1-1-1998

Hadamard Difference Sets in Nonabelian 2-Groups with High Exponent

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

Joel E. Iiams

JOURNAL OF ALGEBRA **199,** 62–87 (1998)
ARTICLE NO. JA977197

Hadamard Difference Sets in Nonabelian 2-Groups with High Exponent

James A. Davis*

Department of Mathematics, University of Richmond, Richmond, Virginia 23173

and

Joel E. Iiams

Department of Mathematics, University of North Dakota, Grand Forks, North Dakota 58202

Communicated by Walter Feit

Received July 31, 1996

Nontrivial difference sets in groups of order a power of 2 are part of the family of difference sets called Hadamard difference sets. In the abelian case, a group of order 2^{2t+2} has a difference set if and only if the exponent of the group is less than or equal to 2^{t+2}. In a previous work (R. A. Liebler and K. W. Smith, *in* "Coding Theory, Design Theory, Group Theory: Proc. of the Marshall Hall Conf.," Wiley, New York, 1992), the authors constructed 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^{4t+2} with exponent 2^{3t+2}. Thus a nonabelian 2-group G with a Hadamard difference set can have exponent $|G|^{3/4}$ asymptotically. Previously the highest known exponent of a nonabelian 2-group with a Hadamard difference set was $|G|^{1/2}$ asymptotically. We use representation theory to prove that the group has a difference set.

1. INTRODUCTION

Let G be a multiplicative group of order v and D be a k-subset of G; then D is called a $(v, k, \lambda; n)$-*difference set* in G provided that the differences dd'^{-1} for $d, d' \in D$, $d \neq d'$ contain every nonidentity element

* The author thanks Hewlett–Packard for their generous support during his sabbatical year 1995–1996. This work is also partially supported by NSA Grant MDA 904-94-H-3057.

0021-8693/98 $25.00

of G exactly λ times. The parameter $n = k - \lambda$ is included in the list of parameters for future convenience. Difference sets are equivalent to symmetric designs with regular automorphism groups: see [12] for background on difference sets. We shall consider $(2^{2t+2}, 2^{2t+1} \pm 2^t, 2^{2t} \pm 2^t; 2^{2t})$-difference sets (known as *Hadamard*, or alternatively as *Menon*, difference sets). In the abelian case, the existence question was completely answered by the following theorem due to Kraemer [11], Jedwab [9], and Turyn [18].

THEOREM 1.1. *An abelian 2-group G of order 2^{2t+2} has a Hadamard difference set if and only if the exponent of the group is less than or equal to 2^{t+2}.*

The nonabelian case has also been studied, and there are both existence and nonexistence results. McFarland [17] provided a construction that was generalized by Dillon [7], and they both have applications in nonabelian groups. Davis [4] showed how the constructions that solved the abelian case can be generalized to include some nonabelian cases. Davis and Smith [6] showed that the example in Liebler and Smith [15] could be extended to an infinite family of difference sets in groups of order 2^{2t+2} and exponent 2^{t+3}, thus exceeding the exponent bound from the abelian case. As for nonexistence, there are two known results. The first one is due to Turyn [18].

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

The second result, generalized by Ma [16], is due to Dillon [7].

THEOREM 1.3. *Let G be a 2-group of order 2^{2t+2}, and H a normal subgroup so that G/H is dihedral. If $|H| < 2^t$, then G does not have a Hadamard difference set.*

Existence of Hadamard difference sets has been exhaustively studied for groups of order 16 [10] and groups of order 64 [8]. In both cases Theorems 1.2 and 1.3 prove sufficient as well as necessary.

The aim of this paper is to construct difference sets, similar to the Liebler and Smith example, in groups of very high exponent. In particular, we will construct a $(2^{4t+2}, 2^{4t+1} - 2^{2t}, 2^{4t} - 2^{2t}, 2^{4t})$-difference set in the group

$$G_t = \langle x, y \mid x^{2^{3t+2}} = y^{2^t} = 1, yxy^{-1} = x^{2^{2t+2}+1} \rangle, \qquad \text{for any } t \geq 1.$$

Note that G_t has no dihedral quotient group, and its largest cyclic quotient group has order 2^{2t}, and is formed modulo the subgroup $H = \langle x^{2^{2t+2}}, y \rangle$.

