4-1994

A Construction of Difference Sets in High Exponent 2-Groups Using Representation Theory

James A. Davis
University of Richmond, jdavis@richmond.edu

Ken Smith

Journal of Algebraic Combinatorics 3 (1994), 137–151

A Construction of Difference Sets in High Exponent 2-Groups Using Representation Theory

JAMES A. DAVIS*
Department of Mathematics, University of Richmond, Richmond, VA 23173

KEN SMITH
Department of Mathematics, Central Michigan University, Mt. Pleasant, MI 48859

Received March 11, 1993; Revised August 9, 1993

Abstract. Nontrivial difference sets in groups of order a power of 2 are part of the family of difference sets called Menon difference sets (or Hadamard), and they have parameters $(2^{2d+2}, 2^{2d+1} \pm 2^d, 2^{2d} \pm 2^d)$. In the abelian case, the group has a difference set if and only if the exponent of the group is less than or equal to 2^{d+2}. In [14], the authors construct a difference set in a nonabelian group of order 64 and exponent 32. This paper generalizes that result to show that there is a difference set in a nonabelian group of order 2^{2d+2} with exponent 2^{d+3}. We use representation theory to prove that the group has a difference set, and this shows that representation theory can be used to verify a construction similar to the use of character theory in the abelian case.

Keywords: difference set, representation theory, abelian group, and nonabelian group

1. Introduction

Let G be a multiplicative group of order v and D be a k-subset of G; then D is called a (v, k, λ)-*difference set* in G provided that the differences dd'^{-1} for $d, d' \in D$, $d \neq d'$ contain every nonidentity element of G exactly λ times. See [11] for results on difference sets. We shall consider $(2^{2d+2}, 2^{2d+1} \pm 2^d, 2^{2d} \pm 2^d)$-difference sets (known as *Menon* or, alternatively, *Hadamard* difference sets). In the abelian case, the existence question was completely answered by the following theorem due to Kraemer [10] and Jedwab [8].

THEOREM 1.1. *The abelian group G has a $(2^{2d+2}, 2^{2d+1} \pm 2^d, 2^{2d} \pm 2^d)$ if and only if the exponent of the group is less than or equal to 2^{d+2}.*

The nonabelian case had also been studied, and there are both existence and nonexistence results. McFarland [16] provided a construction that was generalized by Dillon [6], and they both have applications in nonabelian groups. Davis, in [4, 5] showed how the constructions that solved the abelian groups can

*This work is partially supported by NSA grant MDA 904-92-H-3057.

be generalized into nonabelian cases. All of these constructions are in groups whose exponents are less than or equal to 2^{d+2}. As for nonexistence, there are two known results. The first one is due to Turyn [17].

THEOREM 1.2. *Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup so that G/H is cyclic. If $|H| < 2^d$, then G does not have a difference set.*

The second nonexistence result is due to Dillon [6], and then it has been generalized by Ma [15].

THEOREM 1.3. *Let G be a group of order 2^{2d+2} with a normal subgroup H of order $2^r < 2^d$ so that G/H is a dihedral group: G does not have a nontrivial difference set.*

These are the only known nonexistence results, and it would be interesting to know if there are any other conditions that will exclude a 2-group from having a difference set. In the cases that have been exhaustively studied, namely the groups of order 16 [9] and the groups of order 64 [7], these are the only types of groups that have been ruled out.

A major advance in understanding was made in the paper by Liebler and Smith [14], where they construct a difference set in a group of order 64 with exponent 32. The aim of this paper is to show that the difference set found in that paper is part of a family of difference sets in groups of order 2^{2d+2} with exponent 2^{d+3}; this shows that the exponent bound in the abelian case does not apply to the nonabelian case. This paper will also demonstrate how the traditional techniques involving character theory can be generalized to techniques involving representation theory.

We will develop the representation theoretic point of view in the second section, and we will introduce the group that we are working with as well as its irreducible representations. The third section introduces the family of groups that we will work with as well as the representations associated to those groups. In addition to that, that section will show how the difference set found by Liebler and Smith can be viewed as a K-matrix structure as defined in [3]. The fourth section will give the difference set construction for the general group, and we will prove that this construction works. Finally, the fifth section gives two examples of difference sets in groups of order 256.

2. Representation theoretic preliminaries

Consider the group ring $Z[G]$. If A is a subset of G, we will abuse notation by writing A as a member of the group ring, $A = \sum_{a \in A} a$. Similarly we will define the group ring element $A^{(-1)} = \sum_{a \in A} a^{-1}$. If D is a difference set in G, then the definition of a difference set immediately yields the group ring equation

$$DD^{(-1)} = k - \lambda + \lambda G$$

Now consider a representation of G, call it ϕ. A representation is simply a homomorphism from G to the multiplicative group of $m \times m$ matrices. We can always choose our basis so that the representation is unitary; namely, the inverse of the matrix $\phi(g)$ will be the conjugate transpose (see [2]). This homomorphism can be extended to a ring homomorphism from the group ring $Z[G]$ to the ring of $m \times m$ matrices, and we will use the notation $\phi(A) = \sum_{a \in A} \phi(a)$. Note that if ϕ is an irreducible representation of degree > 1, then $\phi(G) = 0$. We show this by contradiction; if not, then we could find a vector v so that $u = \phi(G)(v) \neq 0$. The vector u generates a 1-dimensional subspace that is left invariant by all $\phi(g)$, which cannot happen if ϕ is irreducible.

If we apply an irreducible nontrivial ϕ to the group ring equation above, we get

$$\phi(DD^{(-1)}) = \phi(D)\phi(D^{(-1)}) = \phi(k - \lambda) + \lambda\phi(G) = (k - \lambda)I_m$$

In the above, I_m is the $m \times m$ identity matrix, where m is the degree of ϕ. The next theorem is the reason why we want to look at these representation sums over D.

THEOREM 2.1. *Let D be a subset of size k of a group G. If $\phi(D)\phi(D^{(-1)}) = nI_m$ for every nontrivial irreducible representation ϕ of G, then D is a difference set in G.*

Proof. Any subset D of G is completely determined by its image under the regular representation. The regular representation is a sum of all irreducible representations; this implies that D is completely determined by its image under all the irreducible representations (see [12]). □

Thus, we need to find a matrix so that when we multiply it by its conjugate transpose we get a multiple of the identity. There may be many ways to do this, but Liebler and Smith found a way to do it with a 2×2 nondiagonal matrix, and that was the key to getting the difference set in the modular group. The following lemma is a generalization of that idea.

