Proof of a Conjecture on Hadamard 2-Groups

ROBERT G. KRAEMER

Department of Defense, Fort George G. Meade, Maryland 20755-6000

Communicated by the Managing Editors

Received February 1, 1989

By expanding on the results of James Davis, we prove by construction that every abelian 2-group that meets the exponent bound has a difference set. © 1993 Academic Press, Inc.

1. INTRODUCTION

Let $G$ be an arbitrary finite group of order $v$. A subset $D \subseteq G$ of size $k$ is called a $(v, k, \lambda)$-difference set if every nonidentity element in $G$ can be expressed in exactly $\lambda$ ways as a “difference,” $d_1 d_2^{-1}, d_1, d_2 \in D$.

Let $G$ be an abelian 2-group. It is known from earlier work [6] that if $G$ is to admit a nontrivial difference set, then the parameters $(v, k, \lambda)$ can be assumed to be $(2^{2d+2}, 2^{2d+1}-2^d, 2^{2d}-2^d)$ for some $d$. We also know [7] that the exponent of $G$, i.e., the smallest positive number $m$ such that $g^m = 1$ for all $g \in G$, cannot be greater than $2^d + 2$. It is the purpose of this paper to show that the exponent bound is not only necessary, but also sufficient for $G$ to admit a nontrivial difference set.

We begin with a review of some properties of characters on abelian 2-groups. A mapping, $\chi$, from $G$ into the complex numbers is called a character on $G$ if $\chi(gh) = \chi(g) \chi(h)$ for all $g, h \in G$. It is clear that $\chi$ must take every element of $G$ into a $2^m$th root of unity, where $2^m$ is the exponent of $G$. For any abelian group there is always the trivial character which sends every element to 1. Such a mapping is called a principal character. In [5] the following basic result is shown:

**Lemma 1.** For any abelian group $G$, the characters of $G$ form a group isomorphic to $G$.

Now suppose that $D \subseteq G$ and $|D| = 2^{2d+1} - 2^d$. Then we have

**Lemma 2.** $D$ is a difference set with parameters $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$, if and only if for every nonprincipal character $\chi$, $|\sum_{d \in D} \chi(d)| = 2^d$.  

1
Let $H$ be any subgroup of $G$ of order $2^{d+1}$. We define an equivalence relation on the character group of $G$ as

$$
\chi \equiv \chi' \text{ if and only if } \ker(\chi) \cap H = \ker(\chi') \cap H.
$$

The equivalence class associated to $\chi$ is denoted $[\chi]$. In particular, the equivalence class associated to the principal character $\chi_0$ is denoted $[\chi_0]$. The following lemma due to Davis characterizes the equivalence class $[\chi]$.

**Lemma 3 (Davis).** $[\chi] = \{\chi^a \gamma | a \text{ is odd and } \gamma \text{ is principal on } H\}$. Furthermore, if $\chi'$ is principal on $\ker(\chi) \cap H$ but not in $[\chi]$, then $\chi' = \chi^{2a} \gamma$, for some $a$ and some $\gamma$ principal on $H$.

**Proof.** Suppose $\chi' = \chi^a \gamma$, where $a$ is odd and $\gamma$ is principal on $H$. Let $h \in H$ be such that $\chi(h) = 1$. Then clearly $\chi'(h) = 1$. Suppose that $\chi'(h) = 1$, then $\chi^a(h) = (\chi(h))^a = 1$. But since $G$ is an abelian 2-group, there exists a unique minimal $k$ so that $\chi(h)^{2k} = 1$. Hence $2k | a$. But $a$ is odd; therefore $k$ must be 0, and so $\chi(h) = 1$. Therefore $\chi \equiv \chi'$.

Now suppose that $\chi' \equiv \chi$. Let $K$ be the $\ker(\chi) \cap H$. It is a trivial consequence of the isomorphism theorems for groups that $H \backslash K$ is cyclic, say, generated by $hK$. Since $\chi \equiv \chi'$, $\chi'$ is uniquely determined on $H$ by where it sends $h$. Let the order of $\chi$ on $H$ (and hence $\chi'$ on $H$) be $2^k$. Then $\chi(h)$ is a primitive $2^k$th root of unity, say $\omega$. $\chi(h)$ must also be a primitive $2^k$th root of unity, else $\chi' \not\equiv \chi$. Hence $\chi'(h) = \omega^a$ for some odd $a$, which implies that on $H$, $\chi' = \chi^a$. Hence there exists a $\gamma$ principal on $H$ so that $\chi' = \chi^a \gamma$ on $G$.