The size of H is the boundary value for the cyclic nonexistence condition. By constructing a difference set in G_t, we demonstrate that asymptotically the exponent of a 2-group with a Hadamard difference set can be $|G|^{3/4}$, where $|G|$ is the order of G. Previously the highest known exponent was $|G|^{1/2}$ asymptotically.

In order to build the difference set, we first translate our problem from a combinatorial one to an algebraic one—we abuse notation by equating a subset of the group with the sum of its elements in the group ring. A difference set is then an element of the integral group ring with coefficients 0 and 1 which satisfies a certain equation for every irreducible representation in a decomposition of the right regular representation. This is discussed in more detail in Section 2.

The third section provides the background for constructing one subset $D_{2^j,b}$ of G for every conjugacy class $C = \Phi_{2^j,b}$ of nonlinear irreducible representations.

In Section 4 we show that each subset $D_{2^j,b}$ has the added property that it is annihilated by any nontrivial irreducible representation in our decomposition of $\mathbb{Z}G$ which is not in C. Also the union, P, of these subsets is shown to be a disjoint union (since we want a difference set and not a difference multiset). Finally the linear (degree 1) irreducible representations for G_t are dealt with. Specifically we construct a subset L of G_t, which is disjoint from P, using the K-matrix construction of Davis [3], and a scheme of McFarland [17]. L is annihilated by any nonlinear irreducible representation of G_t.

As a consequence we prove

THEOREM 4.1. *The set* $D := P \cup L$ *is a Hadamard difference set in* G_t *with parameters* $(2^{4t+2}, 2^{2t}(2^{2t+1} - 1), 2^{2t}(2^{2t} - 1); 2^{4t})$.

Naturally there is quite a bit of combinatorial bookkeeping to be done. To help with this our difference set is broken down into subsets of cosets of the subgroup $H_t := \langle x^{2t+1}, y \rangle$ of order $|G_t|^{1/2}$. There are 2^{2t+1} cosets of H_t in G_t. One of the cosets will have an empty intersection with the difference set. All of the other cosets will intersect the difference set in a subset with 2^{2t} elements. Each subset is in turn a union of cosets of subgroups of H_t.

The final section gives examples of difference sets in a group of order 1024 and exponent 256 as well as a group of order 16,384 and exponent 2048.

The only known nonexistence results for Hadamard difference sets in 2-groups are Theorems 1.2 and 1.3. Our result lends credence to the

Conjecture 1.1. Theorems 1.2 and 1.3 are sufficient as well as necessary.

The authors gratefully acknowledge many helpful suggestions from the referee.

2. REPRESENTATION THEORETIC PRELIMINARIES

Consider the group ring $\mathbb{Z}G$. 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 a homomorphism from G to $GL(m, \mathbb{C})$, the multiplicative group of $m \times m$ matrices over $\mathbb{C}$. The degree of the representation is m. 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 $\mathbb{Z}G$ to $M_{m \times m}(\mathbb{C})$, the ring of all $m \times m$ matrices over $\mathbb{C}$. We will use the notation $\phi(A) = \sum_{a \in A} \phi(a)$, where ϕ is a representation and A is a subset of G. This is known as a representation sum of the subset. Note that G (the group ring element that is the sum of the elements of G) is in the center of the complex group algebra $\mathbb{C}G$. Thus for any irreducible representation ϕ of G, we have that $\phi(G)$ is in the center of $M_{m \times m}(\mathbb{C})$. Hence $\phi(G)$ is a scalar matrix. A representation ϕ is called *nontrivial* if there is an $x \in G$ with $\phi(x) \neq I_m$, where I_m is the $m \times m$ identity matrix and m is the degree of ϕ. When ϕ is a nontrivial irreducible representation for G and $\phi(x) \neq I_m$, then $\phi(G) = \phi(xG) = \phi(x)\phi(G)$ implies that $\phi(G) = 0$.