LEMMA 2.1. *Let η be a primitive 2^r root of unity. The matrix*

$$\begin{pmatrix} \eta^2 + \eta^3 + \eta^{-2} - \eta^{-3} & \eta^2 + \eta^3 - \eta^{-2} + \eta^{-3} \\ \eta^2 - \eta^3 - \eta^{-2} - \eta^{-3} & \eta^2 - \eta^3 + \eta^{-2} + \eta^{-3} \end{pmatrix}$$

times its conjugate transpose is $8\ I_2$.

Proof. We give the computation for the upper left corner of the product as a motivation for why this works; the other computations are similar. If we collect the η^2 and η^{-2} terms and the η^3 and $\eta^{2^{r-1}-3}$ terms, the upper left corner of the

product will be

$$\begin{aligned}
&((\eta^2+\eta^{-2})+(\eta^3-\eta^{-3}))((\eta^2+\eta^{-2})+(-\eta^3+\eta^{-3}))\\
&\quad+((\eta^2-\eta^{-2})+(\eta^3+\eta^{-3}))((-\eta^2+\eta^{-2})+(\eta^3+\eta^{-3}))\\
&\qquad=(\eta^2+\eta^{-2})^2+(\eta^2+\eta^{-2})(-\eta^3+\eta^{-3}+\eta^3-\eta^{-3})-(\eta^3-\eta^{-3})^2\\
&\qquad\quad-(\eta^2-\eta^{-2})^2+(\eta^2-\eta^{-2})(\eta^3+\eta^{-3}-\eta^3-\eta^{-3})+(\eta^3+\eta^{-3})^2\\
&\qquad=\eta^4+2+\eta^{-4}-(\eta^6-2+\eta^{-6})-(\eta^4-2+\eta^{-4})+\eta^6+2+\eta^{-6}\\
&\qquad=8
\end{aligned}$$

□

In this paper, we will be working with the group defined by $G=\langle x, y : x^{2^{d+3}} = y^{2^{d-1}} = 1, yxy^{-1} = x^{2^{d+2}+1}\rangle$. In order to apply the theorems of the previous section, we need a complete list of the irreducible representations of G. For this group, we have linear representations (degree 1) and degree 2 representations. There are 2^{2d-1} inequivalent irreducible degree 2 representations, all of the form

$$\phi_m : x \to \begin{pmatrix} \eta & 0 \\ 0 & -\eta \end{pmatrix}, y \to \begin{pmatrix} 0 & \eta^{-16m} \\ \eta^{-16m} & 0 \end{pmatrix},$$

where η is a primitive 2^{d+3} root of unity (we have 2^{d+1} choices for the primitive root of unity to $\pm$), and $m = 0, 1, \ldots, 2^{d-2}-1$. When d is odd, we will write $m = \mu 2^{\frac{d-1}{2}} + \delta 2^{\frac{d-3}{2}} + \gamma$, $\mu = 0, 1, \ldots, 2^{\frac{d-5}{2}}-1$; $\delta = 0, 1$; $\gamma = 0, 1, \ldots, 2^{\frac{d-3}{2}}-1$. This will make some of our arguments later break into cases. The linear representations are all of the form $x \to \eta^{2i}$, $y \to \eta^{16j}$, where $i = 0, 1, \ldots, 2^{d+2}-1$, $j = 0, 1, \ldots, 2^{d-1}-1$. The nonlinear representations are all irreducible since they are degree 2 and $\phi(x)\phi(y) \neq \phi(y)\phi(x)$. They are inequivalent since they are distinguished by their traces on the set $\{x^2, y^2\}$. A counting argument shows that we have all the irreducible representations. All of our arguments will be separated by the degree of the representation.

3. K-matrix structure

In the abelian case, a construction entitled K-matrices helped answer the existence question. An example might help explain what K-matrices look like.

Example. Consider the semidirect product of Z_{32} and Z_2, with relations $x^{32} = y^2 = 1$, $yxy = x^{17}$. This is the modular group M_{64} (see [1]). In [14], the authors list the following set as a difference set.

$$\begin{aligned}
D &= (1+x^{16})(1+x^4+y+x^{12}y+x+x^9)\\
&\quad+(1+x^8)(x^2+x^{-2}+x^8(x^5+x^{-5}+x^{10}y+x^{-10}y)+x^{13}y+x^{-13}y)
\end{aligned}$$

We are going to reorganize this with respect to the subgroup $H=\langle x^8, y\rangle$. If

we do that, we get the difference set breaking up into subsets of cosets of H as follows:

$$\begin{aligned}
D_1 &= \{1, y, x^{16}, x^{16}y\} = \langle x^{16}, y\rangle \subset H \\
xD_2 &= \{x, x^9, x^{17}, x^{25}\} = x\langle x^8\rangle \subset xH \\
x^2D_3 &= \{x^2, x^{10}, x^{18}y, x^{26}y\} = x^2(1 + x^8)\langle x^{16}y\rangle \subset x^2H \\
x^3D_4 &= \{x^3, x^{11}, x^{19}y, x^{27}y\} = x^3(1 + x^8)\langle x^{16}y\rangle \subset x^3H \\
x^4D_5 &= \{x^4, x^{12}y, x^{20}, x^{28}y\} = x^4\langle x^8y\rangle \subset x^4H \\
x^5D_6 &= \{x^{13}, x^{21}, x^{13}y, x^{21}y\} = x^{13}(1 + x^8)\langle y\rangle \subset x^5H \\
x^6D_7 &= \{x^{30}, x^6, x^{30}y, x^6y\} = x^{30}(1 + x^8)\langle y\rangle \subset x^6H
\end{aligned}$$

We view the difference set as a union of subsets, where each subset is contained in a coset of a specific subgroup. Moreover, each of these subsets is made up of a union of cosets of even smaller subgroups. We write the difference set in this way because it allows us to check the representation sums easily and use Theorem 3.2.

Case 1. Suppose ϕ is an irreducible representation of degree 2. From the previous discussion, ϕ maps x to the matrix with η, $-\eta$ down the diagonal, and y goes to the matrix with 1 on the off diagonals. Since the subgroups used to define D_1, D_2, and D_5 contain x^{16}, the representation sum over those pieces will be 0. Thus, we only need to consider the representation sum over the remaining pieces. When we do this, we get

$$\begin{aligned}
\phi(D) = (1 + i)\Bigg(&\begin{pmatrix} \eta^2 & -\eta^2 \\ -\eta^2 & \eta^2 \end{pmatrix} + \begin{pmatrix} \eta^3 & -\eta^3 \\ \eta^3 & -\eta^3 \end{pmatrix} \\
&+ \begin{pmatrix} \eta^{13} & \eta^{13} \\ -\eta^{13} & -\eta^{13} \end{pmatrix} + \begin{pmatrix} \eta^{-2} & \eta^{-2} \\ \eta^{-2} & \eta^{-2} \end{pmatrix}\Bigg)
\end{aligned}$$

This matrix is similar to the one found in Lemma 2.1, and when it is multiplied times its conjugate transpose, we get $16I_2$.