Now suppose that $\chi'$ is a character which is principal on $K$, but not in $[\chi]$. As before, $\chi'$ is uniquely determined by where it sends $h$. Hence if $\chi(h) = \omega$ is a primitive $2^j$th root of unity, then since $\chi'$ is principal on $K$, $\chi'(h)$ is a $2^j$th root of unity for some $j < k$. But if $j = k$ then by the above $\chi' \in [\chi]$. Hence $j < k$, which implies that there is some even number $2a$ so that $\chi'(h) = \omega^{2a}$. Therefore on $H$ we have $\chi' = \chi^{2a}$, which implies that there is a $\gamma$ principal on $H$ so that $\chi' = \chi^{2a} \gamma$ on $G$.

2. The $K$-Matrix

In the following sections we demonstrate how to construct a difference set in any abelian 2-group that meets the exponent bound. To do this we use a property of the group called a $K$-matrix structure, which was developed by James Davis and shown to exist in any abelian 2-group meeting the exponent bound of rank 2.

Let $[\chi_0], [\chi_1], \ldots, [\chi_{Q}]$ be a list of the distinct equivalence classes of the group characters of $G$. For each $[\chi_i], i \neq 0$, let $K_i = \ker(\chi_i) \cap H$. Let $h_i$ be
an element of \(H \backslash K\) and let \(y_t\) and \(z_t\) be elements of \(G \backslash H\). We associate to 
\([\chi_t]\) the \(2^s \times 2^s\) matrix \(M_t = (m_{i,j})\), where \(2^{s+1}\) is the order of \(\chi_t\) restricted to \(H\), whose entries are in \(G\) and given by

\[ m_{i,j} = y_t z_t h_t^{-(2i+1)} j, \quad 0 \leq i, j \leq 2^s - 1. \]

**Definition.** The group \(G\) is said to possess a \(K\)-matrix structure if and only if the following three properties hold:

1. If \(\chi\) is principal on \(K\), but \(\chi \notin [\chi_t]\) or \([\chi_0]\), then the sum of the values of \(\chi\) on any column of \(M_t\) is 0.
2. If \(\chi \in [\chi_t]\), then the sum of the values of \(\chi\) on any row of \(M_t\) is 0, except for one row, called \(i_0\), which depends on \(\chi\), where the sum has magnitude \(2^s = \frac{1}{2}\) the order of \(\chi\), restricted to \(H\).
3. The set \(\{y_t z_t^j\}\), \(0 \leq j \leq \frac{1}{2}|\chi_t|_H - 1\), \(1 \leq t \leq Q\), together with the identity, constitutes a complete set of distinct coset representatives of \(H\) in \(G\).

In Davis' thesis \([1]\) the following theorem is proved:

**Theorem 1 (Davis).** Any abelian 2-group that possesses a \(K\)-matrix structure has a difference set.

In fact the difference set is easily constructed. For each \([\chi_t]\), \(t \neq 0\), let \(D_t\) be the union of the cosets \(m_{i,j} K_t\), where the \(m_{i,j}\) are the entries in the associated \(K\)-matrix \(M_t\). Let \(D\) be the union of all the \(D_t\). Then \(D\) is the desired difference set in \(G\). The proof involves checking that the character sums over \(D\) always have constant magnitude, namely \(2^d\), for each nonprincipal character \(\chi\).

Since the existence of a difference set is intimately related to the existence of appropriate \(h_t\), \(y_t\), and \(z_t^j\)'s for each \(t \geq 1\), it makes sense to investigate these elements more closely.

For what follows, assume that \([\chi_t]\) is given and that the order of \(\chi_t|_H\) is \(2^{s+1}\), \(s \geq 0\), and that \(K_t = \ker(\chi_t) \cap H\).

**Lemma 4.** If \(\chi \in [\chi_t]\), then for any \(h \in H\), if \(\chi(h)\) is a primitive \(2^s\)th root of unity, so is \(\chi(h)\).