To generalize this slightly, for any subgroup H of G the restriction of ϕ to H is a representation of H. Let $h \in H$ generate a normal cyclic subgroup of H. Then if $\phi \mid_H (h) \neq I_m$ and ϕ does not have the trivial representation of H as a direct summand, then we also get $\phi(H) = 0$. We will use this property extensively in Section 4 by displaying an element h of a particular subgroup H. The existence of h with the above property will ensure that the representation sum over the subgroup will be zero. For more background on representation theory see [2].

If we apply an irreducible nontrivial representation ϕ to the difference set equation, we get

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

This fact and the next theorem explain why we want to look at representation sums over D.

THEOREM 2.1. *Let D be a subset of size k of a group G. Let S be a complete set of distinct, inequivalent, nontrivial, irreducible representations for G. If $\phi(D)\phi(D^{(-1)}) = nI_m$ for all $\phi \in S$, then D is a $(v, k, \lambda; n)$-difference set in G.*

Proof. Any subset D of G is completely determined by its image under the regular representation. The regular representation decomposes as the direct sum of a complete set of distinct, inequivalent, irreducible representations for G. Since D has size k, D satisfies the difference set equation for the trivial representation. If in addition, D satisfies the difference set equation for all $\phi \in S$, then D satisfies the difference set equation for the right regular representation. Therefore D is a difference set (see [13]). ∎

In the following sections, our strategy will be to use this result to build the difference set a piece at a time. We will find a subset of the group which will give us the correct representation sum for every representation of a certain degree, and then we will show that the pieces put together have the correct representation sum.

As mentioned in the Introduction, we will be working with the group G_t defined as $G_t = \langle x, y \mid x^{2^{3t+2}} = y^{2^t} = 1, yxy^{-1} = x^{2^{2t+2}+1} \rangle$. In order to list the irreducible representations on this group, we need to establish some notation. All irreducible representations are induced from characters on the cyclic normal subgroup of order 2^{3t+2}, so we need to list the characters of this subgroup.

Let $C_{2^u} = \langle z \rangle$ be the cyclic group or order 2^u. Define $\chi(z) = e^{2\pi i/2^u}$. All characters of C_{2^u} are of the form $\chi^l(z) := (\chi(z))^l$, where $l = 0, 1, \ldots, 2^u - 1$. When l is even, χ^l is nonfaithful and can be viewed as a character of the cyclic group of order 2^{u-1}. Define F_{2^u} to be the character table of C_{2^u}. The rows of F_{2^u} are indexed by the characters. We first list the rows corresponding to the nonfaithful characters. We order these inductively as characters of $C_{2^{u-1}}$. Then we list the rows labeled by χ, χ^3, $\chi^5, \ldots, \chi^{2^u-1}$. The columns are indexed by group elements. The group elements can be ordered in such a way that the first 2^{u-1} rows of F_{2^u} form two copies of $F_{2^{u-1}}$ next to each other.

Now let η be a primitive 2^s root of unity, and let $t \leq s - 2$. For each $j = 0, 1, \ldots, t$, form the number ring $\mathbb{Z}[\eta^{2^j}]$. We induce an automorphism σ_j of order 2^{t-j} on $\mathbb{Z}[\eta^{2^j}]$ by $\eta^{\sigma_j} = \eta^{2^{s-(t-j)}+1}$. We use σ_j to define an algebra R_{t-j} of $2^{t-j} \times 2^{t-j}$ matrices generated by matrices B whose first row is the vector $(b_0, b_1, \ldots, b_{2^{t-j}-1})$ and whose (i, k) entry is $b_{k-i}^{\sigma_i}$, where $k - i$ is read modulo 2^{t-j}, and $b_0, b_1, \ldots, b_{2^{t-j}-1} \in \mathbb{Z}[\eta^{2^j}]$. For conve-