Case 2. Suppose that ϕ is a linear irreducible representation. In that case, x must be sent to η^{2j} (an even power of η), and y can be mapped to ± 1. The sum should have modulus 4. We break this up into two subcases:

Subcase a. If ϕ is nonprincipal on $\langle x^8, y\rangle$, then ϕ will send x^8, y, or both to -1. If it just sends x^8 to -1, then ϕ will have a sum of 0 over all of the D_i except D_1, so it has a sum of 4. If it just sends y to -1, then it will have a sum of 0 over all of the D_i except D_2, so its sum will be $4\phi(x)$. Finally, if it sends both x^8 and y to -1, then it will have a sum of 0 over all of the D_i except D_5, where it will have a sum of $4\phi(x^4)$.

Subcase b. If ϕ is principal on $\langle x^8, y\rangle$ but nonprincipal on G, then ϕ will have a sum of $4\phi(x^{i-1})$ over all of the D_i. When we add all of these up, we get $-4\phi(x^7)$, which has modulus 4.

Thus, all of the representation sums are correct, so by Theorem 2.1, this is a difference set.

In [3], a general K-matrix structure is defined for abelian groups. The idea is essentially the same as the example that was worked out above: we build the difference set out of D_i, and the representation sums are usually 0 except on a few of the D_i. We sometimes have to link several D_i together to make the representation sums work out correctly (in other words, there may be several of the D_i that do not have a 0 representation sum, but they add together in the proper way). This is formalized by the following definition.

Definition 3.1. The abelian group G of order 2^{2d+2} is said to have a K-matrix structure relative to a subgroup H of order 2^{d+1} if there is a subset D of G so that three conditions are met:

1. Every coset of H intersects D in 2^d elements except one, which has an empty intersection.
2. If χ is a representation that is nonprincipal on H, then χ has a 0 sum over all of the D_i (D_i is the intersection of the ith coset with D) except $\frac{2^d}{|Ker(\chi|H)|}$ of them. The character sum over those D_i has modulus 2^d.
3. The coset representatives of the $\frac{2^d}{|Ker(\chi|H)|}$ cosets that do not have a 0 character sum are of the form wz^j for some $w, z \in G$.

Any group with a K-matrix structure has a difference set, as shown in [3]. That paper also proves the next theorem.

THEOREM 3.1. *Let d be odd. The group $Z_{2^{d+1}} \times Z_{2^{d-1}}$ has a difference set by using a K-matrix structure relative to the subgroup $H \cong Z_{2^{\frac{d+1}{2}}} \times Z_{2^{\frac{d-1}{2}}}$. Moreover, if we write the group additively, the z mentioned in part 3 of the K-matrix definition will have first component that is* 0 mod 4.

There is a similar theorem for the d even case from that paper. We will only do the d odd case in this paper because the d even case is very similar. The difference set that is constructed in this theorem is used in the next section to build a difference set in a nonabelian group.

4. Main result

We will take steps in our attempts to build up the difference set. The first step will be to figure out a way to choose some D_i so that the linear characters of the group

will have the proper sum. In order to do that, we want to take the structure from Theorem 3.1 and lift it up to the group $\langle x, y : x^{2^{d+3}} = y^{2^{d-1}} = 1, yxy^{-1} = x^{2^{d+2}+1}\rangle$. To do this, first take the 1-1 homomorphism from $Z_{2^{d+1}} \times Z_{2^{d-1}} \to Z_{2^{d+2}} \times Z_{2^{d-1}}$, where the homomorphism doubles the first component. The elements from the K-matrix structure will map to elements in this bigger group; they will not form a K-matrix structure in the bigger group, but they will have the property that any character that is nonprinciple on $\langle (2, 0), (0, 1)\rangle$ will have a character sum of 2^{d-1}. Then take all of the elements of $\langle x, y\rangle$ that map down to these elements under the contraction by $x^{2^{d+2}}$. Notice that the subgroup in $\langle x, y\rangle$ that corresponds to H is $H' = \langle x^{2^{\frac{d+3}{2}}}, y^{2^{\frac{d-1}{2}}}\rangle \cong Z_{2^{\frac{d+3}{2}}} \times Z_{2^{\frac{d-1}{2}}}$, and that is the subgroup that we will work with in $\langle x, y\rangle$. We also remark here that since this is a contraction by a subgroup of order 2, then there will be 2 elements contracting down to every element in the K-matrix structure, so the character sum will be doubled to 2^d. Thus, if we start building our difference set in $\langle x, y\rangle$ out of this smaller difference set, this will have the proper representation sum for all of the linear representations that are nonprincipal on H'. Call the set defined above B.

We need to make one slight modification to this lifting of the K-matrix structure. In order to leave ourselves room for the rest of the difference set, we need to "slide" some of the K-matrices around. Let $b \in B : b = x^i y^j$ in the group $\langle x, y\rangle$. We will define a new set C as follows: if b is an element of B so that $i \equiv 2 \bmod 8$, then place $c = x^{-1}b$ into C. If b is an element of B so that $i \equiv 6 \bmod 8$, then place $c = xb$ into C. All of the other elements of B should be placed in C without modification. This forces all of the elements of C to have x-components that are 0, 1, 4, or 7 mod 8. We can do this without jeopardizing the good that we have accomplished in getting the representation sums to work out. The reason why this is true involves the last statement of Theorem 3.1, which talks about the z mentioned in part 3 of the definition of a K-matrix. Since the x-component of the z is divisible by 4, when we double everything in the lift to $Z_{2^{d+2}} \times Z_{2^{d-1}}$, the x-component of the z becomes divisible by 8. The z is the group element that links several of the cosets together to make the correct character sum, and all of the linked cosets will either be fixed or slid together. This implies that the representation sums will still be the same for the linear representations that are nonprincipal on H'. We state this in the following lemma.