**Proof:** Without loss of generality we may assume that \(\chi(h) = \omega\) and that \(\chi(h) = \omega^2a\), where \(a\) is odd and \(\omega\) is a primitive \(2^s\)th root of unity. Then \(\chi(h^{2^s-i}) = \omega^{2^s-a} = 1\), which implies that \(\chi(h^{2^s-i}) = 1\), which implies that \(\omega\) is a \(2^s-k\)th root of unity, which implies that \(k = 0\).

**Lemma 5.** An \(h_t\) can always be found for all \(t\), \(1 \leq t \leq Q\), so that property 1 is satisfied.
Proof. Recall that $H/K_t$ is cyclic. Let $h_t K_t$ generate $H/K_t$. Let $\chi$ be a character that is principal on $K_t$ but not principal on $H$ or in $[\chi_t]$. Then we know by Lemma 3 that $\chi = \chi_t^{2a} \gamma$, where $\gamma$ is principal on $H$ and $\chi_t^{2a}$ is not principal on $H$. For a fixed column $j$, the sum of the values of $\chi$ on the $j$th column of $M_t$ is

$$\chi(y_t z_i h_t^{-j}) \sum_{i=0}^{2^{t-1}-1} \chi_t^{2a}(h_t^{-2/2})^i$$

which is zero, since $\chi_t^{(h_t^{2a}(1-2j))}$ is a nontrivial $2^t$th root of unity.

To find the $y_t$’s and $z_i$’s and to show that they are compatible with the $h_t$’s chosen above, we need the following lemma.

**Lemma 6.** If $\chi \in [\chi_t]$ and $z \in G \setminus H$ such that $z^{2m} \in H \setminus K_t$, then if $\chi(z)$ is a primitive $2^r$th root of unity, so is $\chi(z)$.

Proof. Without loss of generality, we may assume that $\chi_t(z) = \omega$, a primitive $2^r$th root of unity and that $\chi(z^{2m})$ is a $2^r - k - m$th root of unity with $r > k + m$ (else $z^{2m}$ is in $K_t$). But by Lemma 4, this implies that $\chi_t(z^{2m})$ is also a $2^r - k - m$th root of unity (not necessarily primitive). Hence $\omega^{2m}$ is a $2^r - k - m$th root of unity, which implies that $k = 0$.

**Lemma 7.** For any group $G$ meeting the exponent bound there exists a subgroup $H$ of order $2^{d+1}$ so that we can always find $z_t$ and an $h_t$ for all $t$, $1 \leq t \leq Q$, that satisfy properties 1 and 2.

Proof. We break up the proof into two cases. First assume that $G = \mathbb{Z}_{2^{d+2}} \times A$, where $A$ is any abelian 2-group of order $2^d$. Let $c$ be any element in $G \setminus A$ of order $2^{d+2}$ and set $H = A \times \langle c^{2^{d+1}} \rangle$. Let $h_t$ be chosen as in Lemma 5; hence property 1 is satisfied. It remains to choose a $z_t$ which is compatible with this $h_t$.

Let the order of $\chi_t$ restricted to $H$ be $2^{s+1}$. Note that $s$ is always strictly less than $d$. Suppose that $c^{2^{d+1}} \notin K_t$. Then let $z_t = c^{2^{d-s+1}}$. Otherwise let $z_t = h_t c^{2^{d-s+1}}$. Clearly this $z_t$ satisfies all the conditions of Lemma 6 with $m = s$. Hence for all $\chi \in [\chi_t]$ we have that $\chi(z)$ is a primitive $2^{s+1}$th root of unity.

