -1\}$-valued group ring element $D_0$ satisfying condition (27), namely that $\natural(D_0)$ is a perfect ternary array of weight $\frac{|G|}{4}$ in the factor group $G/\langle g\rangle$. We then seek a $\{+1, 0, -1\}$-valued group ring element $D_1$ satisfying (28) for which $D_0(1+g)$ and $D_1(1-g)$ have disjoint supports whose union is $G$. It turns out that finding $D_0$ is relatively easy, whereas finding $D_1$ is much more difficult.

**Example 4.9** (Liebler and Smith construction for $M_{64}$ [27])**.** *We apply Proposition 4.8 to construct a Hadamard difference set in $M_{64} = C_{32} \rtimes_{17} C_2 = \langle x, y : x^{32} = y^2 = 1,\ yxy^{-1} = x^{17}\rangle$. The center of $M_{64}$ is $\langle x^2\rangle$, so $x^{16}$ is a central involution.*

*A $\{+1, 0, -1\}$-valued group ring element $D_0$ satisfying*

$$\natural(D_0)\natural(D_0)^{(-1)} = 16 \quad \text{in } \mathbb{Z}(M_{64}/\langle x^{16}\rangle)$$

*is given by*

$$D_0 = A_{00}(1+y) + A_{01}(1-y),$$

*where*

$$A_{00} = -x^7(1+x^8) + (1-x^8),$$
$$A_{01} = x(1+x^8) + x^4(1-x^8).$$

*This was easily found by hand, because the factor group $M_{64}/\langle x^{16}\rangle$ is isomorphic to the abelian group $C_{16}\times C_2$.*

*A $\{+1, 0, -1\}$-valued group ring element $D_1$ satisfying*

$$D_1(1-x^{16})D_1^{(-1)} = 16(1-x^{16}) \quad \text{in } \mathbb{Z}M_{64}$$

*is given by*

$$D_1 = A_{10}(1+y) + A_{11}(1-y),$$

*where*

$$A_{10} = (x^6 - x^5)(1-x^8),$$
$$A_{11} = (x^2 + x^3)(1+x^8).$$

*This was found by hand using the irreducible representations induced by the character (homomorphism) that maps $x^{16}$ to $-1$.*

*Now $D_0(1+x^{16})$ has support $(1+x+x^4+x^7)\langle x^8, y\rangle$, and $D_1(1-x^{16})$ has support $(x^2+x^3+x^5+x^6)\langle x^8, y\rangle$. These supports are disjoint and their union is $M_{64}$. We conclude from the construction of Proposition 4.8 that $D = D_0(1+x^{16}) + D_1(1-x^{16})$ corresponds to a difference set in $M_{64}$.*

**Example 4.10** (Yolland construction for SmallGroup(256, 536) [38])**.** *We apply Proposition 4.8 to construct a Hadamard difference set in $G = C_{64} \rtimes_{47} C_4 = \langle x, y : x^{64} = y^4 = 1, yxy^{-1} = x^{47}\rangle$. The center of $G$ is $\langle x^{32}\rangle$, so $x^{32}$ is a central involution.*

*A $\{+1, 0, -1\}$-valued group ring element $D_0$ satisfying*

$$\natural(D_0)\natural(D_0)^{(-1)} = 64 \quad \text{in } \mathbb{Z}(G/\langle x^{32}\rangle)$$

*is given by*

$$D_0 = A_{00}(1+y^2) + A_{01}(1-y^2),$$

*where*

$$A_{00} = \big((1-x^8) - x^2(1+x^8)\big)(1+x^{16}) + (x^5 + x^6 y)(1+x^8)(1-x^{16}),$$
$$A_{01} = \big((1-x^8) - x^5(1+x^8)\big)y(1+x^{16}) + \big(-x^3(1-x^8)y + x^3(1+x^8)\big)(1-x^{16}).$$

*This was found by hand by seeking a perfect ternary array of weight 64 in the nonabelian factor group $G/\langle x^{32}\rangle \cong C_{32} \rtimes_{15} C_4$.*

*A $\{+1,0,-1\}$-valued group ring element $D_1$ satisfying*

$$D_1(1-x^{32})D_1^{(-1)} = 64(1-x^{32}) \quad \textit{in } \mathbb{Z}G$$

*is given by*

$$D_1 = A_{10}(1+y^2) + A_{11}(1-y^2),$$

*where*

$$\begin{aligned} A_{10} &= -\big((x+x^4+x^9+x^{12}+x^{14})(1+x^{16}) + (x^6+x^7-x^{15})(1-x^{16})\big), \\ A_{11} &= -\big((x-x^9+x^{10})(1+x^{16}) + (x^2+x^4-x^7+x^{12}-x^{15})(1-x^{16})\big)y. \end{aligned}$$

*This was found by a difficult computer search. Although a naive search for $D_1$ involves a search space of size $2^{64}$, the search was shortened by using the irreducible representations induced by the character (homomorphism) that maps $x^{32}$ to $-1$, and by making some simplifying assumptions about the structure of the target difference set [38].*

*Now $D_0(1+x^{32})$ has support $\big(1+x^2+x^3+x^5+(1+x^3+x^5+x^6)y\big)\langle x^8, y^2\rangle$, and $D_1(1-x^{32})$ has support $\big(x+x^4+x^6+x^7+(x+x^2+x^4+x^7)y\big)\langle x^8, y^2\rangle$. These supports are disjoint and their union is $G$. We conclude from the construction of Proposition 4.8 that $D = D_0(1+x^{32}) + D_1(1-x^{32})$ corresponds to a difference set in $G$.*

We now reinterpret Examples 4.9 and 4.10 as arising from a modification of a signature set.