LEMMA 4.1. *If ϕ is an irreducible linear representation of G that is nonprincipal on H', then $|\phi(C)| = 2^d$.*

Thus, we now need to figure out how to build the rest of the difference set around C. We will not be able to use exactly the same definition of a K-matrix structure for the rest of the group, but we do want to mimic the ideas. The first thing that we have to do is to show how we want our difference set to intersect with cosets of H', and then we will need to show how to link them together. First, the

intersections will look like the following (for $l = 0, \ldots, 2^{\frac{d-3}{2}-1}$, $k = 0, \ldots, 2^{\frac{d-1}{2}-1}$):

$$D_{l,k} = \left(\left(\bigcup_{i=0}^{2^{\frac{d-3}{2}}-1} x^{i2^{\frac{d+5}{2}}+ik2^{\frac{d+7}{2}}} \left\langle x^{2^{\frac{d+7}{2}}} y^{2^{\frac{d-1}{2}}} \right\rangle \right) \right.$$
$$\left. \bigcup \left(\bigcup_{j=0}^{2^{\frac{d-3}{2}}-1} x^{2^{\frac{d+3}{2}}+(j-k)2^{\frac{d+5}{2}}+jk2^{\frac{d+7}{2}}} \left\langle x^{2^{\frac{d+7}{2}}\left(l+2^{\frac{d-3}{2}}\right)} y^{2^{\frac{d-1}{2}}} \right\rangle \right) \right) \left(1 + x^{2^{d+1}}\right)$$

I claim that $D_{l,k}$ has 2^d distinct elements. To show this, first observe that $x^{(i-i')2^{\frac{d+5}{2}}(1+2k)} \notin \langle x^{2^{\frac{d+7}{2}}} y^{2^{\frac{d-1}{2}}} \rangle$, so the cosets $x^{i2^{\frac{d+5}{2}}+ik2^{\frac{d+7}{2}}} \langle x^{2^{\frac{d+7}{2}}} y^{2^{\frac{d-1}{2}}} \rangle$ and $x^{i'2^{\frac{d+5}{2}}+i'k2^{\frac{d+7}{2}}} \langle x^{2^{\frac{d+7}{2}}} y^{2^{\frac{d-1}{2}}} \rangle$ will be disjoint. A similar argument shows that $x^{2^{\frac{d+3}{2}}+(j-k)2^{\frac{d+5}{2}}+jk2^{\frac{d+7}{2}}} \langle x^{2^{\frac{d+7}{2}}(l+2^{\frac{d-3}{2}})} y^{2^{\frac{d-1}{2}}} \rangle$ and $x^{2^{\frac{d+3}{2}}+(j'-k)2^{\frac{d+5}{2}}+j'k2^{\frac{d+7}{2}}} \langle x^{2^{\frac{d+7}{2}}(l+2^{\frac{d-3}{2}})} y^{2^{\frac{d-1}{2}}} \rangle$ are disjoint. Finally, we can argue that $x^{i2^{\frac{d+5}{2}}+ik2^{\frac{d+7}{2}}} \langle x^{2^{\frac{d+7}{2}}} y^{2^{\frac{d-1}{2}}} \rangle$ and $x^{2^{\frac{d+3}{2}}+(j-k)2^{\frac{d+5}{2}}+jk2^{\frac{d+7}{2}}} \langle x^{2^{\frac{d+7}{2}}(l+2^{\frac{d-3}{2}})} y^{2^{\frac{d-1}{2}}} \rangle$ are disjoint by observing that the x coordinates of the first coset have exponents that are 0 mod $2^{\frac{d+5}{2}}$, and the x coordinates of the second coset have exponents that are $2^{\frac{d+3}{2}}$ mod $2^{\frac{d+5}{2}}$. Thus, $D_{l,k}$ is defined as a disjoint union of cosets, and a counting argument shows that there are 2^d elements in this set.

Every $D_{l,k}$ with the same l will be "linked" together by using the ks. Notice, for example, that when $l = 0$, then we are using the subgroups $\langle y^{2^{\frac{d-1}{2}}} \rangle$ and $\langle x^{2^{d+2}} y^{2^{\frac{d-1}{2}}} \rangle$ to define the intersection with the difference set. The ls will run from 0 to $2^{\frac{d-3}{2}} - 1$, and the ks will run from 0 to $2^{\frac{d-1}{2}} - 1$. We link them together as follows:

$$C' = \left(\bigcup_{l=0}^{2^{\frac{d-3}{2}}-1} \bigcup_{k=0}^{2^{\frac{d-1}{2}}-1} x^{8l}(x^{16l}y)^k D_{l,k} \right) \left(x^2 + x^3\right)$$
$$\bigcup \left(\bigcup_{l'=0}^{2^{\frac{d-3}{2}}-1} \bigcup_{k'=0}^{2^{\frac{d-1}{2}}-1} x^{8l'}(x^{2^{d+2}+16l'}y)^{k'} D_{l',k'} \right) \left(x^{-2} + x^{2^{d+2}-3}\right)$$

We need to make 2 observations before we go on to prove this. First, notice that all of the x-components are 2, 3, 6, or 5 mod 8: this is why we did the sliding of the elements of C. Thus, these will not overlap at all with C. Second, notice that the 2, 3, -2, and $2^{d+2} - 3$ are the exponents on the η in Lemma 2.1. We will use that lemma to get the degree 2 irreducible representations to work out properly, and the linking appears to have us set up to do that.

It would be nice if the representation sum were 0 over most of C' just like we were able to do with the K-matrix structure, and that is the purpose of the next lemma. This lemma is the reason why we chose such a strange notation when we defined the representations.

LEMMA 4.2. $\phi_m(\langle x^{2^{\frac{d+1}{2}}l} y^{2^{\frac{d-1}{2}}} \rangle) = 2^{\frac{d-1}{2}} I$ *if* $l \leftarrow \gamma$, $\delta = 0$ *or* $l = \gamma + 2^{\frac{d-3}{2}}$, $\delta = 1$, *and it is* 0 *otherwise.*

Proof. To show that this is true, we observe that $\phi_m(x^{2^{\frac{d+1}{2}}l} y^{2^{\frac{d-1}{2}}})$ is a diagonal matrix (since we have an even power of y here). If the entries down the diagonal are not equal to 1, then when we sum over the whole subgroup, we will get 0. If the entries are 1, then we will add 1 to itself the number of elements of the group, which is $2^{\frac{d-1}{2}}$. Thus, we only need to calculate the diagonal entries. We wrote $m = \mu 2^{\frac{d-1}{2}} + \delta 2^{\frac{d-3}{2}} + \gamma$ back in the previous section when we defined the representations, and this means that the upper right entry of $\phi_m(x^{2^{\frac{d+1}{2}}l} y^{2^{\frac{d-1}{2}}}) = \eta^{2^{\frac{d+1}{2}}l - \mu 2^{d+3} - \delta 2^{d+2} - \gamma 2^{\frac{d+1}{2}}}$, where η is a primitive 2^{d+3} root of unity. The exponent is 0 mod 2^{d+3} precisely when the conditions for the sum to be a multiple of the identity are met. □

The next lemma is the key to understanding the representation theoretic construction. In this lemma, we will show that the representation sum over C' will be a matrix which, when multiplied by its conjugate transpose, will be a multiple of the identity matrix. We will then show that when we combine C and C', that everything will still work. The C part can be thought of as the "abelian" part of the construction, and the C' part can be thought of as the "nonabelian" part of the construction.