nience, we will use the notation $m(b_0, b_1, \ldots, b_{2^{t-j}-1})$ for the matrix B, that is,

$$m(b_0, b_1, \ldots, b_{2^{t-j}-1}) = B = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{2^{t-j}-1} \\ b_{2^{t-j}-1}^{\sigma_j} & b_0^{\sigma_j} & b_1^{\sigma_j} & \cdots & b_{2^{t-j}-2}^{\sigma_j} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_1^{\sigma_j^{2^{j-1}}} & b_2^{\sigma_j^{2^{j-1}}} & b_3^{\sigma_j^{2^{j-1}}} & \cdots & b_0^{\sigma_j^{2^{j-1}}} \end{pmatrix}.$$

If the matrix is of the form $m(b, 0, \ldots, 0)$, we will write it as $m_{2^{t-j}}(b)$ for $b \in \mathbb{Z}[\eta^{2^j}]$. Finally, the automorphism $\sigma_j^{2^{t-j-1}}$ on $\mathbb{Z}[\eta^{2^j}]$ will be denoted by τ_j.

Let $\mathbf{a}_l = (a_{l,0}, a_{l,1}, \ldots, a_{l,2^u-1})$ denote the lth row of F_{2^u}. We then define $E_l := m(a_{l,0}, a_{l,1}, \ldots, a_{l,2^u-1})$. By character orthogonality, $E_i E_k = \delta_{ik} 2^u E_k$. We also note that $\overline{E}_i^T = E_i$ (as long as $u \le s/2$).

With the notation established, we are now in a position to define a complete set of distinct, inequivalent, irreducible representations for our groups G_t. All of our representations are induced from linear representations of $K := \langle x \rangle$.

We let η be a 2^{3t+2}nd root of unity. When a linear character of K sends x to an odd power of η, the resulting induced representation ϕ is of degree 2^t. We can define ϕ simply by presenting the images of x and y. The following lemma describes all irreducible representations of degree 2^t.

LEMMA 2.1. *The set of inequivalent irreducible representations of degree* 2^t *is*

$$\Phi_{2^t,0} = \Big\{ (\phi)^{2f+1} \mid \phi(x) = m_{2^t}(\eta),\ \phi(y) = \eta^{2^{2t+2+k}(2i+1)} m(0,1,0,\ldots,0),$$
$$k = 1, \ldots, t;\ i = 0, 1, \ldots, 2^{t-k} - 1,\ i = 0 \text{ when } k = 0 \Big\},$$

where $0 \le f \le 2^{3t+1} - 1$, *and* ϕ^{2f+1} *denotes replacing* η *by* η^{2f+1}.

Up to replacing y by $x^{-2^{2t+2+k}(2i+1)} y$ we can take $\phi(y) = m(0,1,0,\ldots,0)$. Also ϕ is equivalent to ϕ^{2f+1} whenever $\eta^{2f+1} = \eta^{\sigma_0^e}$ for any power e. Since $\eta^{\sigma_0} = \eta^{2^{2t+2}+1}$, we have that the first 2^{2t+1} values of f run through all the inequivalent representations in this set. Thus $\Phi_{2^t,0}$ contains 2^{2t+1} distinct, inequivalent representations. These cover $(2^t)^2 2^{2t+1} = 2^{4t+1}$ dimensions of the group ring.

In general, there will be 2^j conjugacy classes of irreducible representations of degree 2^{t-j}. We will use two subscripts to describe each class of irreducible representations. The first subscript will be the degree of a representation. The second subscript will indicate which conjugacy class the representation belongs to. The second subscript, b, will have values

ranging from 0 to $2^j - 1$. For convenience we will write $b = 2^\alpha\beta$ where $0 \le \alpha \le j-1$ and $\beta \in \{1, 3, \dots, 2^{j-\alpha} - 1\}$. We make the convention that the $b = 0$ case corresponds to $\alpha = j$ and $\beta = 1$. When a linear character of K sends x to an odd power of η^{2^j} the resulting induced representations will have degree 2^{t-j}. These classes of representations are listed in the following lemma.