Now assume that the exponent of $G$ is strictly less than $2^{d+2}$ and let $G = \mathbb{Z}_{2a_1} \times \cdots \times \mathbb{Z}_{2a_k} = A \times \mathbb{Z}_{2a_k}$, where $a_1 \leq a_2 \leq \cdots \leq a_k \leq d + 1$. Let $H$ be any subgroup contained in $A$ of order $2^{d+1}$ and let $c$ be any element in $G \setminus A$ of order $2^{a_k}$. Let the order of $\chi_t$ restricted to $H$ be $2^{s+1}$. Note that $s$ is strictly less than $a_k$. Let $z_t = h_t c^{2^{a_k-s}}$. It is clear that $z_t$ satisfies all the conditions of Lemma 6 with $m = s$. Hence for all $\chi \in [\chi_t]$ we have that $\chi(z)$ is a primitive $2^{s+1}$th root of unity.
To check property 2, we need to show that
\[
\sum_{j=0}^{2^i-1} \chi(y, z_j h_t^{-(2j+1)}) = \chi(y, h_t^{i}) \sum_{j=0}^{2^i-1} \chi(z, h_t^{-(2j+1)})^j
\]
is zero for any \(\chi \in [X_i]\) for all \(i\) except one, called \(i_0\), which depends on \(\chi\), in which case the sum has magnitude \(2^s\). From above, we have chosen \(z_t\) so that \(\chi(z_t)\) is a primitive \(2^{a+1}\)th root of unity for any \(\chi \in [X_i]\) for any \(G\) meeting the exponent bound. Now by Lemma 4 we know that \(\chi(h_t)\) is also a \(2^{a+1}\)th primitive root of unity, call it \(\omega\). Let \(\chi(z_t) = \omega^a\), where \(a\) is odd. Then \(\chi(z_t h_t^{-(2j+1)}) = \omega^{a-2i-1}\). As long as \(a - 2i - 1 \equiv 0 \mod 2^{s+1}\), the sum is zero. At \(2i \equiv a - 1 \mod 2^{s+1}\), which has a unique solution modulo \(2^s\), we obtain \(\sum_{j=0}^{2^i-1} \chi(z_t h_t^{-(2j+1)})^j = 2^s\). Since \(\chi(y, h_t^0)\) is a root of unity, the sum has magnitude \(2^s\). Thus property 2 can always be satisfied.

### 3. Choosing the \(y_t\)'s

It remains to show that there is a method for choosing \(y_t\) for all \(t\) given our choice of \(z_t\) and \(h_t\) such that property 3 is satisfied. We consider the case \(\exp(G) = 2^{d+2}\) first.

Let \(G = A \times \mathbb{Z}_{2^d+2}\), where \(A\) is some abelian 2-group and let \(c\) be any element in \(G \setminus A\) of order \(2^{d+1}\). Recall that \(H = A \times \langle c^{2^d+1} \rangle\). The cosets of \(H\) in \(G\) are \(H, cH, c^2H, \ldots, c^{2^{d+1}+1}H\). Now for each \(t\), \(z_t^j\) has the form \(c^{j+1} h_t^{-(2j+1)}\) or \(h_t^{j+1} c^{j+1} h_t^{-(2j+1)}\). Hence the only thing of interest is the exponent of \(c\) after multiplication by \(y_t\), which is of the form \(c^b\).

We begin by enumerating the distinct equivalence classes not equal to \([x_0]\) as \([x_1], [x_2], \ldots, [x_Q]\), so that the order of \(\chi_t\) restricted to \(H\) is always greater than or equal to the order of \(\chi_{t+1}\) restricted to \(H\). We have the following useful fact concerning these \(Q\) equivalence classes:

**Lemma 8.** \(\sum_{i=1}^{Q} |\chi_t|_{|H|} = 2(2^{d+1} - 1)\).

**Proof.** By Lemma 3 we know that each equivalence class \([\chi_i]\) has exactly \(\frac{1}{2}|\chi|_{|H|}\) distinct elements when considered as characters on \(H\). The sum is therefore merely asking for twice the total number of distinct nonprincipal characters on \(H\), which is \(2(2^{d+1} - 1)\).

We now choose \(y_t\) according to the following procedure:

1. Let \(S\) be an order list of integers from 1 to \(2^{d+1} - 1\) all initially unmarked.
2. Set \(t = 1\).
3. Let \( b_t \) be the minimal unmarked integer in \( \mathcal{L} \). Mark all integers of the form \( b_t + k2^{d-s+1} \), \( 0 \leq k \leq 2^s - 1 \), where the order of \( \chi_t \) restricted to \( H \) is \( 2^{s+1} \).

4. Set \( y_t = e^{b_t} \).

5. Increment \( t \). Doing 3, 4, and 5 constitutes one step (step \( t \)). Go to 3 and repeat until \( Q \) steps have been taken.

The \( y_t \)'s chosen in this manner satisfy property 3, provided we show the following three things:

**Lemma 9.**

1. We are never required to mark or choose an element outside of \( \mathcal{L} \).
2. We never mark any integer in \( \mathcal{L} \) more than once.
3. We eventually mark every integer in \( \mathcal{L} \).