LEMMA 4.3

$$\phi_m(C') = 2^{d-2}(1 + \sqrt{-1})\eta^{\alpha} \times \begin{pmatrix} \eta^2 + \eta^3 + \eta^{-2} + \eta^{2^{d+2}-3} & \eta^2 + \eta^3 - \eta^{-2} - \eta^{2^{d+2}-3} \\ \eta^2 - \eta^3 - \eta^{-2} + \eta^{2^{d+2}-3} & \eta^2 - \eta^3 + \eta^{-2} - \eta^{2^{d+2}-3} \end{pmatrix}$$

for some α.

Proof. We will only consider the case where $m = \mu 2^{\frac{d-3}{2}} + \gamma$; in other words, $\delta = 0$. The $\delta = 1$ case is similar. By the previous lemma, to calculate this representation sum, we only need consider the $D_{l,k}$ where $l = \gamma$ since that is the only case that doesn't sum to 0. Even within $D_{l,k}$ half of the set is built using $\langle x^{2^{\frac{d+1}{2}}l} y^{2^{\frac{d-1}{2}}} \rangle$, and the other half uses $\langle x^{2^{\frac{d+1}{2}}(l+2^{\frac{d-3}{2}})} y^{2^{\frac{d-1}{2}}} \rangle$, and the second subgroups sums to 0 over this representation. This implies the following calculations.

$$\phi_m(C') = \phi_m(x^{8\gamma}) \sum_{k=0}^{2^{\frac{d-1}{2}}-1} \phi_m(x^{16\gamma} y)^k \sum_{i=0}^{2^{\frac{d-3}{2}}-1} \phi_m\left(x^{i2^{\frac{d+5}{2}} + ik2^{\frac{d+1}{2}}}\right) 2^{\frac{d-1}{2}} I \times (1 + \sqrt{-1}) \begin{pmatrix} \eta^2 + \eta^3 & 0 \\ 0 & \eta^2 - \eta^3 \end{pmatrix}$$

$$+\left(\phi_m(x^{8\gamma})\sum_{k'=0}^{2^{\frac{d-1}{2}}-1}\phi_m(x^{16\gamma+2^{d+2}}y)^{k'}\sum_{i'=0}^{2^{\frac{d-3}{2}}-1}\phi_m\left(x^{i'2^{\frac{d+5}{2}}+i'k'2^{\frac{d+7}{2}}}\right)2^{\frac{d-1}{2}}I\right.$$

$$\left.\times(1+\sqrt{-1})\begin{pmatrix}\eta^{-2}+\eta^{2^{d+2}-3} & 0\\ 0 & \eta^{-2}-\eta^{2^{d+2}-3}\end{pmatrix}\right)$$

$$=2^{\frac{d-1}{2}}I(1+\sqrt{-1})\phi_m(x^{8\gamma})$$

$$\times\left(\sum_{i=0}^{2^{\frac{d-3}{2}}-1}\phi_m\left(x^{i2^{\frac{d+5}{2}}}\right)\sum_{k=0}^{2^{\frac{d-1}{2}}-1}\phi_m(x^{16\gamma}y)^k\phi_m\left(x^{ik2^{\frac{d+7}{2}}}\right)\right.$$

$$\times\begin{pmatrix}\eta^2+\eta^3 & 0\\ 0 & \eta^2-\eta^3\end{pmatrix}+\sum_{i'=0}^{2^{\frac{d-3}{2}}-1}\phi_m\left(x^{i'2^{\frac{d+5}{2}}}\right)\sum_{k'=0}^{2^{\frac{d-1}{2}}-1}\phi_m$$

$$\times(x^{2^{d+2}+16\gamma}y)^{k'}\phi_m\left(x^{i'k'2^{\frac{d+7}{2}}}\right)$$

$$\left.\times\begin{pmatrix}\eta^{-2}+\eta^{2^{d+2}-3} & 0\\ 0 & \eta^{-2}-\eta^{2^{d+2}-3}\end{pmatrix}\right)$$

If we pull out a factor of $2^{\frac{d-1}{2}}I(1+\sqrt{-1})\phi_m(x^{8\gamma})$, then we get

$$\sum_{i=0}^{2^{\frac{d-3}{2}}-1}\phi_m\left(x^{i2^{\frac{d+5}{2}}}\right)\sum_{k=0}^{2^{\frac{d-1}{2}}-1}\begin{pmatrix}\eta^{16\gamma k} & 0\\ 0 & \eta^{16\gamma k}\end{pmatrix}\begin{pmatrix}0 & \eta^{-16(\gamma+\mu 2^{\frac{d-1}{2}})}\\ \eta^{-16(\gamma+\mu 2^{\frac{d-1}{2}})} & 0\end{pmatrix}^k$$

$$\times\begin{pmatrix}\eta^{ik2^{\frac{d+7}{2}}} & 0\\ 0 & \eta^{ik2^{\frac{d+7}{2}}}\end{pmatrix}\begin{pmatrix}\eta^2+\eta^3 & 0\\ 0 & \eta^2-\eta^2\end{pmatrix}+\sum_{i'=0}^{2^{\frac{d-3}{2}}-1}\phi_m\left(x^{i'2^{\frac{d+5}{2}}}\right)$$

$$\times\sum_{k'=0}^{2^{\frac{d-1}{2}}-1}\begin{pmatrix}\eta^{(16\gamma+2^{d+2})k'} & 0\\ 0 & \eta^{(16\gamma+2^{d+2})k'}\end{pmatrix}\begin{pmatrix}0 & \eta^{-16\left(\gamma+\mu 2^{\frac{d-1}{2}}\right)}\\ \eta^{-16\left(\gamma+\mu 2^{\frac{d-1}{2}}\right)} & 0\end{pmatrix}^{k'}$$

$$\times\begin{pmatrix}\eta^{i'k'2^{\frac{d+7}{2}}} & 0\\ 0 & \eta^{i'k'2^{\frac{d+7}{2}}}\end{pmatrix}\begin{pmatrix}\eta^{-2}+\eta^{2^{d+2}-3} & 0\\ 0 & \eta^{-2}-\eta^{2^{d+2}-3}\end{pmatrix}$$