LEMMA 2.2. *The inequivalent irreducible representations of degree* $2 \le m < 2^t$ *are contained in conjugacy classes of the form*

$$\Phi_{2^{t-j},2^\alpha\beta} = \Big\{(\phi)^{2f+1} \mid \phi(x) = m_{2^{t-j}}\big(\eta^{2^j}\big),$$
$$\phi(y) = \big(\eta^{e(2^\alpha\beta)}\big)m(0,1,0,\dots,0)$$
$$e(2^\alpha\beta) = 2^{2t+2+\alpha}\big(2^{j-\alpha+1}i + (\beta + n2^{j-\alpha})\big),$$
$$i = 0,1,\dots,2^{t-j-1} - 1,$$
$$0 \le \alpha \le j-1,\ \beta \in \{1,3,5,\dots,2^\alpha - 1\},\ n = 0,1\}$$

$$\Phi_{2^{t-j},0} = \Big\{(\phi)^{2f+1} \mid \phi(x) = m_{2^{t-j}}\big(\eta^{2^j}\big),\ \phi(y) = \big(\eta^{e(0)}\big)m(0,1,0,\dots,0)$$
$$e(0) = 2^{2t+2+j}\big(2i + (1+n)\big),$$
$$i = 0,1,\dots,2^{t-j-1} - 1, n = 0,1\}.$$

where $0 \le f \le 2^{3t+1-j} - 1$ *for each* $\Phi_{2^{t-j},b}$.

As before, the inequivalent representations in these sets use the first 2^{2t+1} values of f. Thus, each set uses up $(2^{t-j})^2 \cdot 2^{2t+1} = 2^{4t+1-2j}$ dimensions of the group ring, and there are 2^j classes. The degree 2^{t-j} representations collectively account for 2^{4t+1-j} dimensions of the regular representation, half as many as the degree 2^{t-j+1} representations.

Lastly, when $j = t$ we get the linear representations for G_t which are defined in the following lemma.

LEMMA 2.3. *The inequivalent linear representations have the form*

$$\chi_{m,\alpha,\beta}(x) = \big(\eta^{2^t}\big)^m, \qquad \chi_{m,\alpha,\beta}(y) = \big(\eta^{2^{2t+2}}\big)^{2^\alpha\beta},$$

for $0 \le m \le 2^{2t+2} - 1$, $0 \le 2^\alpha\beta \le 2^t - 1$, $\beta = 1,3,\dots,2^{t-\alpha} - 1$.

By Theorem 2.1 if we can find a subset of G_t so that the representation sum over the subset times its conjugate transpose is 2^{4t} times the identity, and this is true for every nontrivial, inequivalent, irreducible representation, then the subset will be a difference set. The next section includes several technical lemmas that will be used both to help in determining the

elements to include in the subset as well as to ultimately prove that the subset has the appropriate representation sum in all cases.

3. KEY LEMMAS

Let $s = 3t + 2$, for $t \geq 1$ and $0 \leq j \leq t$. The ring R_{t-j} is the image of $\mathbb{Z}G_t$ in $M_{2^{t-j}\times 2^{t-j}}(\mathbb{C})$ under $\phi \in \Phi_{2^{t-j},b}$ for some $0 \leq b \leq 2^j - 1$. The following three lemmas display a method for generating a possible image of a difference set under ϕ. The first lemma constructs an element of $\mathbb{Z}[\eta^{2^j}]$ which satisfies a number theoretic equation: the fact that such an element exists is a crucial step in the construction of a difference set in G_t.