**Proof.** First note that at step \( t \) we are marking out a number of integers equal to one-half the order of \( \chi_t \) restricted to \( H \). Hence by Lemma 8 we will make exactly \( 2^{d+1} - 1 \) marks upon completion of the algorithm. Therefore at most \( 2^{d+1} - 1 \) distinct integers in \( \mathcal{L} \) will be marked.

To prove the first claim, it suffices to show that for all \( t \), \( 1 \leq t \leq Q \), \( b_t < 2^{d-s+1} \), where the order of \( \chi_t \) restricted to \( H \) is \( 2^{s+1} \). Suppose at step \( t \) that all the integers from 1 to \( 2^{d-s+1} - 1 \) have been marked on previous steps. Let \( r \) be any integer in \( \mathcal{L} \) not congruent to 0 mod \( 2^{d-s+1} \). Then \( r = r' + m2^{d-s+1} \), where \( 1 \leq r' < 2^{d-s+1} - 1 \) and \( 0 \leq m < 2^t - 1 \). But we are assuming that \( r' \) has already been marked. Hence there exists a \( u < t \) so that \( r' = b_u + m'2^{d-s+1} \), where \( s' \geq s \) and \( m' < 2^{s'-s} - 1 \). Hence \( r = b_u + (m + m'2^{s'-s})2^{d-s+1} \). But since \( m' < 2^{s'-s} - 1 \) and \( m < 2^s - 1 \), we obtain \( m + m'2^{s'-s} < 2^s - 1 \). Therefore, \( r \) has been marked at an earlier step.

Now suppose that \( b_t > 2^{d-s+1} \), i.e., suppose that \( 2^{d-s+1} \) has been marked on a previous step. Then there exists a \( u < t \) and an \( s' \geq s \), so that \( 2^{d-s+1} = b_u + m2^{d-s+1} \) for some \( m \) strictly less than \( 2^{s-s} \). But then if \( k \leq 2^s - 1 \), we have \( k2^{d-s+1} = b_u + (2^{s'-s}(k-1) + m)2^{d-s+1} \). And since \( 2^{s'-s}(k-1) + m \leq 2^{s'-s} - 1 \), we have that \( k2^{d-s+1} \) has been marked previously as well, which leaves no unmarked integer at step \( t \). Therefore the algorithm must have ended previously; otherwise we contradict the fact that we make exactly \( 2^{d+1} - 1 \) marks. Hence \( b_t = 2^{d-s+1} \) and all the multiples of \( 2^{d-s+1} \) are the only remaining unmarked integers in \( \mathcal{L} \). But step \( t \) requires that we make \( 2^s \) distinct marks. Since we have already made at least \( 2^{d+1} - (2^s - 1) \) marks on previous steps, this contradicts the fact that exactly \( 2^{d+1} - 1 \) marks are made. Thus the first assertion is true.
To show the second claim, suppose that there is an integer \( r \) in \( \mathcal{L} \) which is marked at least twice. Then there exist two distinct numbers \( t_1 \) and \( t_2 \) such that \( r = b_{t_1} + m2^{d-s} + 1 = b_{t_2} + m'2^{d-s} + 1 \), where as usual \( 2^{s+1} \) denotes the order of \( \chi_{i_1} \) restricted to \( H \) and \( 2^{s+1} \) denotes the order of \( \chi_{i_2} \) restricted to \( H \). Assume that \( t_1 < t_2 \); hence \( s \geq s' \). Then we have that \( 2^{d-s} + 1 | b_{t_2} - b_{t_1} \). Hence we can write \( b_{t_2} = b_{t_1} + k2^{d-s} + 1 \), for some \( k > 0 \). But by claim 1, \( b_{t_2} \) is in \( \mathcal{L} \) and so \( k \leq 2^s - 1 \) and, therefore, \( b_{t_2} \) has already been marked at step \( t_1 \), contradicting the fact that it must be unmarked before step \( t_2 \).

The third claim follows at once from the remark made at the beginning of the proof and the first two claims.