We now want to split the sum over k (and k') into two cases, k, even and k odd. The reason for doing this is that the even case involves diagonal matrices and the odd case involves off-diagonal matrices. If k is even, observe that $\eta^{2^{d+2}k}=\eta^{2^{d+3}\frac{k}{2}}=1$. Thus, we can take the sum from $i=0$ to $2^{\frac{d-3}{2}}-1$, which gives the sum (for both k and k') $\sum_{k=0}^{2^{\frac{d-3}{2}}-1}\begin{pmatrix}\eta^{32\gamma k-32k(\gamma+\mu 2^{\frac{d-1}{2}})+ik2^{\frac{d+9}{2}}} & 0\\ 0 & \eta^{32\gamma k-32k(\gamma+\mu 2^{\frac{d-1}{2}})+ik2^{\frac{d+9}{2}}}\end{pmatrix}$ $\sum_{k=0}^{2^{\frac{d-3}{2}}-1}\begin{pmatrix}\eta^{2^{\frac{d+9}{2}}(i-\mu)k} & 0\\ 0 & \eta^{2^{\frac{d+9}{2}}(i-\mu)k}\end{pmatrix}$. Since $\eta^{2^{\frac{d+9}{2}}}$ is a $2^{\frac{d-3}{2}}$ root of unity, this sum will

be 0 unless $i - \mu \cong 0 \bmod 2^{\frac{d-3}{2}}$, which only happens if $i = \mu$. In this case, the sum is $2^{\frac{d-3}{2}} I$.

Similar calculations in the k odd case show that the sum is $2^{\frac{d-3}{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ when $i = \mu$ (and 0 otherwise). The k' odd case will be $2^{\frac{d-3}{2}} \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ when $i = \mu$ (and 0 otherwise). When we combine these results, we get the following sum.

$$
\begin{aligned}
&= 2^{\frac{d-1}{2}} I(1 + \sqrt{-1})\phi_m(x^{8\gamma})\phi_m\left(x^{\mu 2^{\frac{d+5}{2}}}\right) 2^{\frac{d-3}{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \eta^2 + \eta^3 & 0 \\ 0 & \eta^2 - \eta^2 \end{pmatrix} \\
&\quad + 2^{\frac{d-1}{2}} I(1 + \sqrt{-1})\phi_m(x^{8\gamma})\phi_m\left(x^{\mu 2^{\frac{d+5}{2}}}\right) 2^{\frac{d-3}{2}} \\
&\quad \times \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \eta^{-2} + \eta^{2^{d+2}-3} & 0 \\ 0 & \eta^{-2} - \eta^{2^{d+2}-3} \end{pmatrix} \\
&= 2^{d-2}(1 + \sqrt{-1})\phi_m\left(x^{8\gamma + \mu 2^{\frac{d+5}{2}}}\right) \\
&\quad \times \begin{pmatrix} \eta^2 + \eta^3 + \eta^{-2} + \eta^{2^{d+2}-3} & \eta^2 - \eta^3 - \eta^{-2} + \eta^{2^{d+2}-3} \\ \eta^2 + \eta^3 - \eta^{-2} - \eta^{2^{d+2}-3} & \eta^2 - \eta^3 + \eta^{-2} - \eta^{2^{d+2}-3} \end{pmatrix}
\end{aligned}
$$

This proves the lemma for the $\delta = 0$ case: the $\delta = 1$ case is just as tedious! □

We still need to check that the degree 2 representations have a sum of 0 over C and the linear representations have a sum of 0 over C'. That is the purpose of the next two lemmas.

LEMMA 4.4. *For any m, $\phi_m(C) = 0$.*

Proof. The set C comes from lifting a difference set up from $Z_{2^{d+1}} \times Z_{2^{d-1}}$, and it has the property that if $c \in C$, then $x^{2^{d+2}} c \in C$ also. Thus, $\phi_m(c) + \phi_m(x^{2^{d+2}} c) = \phi_m(c)\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) = 0$. We can do this for all elements of C, so the sum is 0. □

LEMMA 4.5. *If χ is a linear representation of G that is nonprincipal on H, then $\chi(C') = 0$.*

Proof. There are 3 cases to consider here.

Case 1: χ is nonprincipal on $\langle x^{2^{\frac{d+7}{2}}} \rangle$. If χ is principal on $\langle x^{2^{\frac{d+7}{2}}} l y^{2^{\frac{d-1}{2}}} \rangle$, which is one of the subgroups used to construct $D_{l,k}$, then $\chi(D_{l,k}) = \sum_{i=0}^{2^{\frac{d-3}{2}}-1} \chi(x^{i2^{\frac{d+5}{2}} + ik2^{\frac{d+7}{2}}})\, 2^{\frac{d-1}{2}}(1 + \chi(x^{2^{d+1}}))$ (the second term of $D_{l,k}$ will be the

same argument). Note that if x is sent to a primitive 2^{d+2} root of unity, then the term $(1+\chi(x^{2^{d+1}}))$ will be 0, making the whole sum 0. Thus, we can assume that x is sent to a 2^{d+1} root of unity. Since χ is nonprincipal on the subgroup generated by $x^{2^{\frac{d+7}{2}}}$, it must also be nonprincipal on the subgroup generated by $x^{2^{\frac{d+5}{2}}}$. The summand above can be rewritten as $\chi(x^{i2^{\frac{d+5}{2}}(1+2k)})$, which is a $2^{\frac{d-3}{2}}$ root of unity not equal to 1 (when χ is nonprincipal on $x^{2^{\frac{d+7}{2}}}$). We are adding this over $2^{\frac{d-3}{2}}$ powers, so this sum is 0. Thus, in this case, $\chi(C') = 0$.

Case 2: χ is principal on $\langle x^{2^{\frac{d+7}{2}}} \rangle$ but nonprincipal on $\langle y^{2^{\frac{d-1}{2}}} \rangle$. The set C' is built by using cosets of the subgroups $\langle x^{2^{\frac{d+7}{2}}l} y^{2^{\frac{d-1}{2}}} \rangle$, and χ is nonprincipal on all of these subgroups. Therefore, it has a sum of 0 over all of C'.