**Lemma 4.11.** *Let $G$ be a group containing a normal subgroup $E \cong C_2^r$, and let $\{\chi_u : u \in U_r\}$ be the set of characters of $E$. Let $A_u$ be a $\{+1,0,-1\}$-valued function on $G$ for each $u \in U_r$, where the $A_u$ have disjoint supports whose union is a set of coset representatives for $E_r$ in $G$. Suppose that*

$$\sum_{u \in U_r} A_u \chi_u A_u^{(-1)} = \frac{|G|}{2^r} \quad \textit{in } \mathbb{Z}G. \tag{31}$$

*Then $G \in \mathcal{H}$.*

*Proof.* Let

$$D = \sum_{u \in U_r} A_u \chi_u \quad \text{in } \mathbb{Z}G,$$

which by the assumption on the supports of the $A_u$ is a $\{\pm 1\}$-valued function on $G$. We calculate $DD^{(-1)} = |G|$ using Proposition 1.7 ($i$), and so $D$ corresponds to a Hadamard difference set in $G$. □

By Proposition 1.7 ($ii$), one way to achieve (31) in Lemma 4.11 would be for the $A_u$ to satisfy the condition in $\mathbb{Z}G$ that

$$A_u \chi_u A_u^{(-1)} = \tfrac{|G|}{2^{2r}} \chi_u \quad \text{for each } u \in U_r. \tag{32}$$

Such a set of $A_u$ would be similar, but not identical, to a signature set on $G$ with respect to $E$: the conditions on the supports in Lemma 4.11 are different from those in Definition 2.1, and the constant in (32) is $\frac{|G|}{2^{2r}}$ rather than $\frac{|G|}{2^r}$.

A crucial observation in reinterpreting Examples 4.9 and 4.10 is that a weaker condition than (32) suffices. In particular, in the case $r=2$, this condition can be weakened to

$$A_{0j}\chi_{0j}A_{0j}^{(-1)} = \tfrac{|G|}{16}\chi_{0j} \quad \text{for each } j \in \{0,1\}, \tag{33}$$

$$A_{10}\chi_{10}A_{10}^{(-1)} + A_{11}\chi_{11}A_{11}^{(-1)} = \tfrac{|G|}{16}(\chi_{10}+\chi_{11}), \tag{34}$$

in which the expressions $A_{10}\chi_{10}A_{10}^{(-1)}$ and $A_{11}\chi_{11}A_{11}^{(-1)}$ behave like a "complementary pair" whose sum is the same as if (32) held.

In Example 4.9, the group $M_{64}$ contains the normal subgroup $E_2 = \langle x^{16}, y\rangle \cong C_2^2$ whose characters are

$$\chi_{ij} = \big(1+(-1)^i x^{16}\big)\big(1+(-1)^j y\big) \quad \text{for } (i,j) \in U_2.$$

The difference set $D$ takes the form

$$D = D_0(1+x^{16}) + D_1(1-x^{16}) = \sum_{(i,j)\in U_2} A_{ij}\chi_{ij}$$

where the $A_{ij}$ take the values specified in the example. These $A_{ij}$ satisfy the conditions of Lemma 4.11 on their supports. Since conjugation by $x$ fixes $\chi_{00}$ and $\chi_{01}$ but swaps $\chi_{10}$ and $\chi_{11}$, we find by direct calculation that

$$A_{0j}\chi_{0j}A_{0j}^{(-1)} = 4\chi_{0j} \quad \text{for each } j \in \{0,1\}$$

and

$$\begin{aligned} A_{10}\chi_{10}A_{10}^{(-1)} &+ A_{11}\chi_{11}A_{11}^{(-1)} \\ &= \Big(2(1-x^{-1})\chi_{10} + 2(1-x)\chi_{11}\Big) + \Big(2(1+x^{-1})\chi_{10} + 2(1+x)\chi_{11}\Big) \\ &= 4(\chi_{10}+\chi_{11}), \end{aligned}$$

so that (33) and (34) hold.