We have demonstrated that \( h_t, z_t \) and \( y_t \) can always be chosen so that properties 1, 2, and 3 are satisfied for any abelian 2-group whose exponent is \( 2^{d+2} \) and hence we have shown:

**Theorem 2.** If \( G \) is an abelian 2-group with \( \exp(G) = 2^{d+2} \), then \( G \) has a difference set.

Now let us assume that the exponent on \( G \) is \( 2^e \) and write \( G = A \times \mathbb{Z}_{2^e} \). Recall that \( H \) is chosen to be any order \( 2^{d+1} \) subgroup contained in \( A \). Let \( a_1, a_2, \ldots, a_m = 1 \) be a complete set of \( m = 2^{d+1} - e \) distinct coset representatives of \( H \) in \( A \). Let \( c \) be any element of \( G \setminus A \) of order \( 2^e \). Recall that \( z_t = h_i c^{2^{e-s}}, \) where the order of \( \chi_i \) restricted to \( H \) is \( 2^{s+1} \), and that \( s < e \) for all \( t \). We choose \( y_t \) to be of the form \( a_i c^j, 1 \leq i \leq m \) and \( 1 \leq j \leq 2^e \), with the proviso that \( y_t \) is never chosen to be the identity. Hence the only concern for satisfying property 3 is that as we run over all \( t \geq 1 \) the elements \( a_i c^j, a_i c^{j+2^{e-s}}, \ldots, a_i c^{j+(2^e-1)2^{e-s}}, \) together with the identity, comprise a complete set of coset representatives of \( H \) in \( G \).

We begin by enumerating the equivalence classes exactly as before. Having done that, we write the cosets of \( H \) in an array thus:

\[
\begin{pmatrix}
  a_1 c H & a_1 c^2 H & \cdots & a_1 c^{2^e-1} H & a_1 H \\
  a_2 c H & a_2 c^2 H & \cdots & a_2 c^{2^e-1} H & a_2 H \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  a_m c H & a_m c^2 H & \cdots & a_m c^{2^e-1} H & a_m H
\end{pmatrix}
\]

The row indices run from 1 to \( m \) and the column indices run from 1 to \( 2^e \).

The algorithm for choosing \( y_t \) is as follows:

1. Let \( \mathcal{M} \) be an \( m \times 2^e \) matrix of integers, each row of which contains the integers from 1 to \( 2^e \) in order, all initially unmarked.

2. Set \( t = 1 \).

3. Let \( b_t \) be the unmarked entry in \( \mathcal{M} \) of minimal value. In case of a tie, choose the entry in the row of minimal index. Mark out all entries
in that row of the form \( b_t + k2^{e-s} \), for \( 0 \leq k \leq 2^e - 1 \), where \( 2^{e+1} \) is the order of \( \chi \) restricted to \( H \). Call the row where \( b_t \) lies \( r_t \).

4. Set \( y_t = a_m c^{b_t} \), where \( a_m = 1 \).

5. Increment \( t \). Doing 3, 4, and 5 constitutes step \( t \). Go to 3 and repeat until \( Q \) steps have occurred.

To show that when the \( y_t \)'s are chosen in this manner property 3 is satisfied, it suffices to show the following lemma is true:

**Lemma 10.**

1. We are never forced to mark something outside of the matrix \( \mathcal{M} \).
2. We never mark anything more than once.
3. Every entry except \( m_{m,2^{e-1}} \), corresponding to the coset \( H \), is marked.

**Proof.** First note that the proof of Lemma 8 applies here as well. Hence we will never make more than a total of \( 2^{d+1} - 1 \) marks upon completion of the algorithm.

To prove the first assertion it suffices to show that \( b_t \) is always less than or equal to \( 2^{e-s} \), where \( 2^{s+1} \) is the order of \( \chi \) restricted to \( H \). Since by the remark above we will never mark out more than a total of \( 2^{d+1} - 1 \) entries, we are never in the situation of having to step the algorithm, by not having any unmarked integer left in the array. So suppose we are at step \( t \) and \( b_t > 2^{e-s} \). Let \( r \) be any integer, \( 1 \leq r \leq 2^e \), in row \( i \). Then there exists an \( r' \), \( 0 < r' \leq 2^{e-s} \), so that \( r = r' + k2^{e-s} \). Now, by assumption, \( r' \) has been previously marked; hence it is of the form \( r' = b_u + k'2^{e-s} \), where \( s' \geq s \) and \( k' < 2^{s'-s} \). Hence \( r = b_u + (k' + k2^{s'-s})2^{e-s} \). But, since \( k' \leq 2^{e-s} - 1 \) and \( k \leq 2^e - 1 \), we have \( (k' + k2^{s'-s})k \leq 2^{e-1} \), which implies that \( r \) has been previously marked. This holds for any \( i \), since \( b_t \) had to be greater than \( 2^{e-s} \). Hence every entry in \( \mathcal{M} \) has been marked, contradicting the fact that at most \( 2^{d+1} - 1 \) distinct entries can be marked.