Case 3: χ is principal on $\langle x^{2^{\frac{d+7}{2}}} \rangle$ and on $\langle y^{2^{\frac{d-1}{2}}} \rangle$ but is nonprincipal on $\langle x^{2^{\frac{d+3}{2}}} \rangle$. In this case, χ is principal on all of the subgroups, so $\chi(\langle x^{2^{\frac{d+7}{2}}l} y^{2^{\frac{d-1}{2}}} \rangle) = 2^{\frac{d-1}{2}}$. Thus, $\chi(D_{l,k}) = 2^{\frac{d-1}{2}}(1+\chi(x^{2^{d+1}}))((1 \pm \chi(x^{2^{\frac{d+3}{2}}})) \sum_{i=0}^{2^{\frac{d-3}{2}}-1} \chi(x^{2^{\frac{d+5}{2}}(2k+1)i}))$. If $\chi(x^{2^{\frac{d+3}{2}}}) = -1$, then $(1+\chi(x^{2^{\frac{d+3}{2}}})) = 0$ and the sum is 0. If $\chi(x^{2^{\frac{d+3}{2}}}) = \pm\sqrt{-1}$, then $\chi(x^{2^{\frac{d+5}{2}}}) = -1$, and the sum over the powers of $x^{2^{\frac{d+5}{2}}}$ will be 0.

Thus, in all of the cases, $\chi(C') = 0$. □

We have shown that all of the representation sums are what they should be except for one case: we need to show that linear representations that are principal on H but nonprincipal on G have the proper sum. In order for that sum to work out properly, we need to combine C and C': all of the other sums could be calculated separately, but this needs to be together. Thus, we define the set $D = C \cup C'$. Notice that because of the sliding of the elements that we did on C, this is a disjoint union, so the size of the set is $|D| = |C| + |C'| = 2(2^{2d-1} - 2^{d-1}) + 2^d(2^d) = 2^{2d+1} - 2^d = k$. The calculation of the sum is now the same as in the abelian case, and it is included in the next lemma.

LEMMA 4.6. *If χ is a linear representation that is principal on H but nonprincipal on G, then $|\chi(D)| = 2^d$.*

Proof. The intersection of D with every coset of H has size 2^d with one exception, and the exception has an empty intersection. Thus, the sum is $\chi(D) = 2^d \sum_{g \neq g'} \chi(g) = -2^d \chi(g')$, where the sum is over the distinct coset representatives, and g' is the representative for the one coset that is missed. □

Thus, we have shown that the set D has all of the correct representation sums. By Theorem 2.1, this implies that D is a difference set. That is the result that we have been looking for.

THEOREM 4.1. *The set D as defined above is a $(2^{2d+2}, 2^{2d+1}-2^d, 2^{2d}-2^d)$ difference set in the group defined by the following generators and relations:* $\langle x, y : x^{2^{d+3}} = y^{2^{d-1}} = 1, yxy^{-1} = x^{2^{d+2}+1}\rangle$.

All of the lemmas are done for the d odd case: the analogous lemmas will work for the d even case, and the proof of the theorem is simply the sum of the lemmas.

The significance of this result is that it shows that the exponent bound that held in the abelian case definitely does not hold in the nonabelian case. This family of difference sets provides evidence that there is a lot of work left to be done in the nonabelian 2-group case. This paper hopefully shows that the use of representation theory of these groups is a reasonable approach to attempting to construct difference sets in these groups, as well as to provide nonexistence results.

5. Examples

We do this construction for the group $G = \langle x, y : x^{64} = y^4 = 1, yxy^{-1} = x^{33}\rangle$. The outline from the last section says to first start with a difference set from $Z_{16} \times Z_4$, and lift it up to G. This will give us the set $C = (1, 0)\langle(8, 0)\rangle \cup (1, 1)\langle(16, 0), (0, 2)\rangle \cup (7, 0)\langle(8, 2)\rangle \cup \langle(16, 2)\rangle \cup (8, 0)\langle(16, 2)\rangle \cup (24, 1)\langle(16, 2)\rangle \cup (16, 1)\langle(16, 2)\rangle \cup (4, 0)\langle(0, 2)\rangle \cup (12, 0)\langle(0, 2)\rangle \cup (4, 1)\langle(0, 2)\rangle \cup (28, 1)\langle(0, 2)\rangle$. The set C' is built according to the formula in the previous section, and when we combine these, we get the difference set:

$$
\begin{aligned}
D = \{&\{1, 0\}, \{9, 0\}, \{17, 0\}, \{25, 0\}, \{33, 0\}, \{41, 0\}, \{49, 0\}, \{57, 0\},\\
&\{1, 1\}, \{17, 1\}, \{33, 1\}, \{49, 1\}, \{1, 3\}, \{17, 3\}, \{33, 3\}, \{49, 3\},\\
&\{7, 0\}, \{15, 2\}, \{23, 0\}, \{31, 2\}, \{39, 0\}, \{47, 2\}, \{55, 0\}, \{63, 2\},\\
&\{0, 0\}, \{16, 2\}, \{32, 0\}, \{48, 2\}, \{8, 0\}, \{24, 2\}, \{40, 0\}, \{56, 2\},\\
&\{24, 1\}, \{40, 3\}, \{56, 1\}, \{8, 3\}, \{16, 1\}, \{32, 3\}, \{48, 1\}, \{0, 3\},\\
&\{4, 0\}, \{4, 2\}, \{36, 0\}, \{36, 2\}, \{12, 0\}, \{12, 2\}, \{44, 0\}, \{44, 2\},\\
&\{4, 1\}, \{4, 3\}, \{36, 1\}, \{36, 3\}, \{28, 1\}, \{28, 3\}, \{60, 1\}, \{60, 3\},\\
&\{62, 0\}, \{62, 2\}, \{6, 0\}, \{38, 2\}, \{14, 0\}, \{14, 2\}, \{22, 0\}, \{54, 2\},\\
&\{29, 0\}, \{29, 2\}, \{37, 0\}, \{5, 2\}, \{45, 0\}, \{45, 2\}, \{53, 0\}, \{21, 2\},\\
&\{30, 1\}, \{30, 3\}, \{22, 1\}, \{54, 3\}, \{46, 1\}, \{46, 3\}, \{38, 1\}, \{6, 3\},\\
&\{61, 1\}, \{61, 3\}, \{53, 1\}, \{21, 3\}, \{13, 1\}, \{13, 3\}, \{5, 1\}, \{37, 3\},\\
&\{2, 0\}, \{2, 2\}, \{10, 0\}, \{42, 2\}, \{18, 0\}, \{18, 2\}, \{26, 0\}, \{58, 2\},
\end{aligned}
$$