The reinterpretation of Example 4.10 is similar. SmallGroup$(256, 536)$ contains the normal subgroup $E_2 = \langle x^{32}, y^2\rangle \cong C_2^2$, whose characters are

$$\chi_{ij} = \big(1+(-1)^i x^{32}\big)\big(1+(-1)^j y^2\big) \quad \text{for } (i,j) \in U_2.$$

The difference set $D$ takes the form

$$D = D_0(1+x^{32}) + D_1(1-x^{32}) = \sum_{(i,j)\in U_2} A_{ij}\chi_{ij},$$

where the $A_{ij}$ take the values specified in the example. These $A_{ij}$ satisfy the conditions of Lemma 4.11 on their supports. Conjugation by $x$ fixes $\chi_{00}$ and $\chi_{01}$ but swaps $\chi_{10}$ and $\chi_{11}$, and we find once again (after a long calculation) that (33) and (34) hold.

## 4.5 Combination of Signature Sets and Perfect Ternary Arrays

The nonabelian signature set approach of Section 4.1 and the perfect ternary array product construction of Section 4.2 are closely related. For example, Proposition 4.2 may be interpreted as constructing a signature set on $H \times E_1$ from a perfect ternary array $D$ in $H$. We now illustrate how a perfect ternary array in a factor group can be used to create a signature block with respect to a specific character. We believe the illustrated method could be useful in future studies of the existence pattern for Hadamard difference sets in 2-groups of order greater than 256.

**Lemma 4.12.** *Let $K$ be a group containing a central subgroup $E \cong C_2^r$, and let $\chi$ be a character of $E$. Suppose that $\chi = H\chi'$ in $\mathbb{Z}E$ for some subgroup $H$ of $E$. Let $\natural$ be the natural map from $K$ onto $K/H$, and suppose that $A$ is a $\{+1, 0, -1\}$-valued function on $K$ for which $\natural(A)$ is a perfect ternary array of weight $2^{2j}$ in $K/H$. Then*

$$A\chi A^{(-1)} = 2^{2j}\chi \quad \textit{in } \mathbb{Z}K.$$

*Proof.* Since $\natural(A)$ is a perfect ternary array of weight $2^{2j}$ in $K/H$, in $\mathbb{Z}(K/H)$ we have by Lemma 4.5 that

$$2^{2j}1_{K/H} = \natural(A)\natural(A)^{(-1)} = (AH)(A^{(-1)}H) = AA^{(-1)}H.$$

For $k \in K$, interpret the element $kH$ in $K/H$ as $|H|$ elements in $K$, so that in the group ring $\mathbb{Z}K$ the above equation becomes

$$2^{2j}H = AA^{(-1)}H.$$

By assumption we have $\chi = H\chi'$, and $H$ and $\chi'$ are central in $K$ because $E$ is. Therefore in $\mathbb{Z}K$ we have

$$A\chi A^{(-1)} = AH\chi' A^{(-1)} = AA^{(-1)}H\chi' = 2^{2j}H\chi' = 2^{2j}\chi.$$

□

In Lemma 4.12, note that the group ring condition $\chi = H\chi'$ is equivalent to $H \in \mathrm{Ker}(\chi)$ when the character $\chi$ is considered as a homomorphism of $E$. Also note that if $E$ has index $2^{2j}$ in $K$, and $A$ is $\{\pm 1\}$-valued on a set of coset representatives for $E$ in $K$, then the conclusion of Lemma 4.12 is that $A$ is a signature block on $K$ with respect to $\chi$.

We now use Lemma 4.12 to explain the origin of the signature set introduced in Example 1.13.

**Example 4.13.** *Let $K = \langle X, Y\rangle \cong C_4^2$ and $E = \langle X^2, Y^2\rangle \cong C_2^2$, and let $\{\chi_u : u \in U_2\}$ be the set of characters of $E$. We use Lemma 4.12 to construct the signature set*

$$A_{00} = A_{01} = A_{10} = 1 + X + Y - XY \quad \text{and} \quad A_{11} = 1 + X + Y + XY$$

*on $K$ that was presented in Example 1.13 without explanation of its origin.*

*For $\chi = \chi_{00}$ or $\chi_{10}$, take $H = \langle Y^2\rangle$ and $A = 1 - X - Y - XY$. Then $\natural(A)$ is a perfect ternary array of weight 4 in $K/H$ by Example 4.6 (i), because $\natural(Y)$ is an involution that commutes with the nonidentity element $\natural(X)$. Lemma 4.12 then shows that $A$ is a signature block on $K$ with respect to $\chi_{00}$ and $\chi_{10}$. Since $A_{00}\chi_{00} = -XYA\chi_{00}$ and $A_{10}\chi_{10} = XA\chi_{10}$ in $\mathbb{Z}K$, it follows from Definition 2.1 and Proposition 1.7 (i) that $A_{00} = A_{10}$ is a signature block on $K$ with respect to both $\chi_{00}$ and $\chi_{10}$. By symmetry in $X$ and $Y$, it follows that $A_{01}$ is also a signature block on $K$ with respect to $\chi_{01}$.*