To prove the second assertion, assume that there is some row where some integer \( r \) has been marked at least twice. Then there exists a \( t \) and a \( t' > t \) so that \( r = b_t + k2^{e-s} = b_{t'} + k'2^{e-s} \), where \( 2^{s+1} \) is the order of \( \chi \), restricted to \( H \), and \( 2^{e+1} \) is the order of \( \chi \), restricted to \( H \). Since \( t' > t \) then \( s' \leq s \). Therefore \( b_{t'} - b_t \) is divisible by \( 2^{e-s} \), which implies that there is some positive number \( q \) so that \( b_{t'} = b_t + q2^{e-s} \). But, since \( b_{t'} \leq b_t + k2^{e-s} \), then \( q \leq k \leq 2^{e-1} \), which implies that \( b_{t'} \) had previously been marked, which is a contradiction.

To show the third assertion, note that since we mark at most \( 2^{d+1} - 1 \) distinct entries and, by the above, we mark nothing more than once, we must mark exactly \( 2^{d+1} - 1 \) entries in \( \mathcal{M} \). Hence there is one entry which is not marked. Now if the integer \( 2^e \) in the \( m \)th row is marked, then there
PROOF OF A CONJECTURE ON 2-GROUPS

exists a \( t \) and \( s \), so that \( 2^r = b_t + k2^{e-s} \). But that can only occur if \( b_t = 2^{e-s} \)
and \( k = 2^s - 1 \). But this implies that every integer less than or equal to \( 2^{e-s} \)
in all the rows has been previously marked. This, by an argument similar
to the one used to prove the first assertion, implies that all the entries in \( M \) are marked after step \( t \), contradicting the fact that exactly \( 2^{d+1} - 1 \)
entries are marked. Hence the third assertion is true. \( \square \)

Thus, for any abelian 2-group with exponent less than \( 2^{d+2} \) we can
always find an \( h_t \), \( z_t \), and \( y_t \) so that properties 1, 2, and 3 are satisfied.
Combined with the result on groups of exponent \( 2^{d+2} \), we have

**THEOREM 3.** Any abelian 2-group that meets the exponent bound has a
difference set.

4. AN EXAMPLE

We will use the methods outlined above to construct a difference set in
the group \( \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_{64} \). Let \( a \), \( b \), and \( c \) be the generators of \( G \) with
\( a^4 = b^4 = c^{64} = 1 \). Since \( G \) has order 1024, the difference set \( D \) can be
assumed to have parameters \((1024, 496, 240)\). Since the exponent of \( G \) is
64, which is \( 2^{d+2} \), we choose \( H \) to be the subgroup \( \langle a \rangle \times \langle b \rangle \times \langle c^{32} \rangle \).
Thus the cosets of \( H \) are \( H, cH, c^2H, \ldots, c^{31}H \).