{3, 0}, {3, 2}, {11, 0}, {43, 2}, {19, 0}, {19, 2}, {27, 0}, {59, 2}
{2, 1}, {2, 3}, {58, 1}, {26, 3}, {18, 1}, {18, 3}, {10, 1}, {42, 3},
{3, 1}, {3, 3}, {59, 1}, {27, 3}, {19, 1}, {19, 3}, {11, 1}, {43, 3}}

If the reader wants to check this using Mathematica, the set above should be defined as x, and then the following commands will show that it is a difference set:

```
f[{a_,b_},{c_,d_}]:={Mod[a - (33 ^ (Abs[b-d]))c,64],Mod[b-d,4]}
s = Table[f[x[[i]],x[[j]]],{i,1,120},{j,1,120}];
Table[Count[s,{i,j},2],{i,0,63},{j,0,3}]
```

By slightly modifying this construction, we were able to find a difference set in the group $\langle x, y | x^{64} = y^4 = 1, yxy^{-1} = x^{17} \rangle$. The set is:

D = {{1,0}, {17, 0}, {33, 0}, {49, 0}, {1, 2}, {17, 2}, {33, 2}, {49, 2},
{7, 0}, {23, 1}, {39, 2}, {55, 3}, {39, 0}, {55, 1}, {7, 2}, {23, 3}
{9, 0}, {9, 1}, {9, 2}, {9, 3}, {41, 0}, {41, 1}, {41, 2}, {41, 3},
{0, 0}, {16, 0}, {32, 0}, {48, 0}, {0, 1}, {16, 1}, {32, 1}, {48, 1},
{8, 1}, {24, 1}, {40, 1}, {56, 1}, {8, 2}, {24, 2}, {40, 2}, {56, 2},
{4, 0}, {20, 2}, {36, 0}, {52, 2}, {4, 1}, {20, 3}, {36, 1}, {52, 3},
{12, 3}, {28, 1}, {44, 3}, {60, 1}, {28, 0}, {44, 2}, {60, 0}, {12, 2},
{10, 0}, {26, 1}, {42, 2}, {58, 3}, {26, 0}, {42, 1}, {58, 2}, {10, 3},
{11, 0}, {27, 1}, {43, 2}, {59, 3}, {27, 0}, {43, 1}, {59, 2}, {11, 3},
{2, 0}, {18, 3}, {34, 2}, {50, 1}, {18, 0}, {34, 3}, {50, 2}, {2, 1},
{3, 0}, {19, 3}, {35, 2}, {51, 1}, {19, 0}, {35, 3}, {51, 2}, {3, 1},
{6, 0}, {6, 1}, {6, 2}, {6, 3}, {22, 0}, {22, 1}, {22, 2}, {22, 3},
{37, 0}, {37, 1}, {37, 2}, {37, 3}, {53, 0}, {53, 1}, {53, 2}, {53, 3},
{62, 0}, {30, 1}, {62, 2}, {30, 3}, {14, 0}, {46, 1}, {14, 2}, {46, 3},
{29, 0}, {61, 1}, {29, 2}, {61, 3}, {45, 0}, {13, 1}, {45, 2}, {13, 3}}

This difference set will clearly be the model for an infinite family of difference sets in groups of the form $\langle x, y | x^{2^{d+3}} = y^{2^{d-1}} = 1, yxy^{-1} = x^{2^{d+1}+1} \rangle$. In order to argue this, we would need to find the technical lemma similar to Lemma 2.1, and then build up the C and C' parts of the difference sets (we have not done this). This leads to a few questions:

1. Can the exponent bound to extended higher than 2^{d+3} for other nonabelian groups?
2. Are there any nonexistence results for 2-groups other than the exponent bound and the dihedral trick?
3. Can these representation theoretic techniques be used to construct other nonabelian difference sets?

References

1. M. Aschbacher, *Finite Group Theory*, Cambridge University Press, Cambridge, England, 1986.
2. C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley and Sons, New York, NY, 1988.
3. J.A. Davis, "Difference sets in abelian 2-groups," *J. Combin. Theory Series A* **57** (1991), 262–286.
4. J.A. Davis, "A generalization of Kraemer's result on difference sets," *J. Combin. Theory Series A,* **57** (1991), 187–192.
5. J.A. Davis, "A note on nonabelian (64, 28, 12) difference sets," *Ars Combin.,* to appear.
6. J.F. Dillon, "Variations on a scheme of McFarland for noncyclic difference sets," *J. Combin. Theory Series A*, **40** (1980), 9–21.
7. J.F. Dillon, "A survey of difference sets in z-groups," in *Coding Theory, Design Theory, Group Theory: Proc. of the Marshall Hall Conf.,* Dieter Jungnickel, ed. John Wiley & Sons, 1992.
8. J. Jedwab, "Perfect arrays, Barker arrays and difference sets," Ph.D. thesis, University of London, London, England, 1991.
9. R.E. Kibler, "A summary of noncyclic difference sets, $k < 20$," *J. Combin. Theory Series A* **25** (1978), 62–67.
10. R. Kraemer, "A result on Hadamard difference sets," *J. Combin. Theory Series A* **63** (1993), 1–10.
11. E.S. Lander, *Symmetric Designs: an Algebraic Approach,* London Mathematical Society Lecture Notes Series 74, Cambridge University Press, Cambridge, England, 1983.
12. W. Ledermann, *Introduction to Group Characters,* Cambridge University Press, Cambridge, England, 1977.
13. R.A. Liebler, "The inversion formula," *J. Combin. Math. and Combin. Computing* **13** (1993), 143–160.
14. R.A. Liebler and K. Smith, "On difference sets in certain 2-groups," in *Coding Theory, Design Theory, Group Theory: Proc. of the Marshall Hall Conf.,* Dieter Jungnickel, ed. John Wiley & Sons, 1992.
15. S.L. Ma, "Partial difference triples," Submitted.
16. R.L. McFarland, "A family of difference sets in noncyclic groups," *J. Combin. Theory Series A* **15** (1973), 1–10.
17. R.J. Turyn, "Character sums and difference sets," *Pacific J. Math.* **15** (1965), 319–346.