*For $\chi = \chi_{11}$, take $H = \langle X^2Y^2\rangle$ and $A = 1 + X + XY - X^2Y$. Then $\natural(A)$ is a perfect ternary array of weight 4 in $K/H$ by Example 4.6 (i), because $\natural(XY)$ is an involution that commutes with the nonidentity element $\natural(X)$. By Lemma 4.12 and the relation $A_{11}\chi_{11} = A\chi_{11}$ in $\mathbb{Z}K$, we conclude that $A_{11}$ is a signature block on $K$ with respect to $\chi_{11}$.*

# 5 Computer Implementation for Groups of Order 256

In this section, we provide further details of the streamlined procedure used to establish that each of the 56,049 groups of order 256 not excluded by Theorems 1.3 and 1.5 belongs to $\mathcal{H}$. We then describe online databases containing difference sets found by this procedure, and explain how the overall result can be quickly verified on a desktop computer using the accepted GAP package *DifSets* [31, 32]. We note that *DifSets* provides (via the LoadDifferenceSets command) a listing of all inequivalent difference sets in groups of order 16 and 64.

## 5.1 Procedure

As previously summarized in Section 1, the streamlined procedure for groups of order 256 comprises three stages:

**Stage 1.** Use Theorem 1.15 to account for the 54,633 groups containing a normal subgroup isomorphic to $C_2^4$ or $C_4^2 \times C_2$ or $C_8^2$.

**Stage 2.** Use the product construction of Proposition 4.7 to account for $1,358$ further groups.

**Stage 3.** Apply the transfer methods of Section 4.3 to account for 57 further groups, and the modified signature set method of Section 4.4 to account for the final group. We do not describe this stage further.

The relationship between the groups handled by Stages 1 and 2 is shown in Fig. 1.

In Stage 1, we wish to construct a difference set in a group $G$ of order 256 containing a normal abelian subgroup $K$, where $K$ is isomorphic to $C_2^4$ or $C_4^2 \times C_2$ or $C_8^2$. A signature set on $K$ is provided trivially for the case $C_2^4$ (see the remark following Definition 2.1), by Example 3.4 for the case $C_4^2 \times C_2$, and by Example 3.3 for the case $C_8^2$. We then apply the method in the proof of Theorem 2.3 to construct a difference set in $G$. This requires a set $\{g_u : u \in U_r\}$ of coset representatives for $K$ in $G$ satisfying (13), namely

$$\{g_u \chi_u g_u^{-1} : u \in U_r\} = \{\chi_u : u \in U_r\}.$$

The existence of such a set is guaranteed by Theorem 1.9, but the proof of this result in [18] is non-constructive. We therefore conduct a search for a suitable set of coset representatives $\{g_u\}$. This search is exhaustive for the cases $C_4^2 \times C_2$ and $C_8^2$, but random for the case $C_2^4$ whose search space has size $15! > 10^{12}$.

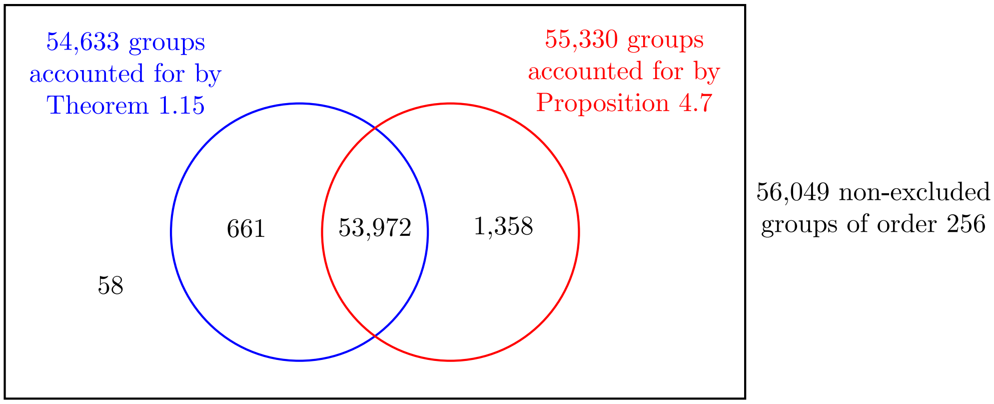


Figure 1: Theorem 1.15 and Proposition 4.7 show that at most 58 of the 56,049 non-excluded groups of order 256 lie outside $\mathcal{H}$.

The results of applying this search procedure to all 56,049 non-excluded groups, for each of the three choices of $K$ independently, are shown in Fig. 2.