TABLE I

<table>
<thead>
<tr>
<th>( t )</th>
<th>Class</th>
<th>Order</th>
<th>( \text{Kern}(z_t) \cap H )</th>
<th>( h_t )</th>
<th>( z_t )</th>
<th>( y_t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[0, 1, 0]</td>
<td>4</td>
<td>( \langle a \rangle \times \langle c^{32} \rangle )</td>
<td>( b )</td>
<td>( bc^{16} )</td>
<td>( c )</td>
</tr>
<tr>
<td>2</td>
<td>[0, 1, 1]</td>
<td>4</td>
<td>( \langle a \rangle \times \langle b^2c^{32} \rangle )</td>
<td>( b )</td>
<td>( c^{16} )</td>
<td>( c^2 )</td>
</tr>
<tr>
<td>3</td>
<td>[1, 0, 0]</td>
<td>4</td>
<td>( \langle b \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( ac^{16} )</td>
<td>( c^3 )</td>
</tr>
<tr>
<td>4</td>
<td>[1, 0, 1]</td>
<td>4</td>
<td>( \langle b \rangle \times \langle a^2c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{16} )</td>
<td>( c^4 )</td>
</tr>
<tr>
<td>5</td>
<td>[1, 1, 0]</td>
<td>4</td>
<td>( \langle ab^2 \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( ac^{16} )</td>
<td>( c^5 )</td>
</tr>
<tr>
<td>6</td>
<td>[1, 1, 1]</td>
<td>4</td>
<td>( \langle ab^2 \rangle \times \langle b^2c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{16} )</td>
<td>( c^6 )</td>
</tr>
<tr>
<td>7</td>
<td>[1, 2, 0]</td>
<td>4</td>
<td>( \langle a^2b \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( ac^{16} )</td>
<td>( c^7 )</td>
</tr>
<tr>
<td>8</td>
<td>[1, 2, 1]</td>
<td>4</td>
<td>( \langle a^2b \rangle \times \langle b^2c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{16} )</td>
<td>( c^8 )</td>
</tr>
<tr>
<td>9</td>
<td>[1, 3, 0]</td>
<td>4</td>
<td>( \langle ab \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( ac^{16} )</td>
<td>( c^9 )</td>
</tr>
<tr>
<td>10</td>
<td>[1, 3, 1]</td>
<td>4</td>
<td>( \langle ab \rangle \times \langle b^2c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{16} )</td>
<td>( c^{10} )</td>
</tr>
<tr>
<td>11</td>
<td>[2, 1, 0]</td>
<td>4</td>
<td>( \langle ab^2 \rangle \times \langle c^{32} \rangle )</td>
<td>( b )</td>
<td>( bc^{16} )</td>
<td>( c^{11} )</td>
</tr>
<tr>
<td>12</td>
<td>[2, 1, 1]</td>
<td>4</td>
<td>( \langle ab^2 \rangle \times \langle b^2c^{32} \rangle )</td>
<td>( b )</td>
<td>( c^{16} )</td>
<td>( c^{12} )</td>
</tr>
<tr>
<td>13</td>
<td>[0, 0, 1]</td>
<td>2</td>
<td>( \langle a \rangle \times \langle b \rangle )</td>
<td>( a )</td>
<td>( c^{13} )</td>
<td>( c^{14} )</td>
</tr>
<tr>
<td>14</td>
<td>[0, 2, 0]</td>
<td>2</td>
<td>( \langle a \rangle \times \langle b^2 \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{14} )</td>
<td>( c^{15} )</td>
</tr>
<tr>
<td>15</td>
<td>[0, 2, 1]</td>
<td>2</td>
<td>( \langle a \rangle \times \langle bc^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{13} )</td>
<td>( c^{16} )</td>
</tr>
<tr>
<td>16</td>
<td>[2, 0, 0]</td>
<td>2</td>
<td>( \langle a^2 \rangle \times \langle b \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{15} )</td>
<td>( c^{29} )</td>
</tr>
<tr>
<td>17</td>
<td>[2, 0, 1]</td>
<td>2</td>
<td>( \langle a \rangle \times \langle ac^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{14} )</td>
<td>( c^{30} )</td>
</tr>
<tr>
<td>18</td>
<td>[2, 2, 0]</td>
<td>2</td>
<td>( \langle ab \rangle \times \langle b^2 \rangle \times \langle c^{32} \rangle )</td>
<td>( a )</td>
<td>( c^{31} )</td>
<td>( c^{31} )</td>
</tr>
</tbody>
</table>
A character on $G$ is uniquely determined by where it sends $a$, $b$, and $c$. Let $\omega$ be a primitive 64th root of unity and define $\chi_{r,s,t}(a^ib^jc^k)$ to be $\omega^{16ri+16sj+tk}$ for $0 \leq r \leq 3$, $0 \leq s \leq 3$, $0 \leq t \leq 63$. Then these are the 1024 distinct group characters on $G$.

We now collect these characters into equivalence classes. For convenience, the equivalence class of $[\chi_{r,s,t}]$ is simply denoted $[r, s, t]$. Table I summarizes the 19 distinct classes not equivalent to $[0, 0, 0]$.

The difference set is then formed by taking for $1 \leq t \leq 12$ the elements in the kernel and multiplying them by the elements $y_i z_j h^i_{-\left(2^i+1\right)}$, where $i$ and $j$ go from 0 to 1 and for $13 \leq t \leq 19$, taking the elements in the kernel and multiplying them by $y_i$.

REFERENCES