LEMMA 3.1. *Let η be a primitive 2^snd root of unity and let a_k and d_k be integers for $1 \leq k$. Let $\lambda_1 = \mu_1 = 1$, $\gamma_1 = (\lambda_1 + \eta^{2d_1+1}\mu_1)\eta^{a_1}$. Also, for l an integer, let $\xi_2 = \sqrt{-1}\,\eta^{2^l}$, and for $k > 2$, let $\xi_k = \sqrt{\xi_{k-1}}$. Finally for $k \geq 2$ define the three quantities $\lambda_k = \lambda_{k-1} + \xi_k\,\mu_{k-1}$, $\mu_k = -\lambda_{k-1} + \xi_k\,\mu_{k-1}$, and $\gamma_k = (\lambda_k + \eta^{2d_k+1}\mu_k)\eta^{a_k}$. Then as long as $k \leq l + 2$, $\gamma_k\overline{\gamma_k} + (\gamma_k\overline{\gamma_k})^{\tau_j} = 2^{k+1}$.*

Proof. We show by induction that $\lambda_k\overline{\lambda_k} + \mu_k\overline{\mu_k} = 2^k$. The $k = 1$ case is obvious, so suppose that the claim is true for $k - 1$.

$$\lambda_k\overline{\lambda_k} = \lambda_{k-1}\,\overline{\lambda_{k-1}} + \mu_{k-1}\,\overline{\mu_{k-1}} + \xi_k\,\mu_{k-1}\,\overline{\lambda_{k-1}} + \overline{\xi_k\mu_{k-1}}\lambda_{k-1}$$

and

$$\mu_k\overline{\mu_k} = \lambda_{k-1}\,\overline{\lambda_{k-1}} + \mu_{k-1}\,\overline{\mu_{k-1}} - \xi_k\,\mu_{k-1}\,\overline{\lambda_{k-1}} - \overline{\xi_k\mu_{k-1}}\lambda_{k-1}.$$

So

$$\lambda_k\overline{\lambda_k} + \mu_k\overline{\mu_k} = 2\big(\lambda_{k-1}\,\overline{\lambda_{k-1}} + \mu_{k-1}\,\overline{\mu_{k-1}}\big) = 2\big(2^{k-1}\big) = 2^k.$$

The lemma follows a similar argument, using the fact that τ_j sends any odd power of η to its negative. We only need $k \leq l + 2$ so that the kth root of ξ_2 still lies in $Z[\eta]$. ∎

In order to apply this lemma, let $s = 3t + 2$, $l = 2t + j$, $k = 2t - 2j - 1$, $a_k = 2^{j+1}$, and $d_k = 2^j - 1$. Put $\zeta_k = \eta^{2^{s-k}}\eta^{2^{t-k+2}}$. Then the expression

$$\lambda_k = \sum_{m=0}^{2^{k-1}-1} (-1)^{q_k(m)}\zeta_k^m$$

defines a binary string q_k whose mth entry is $q_k(m)$, where λ_k is the element defined in Lemma 3.1. Similarly

$$\mu_k = \sum_{m=0}^{2^{k-1}-1} (-1)^{r(m)}\zeta_k^m$$

defines r_k, where μ_k is the element defined in Lemma 3.1. Recursively $q_1 = r_1 = 0$, $q_2 = 00$, $r_2 = 10$, and for $k \geq 3$,

(i) $q_k(m) = q_{k-1}(m/2)$, $m = 0, 2, \ldots, 2^{k-1} - 2$.
(ii) $q_k(m) = r_{k-1}((m-1)/2)$, $m = 1, 3, \ldots, 2^{k-1} - 1$.
(iii) $r_k(m) = 1 + q_{k-1}(m/2)$ modulo 2, $m = 0, 2, \ldots, 2^{k-1} - 2$.
(iv) $r_k(m) = r_{k-1}((m-1)/2)$, $m = 1, 3, \ldots, 2^{k-1} - 1$.