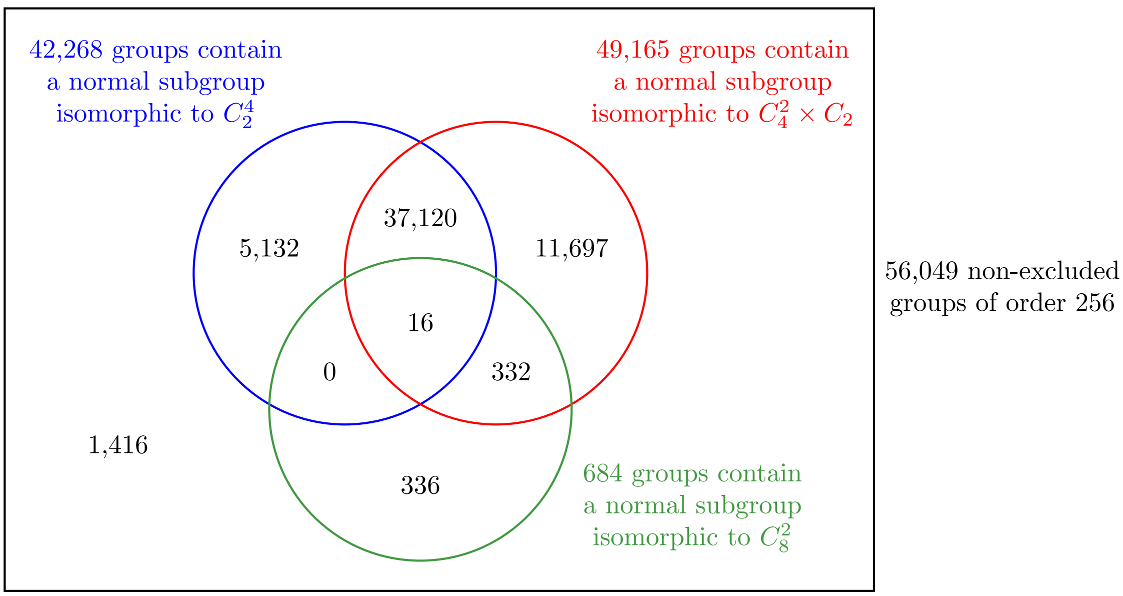


Figure 2: Theorem 1.15 shows that at most 1,416 of the 56,049 non-excluded groups of order 256 lie outside $\mathcal{H}$.

In Stage 2, we distinguish six instances of the product construction of Proposition 4.7 according to the form of its input perfect ternary arrays $T_1, T_2, \ldots, T_s$.

(*i*) $\mathbf{H_{64} \cdot Q_4}$ **form**. Take $T_1$ to be a Hadamard difference set in a subgroup $H_1$ of $G$ of order 64, and $T_2$ to be a perfect ternary array of weight 4 in $G$ having the form of Example 4.6 (*ii*) where the quaternion group $Q = \langle x, y \rangle$ of order 8 intersects $H_1$ in the two-element subgroup $\{1, x^2\}$.

(*ii*) $\mathbf{H_{64} \cdot H_4}$ **form**. Take $T_1$ to be a Hadamard difference set in a subgroup $H_1$ of $G$ of order 64, and $T_2$ to be a Hadamard difference set in a subgroup $H_2$ of $G$ of order 4, where $G = H_1H_2$ and $H_1 \cap H_2 = 1$.

(*iii*) $\mathbf{H_{16} \cdot H_{16}}$ **form**. For $i = 1, 2$, take $T_i$ to be a Hadamard difference set in a subgroup $H_i$ of $G$ of order 16, where $G = H_1H_2$ and $H_1 \cap H_2 = 1$.

(*iv*) $\mathbf{H_{64} \cdot T_1}$ **form**. Take $T_1$ to be a perfect ternary array of weight 4 in $G$ having the form of Example 4.6 (*i*), and $T_2$ to be a Hadamard difference set in a subgroup of $G$ of order 64.

(*v*) $\mathbf{H_{16} \cdot T_1 \cdot T_2}$ **form**. Take each of $T_1, T_2$ to be a perfect ternary array of weight 4 in $G$ having either of the two forms of Example 4.6, and $T_3$ to be a Hadamard difference set in a subgroup of $G$ of order 16.

(*vi*) $\mathbf{T_1 \cdot T_2 \cdot T_3 \cdot T_4}$ **form**. Take each of $T_1, T_2, T_3, T_4$ to be a perfect ternary array of weight 4 in $G$ having either of the two forms of Example 4.6.

For each of these six forms, we conduct a search for a suitable set of perfect ternary arrays satisfying all the required conditions. The search for the forms (*i*) to (*iii*) is relatively fast because the search is restricted to subgroups of the appropriate order. However, the search for the forms (*iv*) to (*vi*) is not constrained in this way and can take considerably longer; the search for form (*vi*) sometimes requires more than a day for a single group.

We therefore begin by searching all $56,049$ non-excluded groups for each of the forms (*i*) to (*iii*) independently, with results as shown in Fig. 2. We then conduct a search for each of the forms (*iv*) to (*vi*) in that order, but only over those groups in which no previous form has been found. The number of groups accounted for and remaining at each step of Stage 2 is shown below.

| | $H_{64} \cdot Q_4$ and $H_{64} \cdot H_4$ and $H_{16} \cdot H_{16}$ | $H_{64} \cdot T_1$ | $H_{16} \cdot T_1 \cdot T_2$ | $T_1 \cdot T_2 \cdot T_3 \cdot T_4$ |
|---|---|---|---|---|
| # groups accounted for | 51,957 | 3,119 | 236 | 18 |
| # groups remaining | 4,092 | 973 | 737 | 719 |

The Stage 2 searches are exhaustive in that none of the remaining 719 groups contains a difference set having one of the six forms (*i*) to (*vi*).

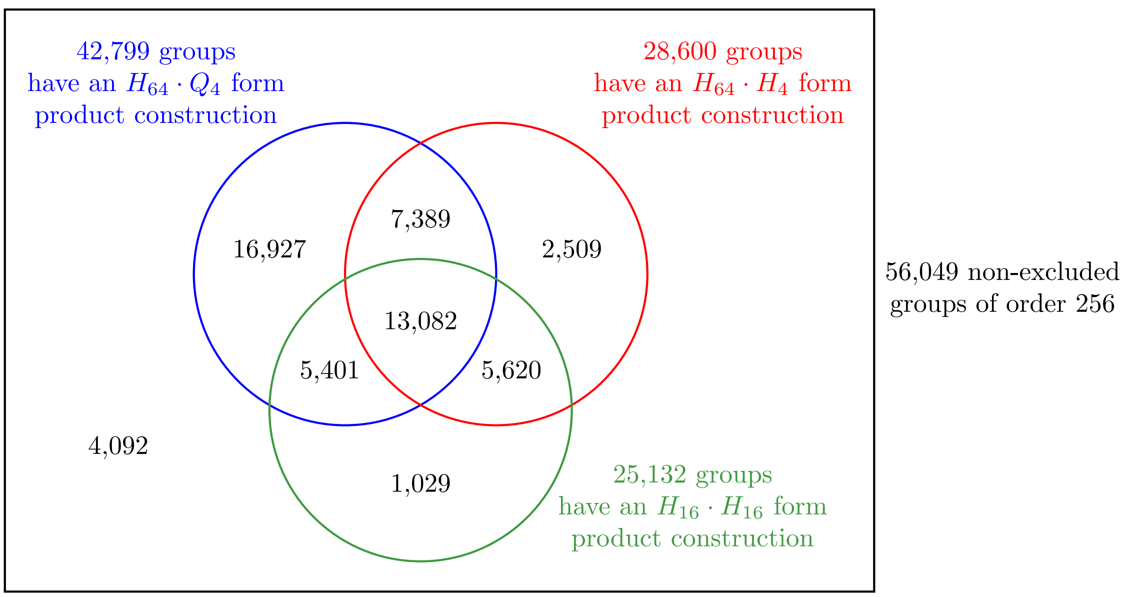


Figure 3: Forms $H_{64} \cdot Q_4$ and $H_{64} \cdot H_4$ and $H_{16} \cdot H_{16}$ of Proposition 4.7 show that at most 4,092 of the 56,049 non-excluded groups of order 256 lie outside $\mathcal{H}$.

## 5.2 Databases and Verification

The website [34] contains ten lists in GAP format, organized into four databases as shown in Table 2.

Lists $L_1$ to $L_3$ correspond to the three circles in Fig. 2 (Stage 1). Lists $L_4$ to $L_6$ correspond to the three circles in Fig. 3 (forms (*i*) to (*iii*) of Stage 2). Lists $L_7$ to $L_9$ correspond to forms (*iv*) to (*vi*) of Stage 2. Each entry of the lists $L_1$ to $L_9$ contains at least two fields: a catalogue number $i$ that identifies the group SmallGroup$(256, i)$, and a list of 120 indices taken from $\{1, 2, \ldots, 256\}$ in which index $j$ labels group element $j$ according to the GAP ordering given by Elements(SmallGroup$(256, i)$).

| List | List name | Database name |
|---|---|---|
| $L_1$ | HDS256_Normal_02x02x02x02 | |
| $L_2$ | HDS256_Normal_04x04x02 | HDS256_NormalSubgroupTransversal.txt |
| $L_3$ | HDS256_Normal_08x08 | |
| $L_4$ | HDS256_H64byQ4 | |
| $L_5$ | HDS256_H64byH4 | HDS256_PTAProduct.txt |
| $L_6$ | HDS256_H16byH16 | |
| $L_7$ | HDS256_H64byT1 | |
| $L_8$ | HDS256_H16byT1byT2 | HDS256_SubgroupProduct.txt |
| $L_9$ | HDS256_T1byT2byT3byT4 | |
| $L_{10}$ | HDS256 | HDS256.txt |

Table 2: Organization of difference set databases in [34].

The list $L_{10}$ contains one entry for each of the 56,092 groups of order 256. If SmallGroup$(256, i)$ is one of the 43 groups excluded by Theorems 1.3 and 1.5 (see Table 1), then entry $i$ of $L_{10}$ is an emtpy list of indices. Otherwise, this entry is a list of 120 indices corresponding to a representative difference set in SmallGroup$(256, i)$. The representative difference set is taken from list $L_1$ if possible, otherwise from $L_2$, and so on to $L_9$. This accounts for the origin of all but 58 of the non-empty entries of $L_{10}$.