We now define two elements of $\mathbb{Z}G_t$ whose representation sums have terms that match γ_k from Lemma 3.1. Let $h = 2^{3t+1-j}$ and $l = 2^{j+1} - 1$. We set

$$A_{2^{t-j}} = x^{2^{j+1}} \left\{ \sum_{m=0}^{2^{k-1}-1} \left[(x^h)^{q_k(m)} + x^l (x^h)^{r_k(m)} \right] \left(x^{2^{t+3+j} + 2^{3+2j}} \right)^m \right\}$$

and

$$B_{2^{t-j}} = x^{-2^{j+1}} \left\{ \sum_{m=0}^{2^{k-1}-1} \left[(x^{-h})^{q_k(m)} + x^{-h-l} (x^{-h})^{r_k(m)} \right] \left(x^{-(2^{t+3+j} + 2^{3+2j})} \right)^m \right\}.$$

LEMMA 3.2. *Let $A_{2^{t-j}}$ and $B_{2^{t-j}}$ be defined as above. Then $A_{2^{t-j}}$ and $B_{2^{t-j}}$ each consist of $2^{2t-2j-1}$ distinct powers of x. Moreover the exponent of any power of x in $A_{2^{t-j}}$ is congruent to 2^{j+1} or $2^{j+2} - 1$ modulo 2^{3+2j}, while the exponent of any power of x in $B_{2^{t-j}}$ is congruent to -2^{j+1} or $-(2^{j+2} - 1)$ modulo 2^{3+2j}.*

Proof. Let ζ be a primitive 2^{3t+2}nd root of unity, and χ a character of $\langle x \rangle$ so that $\chi(x) = \zeta^{2^j} = \eta$. Then $\chi(A_{2^{t-j}}) = \gamma_{2t-2j-1}$ and $\chi(B_{2^{t-j}}) = \overline{\gamma_{2t-2j-1}}^{\tau_j}$, as in Lemma 3.1. By construction, $\gamma_{2t-2j-1}$ consists of $2^{2t-2j-1}$ distinct roots of unity, for our specific choices of s, l, and k. The moreover part is obvious by inspection. ∎

When $0 \leq j < t$, a character χ as in the proof of the previous lemma induces an irreducible representation ϕ for G_t of degree 2^{t-j}. By Lemma 3.1,

$$\phi(A_{2^{t-j}})\overline{\phi(A_{2^{t-j}})} + \phi(B_{2^{t-j}})\overline{\phi(B_{2^{t-j}})} = 2^{2t-2j} I_{2^{t-j}}.$$

It is important to note that $A_{2^{t-j}}$ and $B_{2^{t-j}}$ denote subsets of G_t. The following lemma demonstrates that the combination of the representation values for A_{2^u} and B_{2^u} together with matrices associated to the character table F_{2^u} will satisfy a matrix equation. This matrix equation will be used in the next section to show that certain subsets can be used to construct a difference set in G_t.

LEMMA 3.3. *Let γ_k be as in Lemma* 3.1. *Let z generate the cyclic group of order 2^u and let χ^l be the lth character of C_{2^u}. Let $c_i = (\eta^{2^{s-u}})^{e_i}\gamma_k$ for $i = 0, 1, \ldots, 2^{u-1} - 1$, $e_i \in \mathbb{Z}$, and $c_i = (\eta^{2^{s-u}})^{e_i}(\overline{\gamma_k})^{\tau_j}$ for $i = 2^{u-1}, 2^{u-1} + 1, \ldots, 2^u - 1$, $e_i \in \mathbb{Z}$. If $u \le s/2$, and $S = \sum_{i=0}^{2^u-1} m_{2^u}(c_i)E_i$, then $S\overline{S}^T = 2^{2u+k}I_{2^u}$.*

Proof. We freely use the orthogonality properties for the character table of a group.