After reading the list HDS256 into the current directory, the following GAP code uses Peifer's accepted GAP package *DifSets* [32] to verify that HDS256 contains an index list corresponding to a difference set for 56,049 groups of the 56,092 groups of order 256, and an empty index list for the remaining 43 groups.

```
LoadPackage("DifSets");
empty := 0;
count := 0;
for i in [1..Length(HDS256)] do;
  if HDS256[i] = [] then
    empty := empty+1;
  else
    if IsDifferenceSet(SmallGroup(256,i), HDS256[i]) then
      count := count+1;
    fi;
  fi;
od;
Print("HDS256 contains ", Length(HDS256), " index lists, of which\n");
Print(count, " correspond to a difference set and ", empty, " are empty\n");
```

It took less than 20 minutes to run this code on a 2013 iMac desktop computer using a standard implementation of GAP, producing the following output.

```
HDS256 contains 56092 index lists, of which
56049 correspond to a difference set and 43 are empty
```

Although we found it considerably more difficult to construct a difference set in some groups of order 256 than in others, there is no significant variation in verification time among groups of a given order using the IsDifferenceSet command of *DifSets*.

# 6 Future Directions

In this section, we propose directions for future research into Hadamard difference sets and their relations to other combinatorial objects.

We have described in this paper a streamlined procedure for demonstrating that all groups of order 64 and 256, apart from those that are excluded by the classical nonexistence results of Theorems 1.3 and 1.5, belong to the class $\mathcal{H}$ of Hadamard difference sets. While we consider this to be a major achievement in combinatorics, it is unsatisfactory that we do not yet have a completely theoretical demonstration.

We now propose the following directions for future research into Hadamard difference sets, with three overall objectives in mind. The first objective is to simplify and unify the various techniques of Section 4, removing the reliance on extensive computer search and the non-systematic transfer methods. The second objective is to develop recursive or direct construction techniques for nonabelian groups, that are as powerful as Theorem 3.1 is for constructing signature sets on abelian groups. The third and ultimate objective is to resolve Question 1.17.

D1. The concept of signature sets on abelian groups (Theorem 3.1) and on nonabelian groups (Section 4.1) appears to be very powerful. Develop construction methods to determine all nonabelian groups on which there is a signature set relative to a normal elementary abelian subgroup.

D2. Apply Lemma 4.12 to create signature sets in nonabelian groups, generalizing the model of Example 4.13.

D3. Understand when and why the transfer methods of Section 4.3 succeed.

D4. Develop a general theory based on the method of Section 4.4 so that transfer methods are no longer needed for groups of order 64 and 256.

D5. Representation theory was used to help find the group ring element $D_1$ in Examples 4.9 and 4.10. Apply representation theory to unify and extend the construction methods of Section 4.

D6. In the study of bent functions, which are equivalent to Hadamard difference sets in elementary abelian 2-groups, one asks how many inequivalent examples exist in a given group. Determine how many inequivalent Hadamard difference sets in (not necessarily elementary abelian) 2-groups can be constructed using the methods of this paper.

D7. Formulate a theoretical framework that can be systematically applied to determine all 2-groups belonging to $\mathcal{H}$.

D8. Extend the transfer methods of Section 4.3 to construct Hadamard difference sets in new groups whose order is not a power of 2, for example in groups of order 100 [20], 144 [36], or 400 [26].

We also propose some further research directions involving the relation of Hadamard difference sets to other combinatorial objects.

D9. Difference sets in the Hadamard, McFarland, Spence, and Chen-Davis-Jedwab families have parameters $(v, k, \lambda)$ satisfying $\gcd(v, k - \lambda) > 1$, and are known to share construction methods based on covering extended building sets and semi-regular relative difference sets [12, 9]. Adapt the signature set approach for Hadamard difference sets in order to construct difference sets in nonabelian groups for the other three families, and the associated semi-regular relative difference sets in nonabelian groups for all four families.

D10. Determine how many inequivalent designs arise from the Hadamard difference sets constructed in this paper.

D11. Determine how many inequivalent binary codes arise from the incidence matrices of the Hadamard difference sets constructed in this paper.

## References


[1] T. Applebaum, Difference Sets in Non-Abelian 2-Groups, Honors Thesis, University of Richmond, 2013.

[2] K.T. Arasu and J.F. Dillon, Perfect ternary arrays, eds. A.Pott and others, 1–15, *Difference Sets, Sequences and their Correlation Properties*, NATO Science Series C vol. 542, Kluwer, Dordrecht, 1999.

[3] H.U. Besche, B. Eick, and E.A. O'Brien, A Millenium Project: Constructing small groups, *Int. J. Algebra Comput.* vol. 12, 623–644, 2002.

[4] T. Beth, D. Jungnickel, and H. Lenz, Design Theory, 2nd edition, Cambridge University Press, Cambridge, 1999.

[5] C. Bhattacharya and K.W. Smith, Factoring $(16, 6, 2)$ Hadamard Difference Sets, *Electron. J. Combin.* vol. 15, 2008.

[6] R.H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.* vol. 78, 464–481, 1955.

[7] D. Burrell, On the number of groups of order 1024, *Commun. Algebra*, DOI: 10.1080/00927872.2021.2006680, 2021.

[8] C. Carlet and S. Mesnager, Four decades of research on bent functions, *Des. Codes Cryptog.* vol. 78, 5–50, 2016.

[9] Y.Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Appl.*, vol. 3, 234–256, 1997.

[10] J.A. Davis, Difference sets in abelian 2-groups, *J. Comb. Theory A* vol. 57, 262–286, 1991.

[11] J.A. Davis and J. Jedwab, A survey of Hadamard difference sets, eds. K.T. Arasu and others, 145–156, *Groups, Difference Sets and the Monster*, de Gruyter, Berlin-New York, 1996.

[12] J.A. Davis and J. Jedwab, A unifying construction for difference sets, *J. Comb. Theory A* vol. 80, 13–78, 1997.

[13] J.A. Davis and K. Smith, A construction of difference sets in high exponent 2-groups using representation theory, *J. Algebraic Comb.* vol. 3, 137–151, 1994.

[14] J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Comb. Theory A* vol. 40, 9–21, 1985.

[15] J.F. Dillon, A survey of difference sets in 2-groups (subtitle: Hadamard groups of order 64). Presented at Marshall Hall Conference, University of Vermont, 1990.

[16] J.F. Dillon, Difference sets in 2-groups, *Contemp. Math.* vol. 111, 65–72, 1990.

[17] J.F. Dillon, Some REALLY beautiful Hadamard matrices, *Cryptogr. Commun.* vol. 2, 271–292, 2010.

[18] A.A. Drisko, Transversals in row-Latin rectangles, *J. Comb. Theory A* vol. 84, 181–195, 1998.

[19] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.11.0, 2020. `https://www.gap-system.org`

[20] A. Golemac and T. Vučičić, New difference sets in nonabelian groups of order 100, *J. Comb. Des.* vol. 9, 424–434, 2001.

[21] J. Jedwab, Generalized perfect arrays and Menon difference sets, *Des. Codes Cryptogr.* vol. 2, 19–68, 1992.

[22] D. Jungnickel and B. Schmidt, Difference sets: a second update, *Rend. Circ. Mat. Palermo (2) Suppl.* vol. 53, 89–118, 1998.

[23] P. Kesava Menon, On difference sets whose parameters satisfy a certain relation, *Proc. Amer. Math. Soc.* vol. 13, 739–745, 1962.

[24] R. Kibler, A summary of noncyclic difference sets, $k < 20$, *J. Comb. Theory A* vol. 25, 62–67, 1978.

[25] R. Kraemer, Proof of a conjecture on Hadamard 2-groups, *J. Comb. Theory A* vol. 63, 1–10, 1993.

[26] J. Mandić and T. Vučičić, On the existence of Hadamard difference sets in groups of order 400, *Adv. Math. Commun.* vol. 10, 547–554, 2016.

[27] R.A. Liebler and K.W. Smith, On difference sets in certain 2-groups, *Coding Theory, Design Theory, Group Theory*, eds. D. Jungnickel, S. Vanstone, 195–212, Wiley, NY, 1993.

[28] H.B. Mann, Addition Theorems, Interscience, NY, 1965.

[29] R.L. McFarland, A family of difference sets in non-cyclic groups, *J. Comb. Theory A* vol. 15, 1–10, 1973.

[30] Number of groups of order $2^n$, *The On-Line Encyclopedia of Integer Sequences*, https://oeis.org/A000679.

[31] D. Peifer, An algorithm for enumerating difference sets, *Journal of Software for Algebra and Geometry* vol. 9, 35–41, 2019.

[32] D. Peifer, GAP package DifSets: an algorithm for enumerating all difference sets in a group, Version 2.3.1, 2019. Available online: `https://www.gap-system.org/Packages/difsets.html`

[33] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* vol. 43, 377–385, 1938.

[34] K. Smith, Difference Set Databases, 2022. Available online: `https://drive.google.com/drive/folders/1qEkc-4ZONlVIawnSoarWtqUYSpMkxOPB`

[35] R. Turyn, Character sums and difference sets, *Pac. J. Math.* vol. 15, 319–346, 1965.

[36] T. Vučičić, Hadamard difference sets and related combinatorial objects in groups of order 144, *Rad Hazu. Matematičke Znanosti* vol. 23 = 538, 13–29, 2019.

[37] E.G. Whitehead, Difference sets and sum-free sets in groups of order 16, *Discrete Math.* vol. 13, 399–407, 1975.

[38] W. Yolland, Existence of a difference set in the last group of order 256, Summer Research Report, Simon Fraser University, 2016.