$$
\begin{aligned}
S\overline{S}^T &= \sum_{i=0}^{2^u-1} m_{2^u}(c_i)E_i \sum_{i=0}^{2^u-1} E_i m_{2^u}(\overline{c_i}) \\
&= 2^u \sum_{i=0}^{2^u-1} m_{2^u}(c_i)E_i m_{2^u}(\overline{c_i}) \\
&= 2^u \Bigg[m\Bigg(\gamma_k\overline{\gamma_k} \sum_{l=0}^{2^{u-1}-1} \chi^l(z^0), \ldots, \gamma_k\overline{\gamma_k}^{\sigma^{2^u}-1} \sum_{l=0}^{2^{u-1}-1} \chi^l(z^{2^{u-1}})\Bigg) \\
&\qquad + m\Bigg(\overline{\gamma_k}^{\tau_j}\gamma_k^{\tau_j} \sum_{l=2^{u-1}}^{2^u-1} \chi^l(z^0), \ldots, \overline{\gamma_k}^{\tau_j}\gamma_k^{\tau_j\sigma^{2^{t-1}}} \sum_{l=2^{u-1}}^{2^u-1} \chi^l(z^{2^{u-1}})\Bigg)\Bigg] \\
&= 2^u \Big[m\big(2^{u-1}\gamma_k\overline{\gamma_k}, 0, \ldots, 0, 2^{u-1}\gamma_k\overline{\gamma_k}^{\tau_j}, 0, \ldots, 0\big) \\
&\qquad + m\big(2^{u-1}\overline{\gamma_k}^{\tau_j}\gamma_k^{\tau_j}, 0, \ldots, 0, -2^{u-1}\overline{\gamma_k}^{\tau_j}\gamma_k, 0, \ldots, 0\big)\Big] \\
&= 2^u m_{2^u}\Big(2^{u-1}\big(\gamma_k\overline{\gamma_k} + (\gamma_k\overline{\gamma_k})^{\tau_j}\big)\Big) \\
&= 2^{2u+k}I_{2^u}.
\end{aligned}
$$

The last equality comes from the first lemma. ∎

Note that $A = (1 + \sqrt{-1})S$ satisfies $A\overline{A}^T = 2^{2u+k+1}I_{2^u}$.

4. CONSTRUCTION

Recall that $G_t = \langle x, y \mid x^{2^{3t+2}} = y^{2^t} = 1, yxy^{-1} = x^{2^{2t+2}+1}\rangle$ and define the subgroup $H_t = \langle x^{2^{2t+1}}, y\rangle$. We will define a subset D of G_t with the property that every coset of H_t intersects D in 2^{2t} elements with one exception which has empty intersection. The subset D will be the difference set in G_t. We will show that it is a difference set by using representation theory together with the lemmas proved in the previous section.

We construct D by building a subset B of G for each conjugacy class C of irreducible representations for G_t, where each $\phi \in C$ is nontrivial on H_t. These subsets are shown to be pairwise disjoint. We also show that they have the special properties that $\phi(D) = \phi(B)$ and $\phi(B)\overline{\phi(B)}^T = 2^{4t}I$. In other words, ϕ annihilates $D - B$. Moreover B (and therefore D) satisfies the difference set equation with respect to ϕ.

Since all but one coset of H_t in G_t intersects D in 2^{2t} elements, any nontrivial character χ of G_t which is principal on H_t satisfies $|\chi(D)| = 2^{2t}$ [17]. Thus D satisfies the difference set equation with respect to χ.

In the first subsection we concentrate on the nonlinear irreducible representations for G_t. Since each piece will be associated to a particular conjugacy class of nonlinear representations, we will label a piece $D_{2^{t-j},b}$ if it is associated to the conjugacy class of representations $\Phi_{2^{t-j},b}$.

In the second subsection we deal with the linear representations for G_t which are nonprincipal on H_t. The corresponding subsets are known as K-matrices in the literature [3].

In the final subsection we prove the main theorem using Theorem 2.1 and the results from the previous subsections.

4.1. *The Nonlinear Pieces*

In this subsection we use Lemmas 3.2 and 3.3 to help build the pieces of our difference set which correspond to conjugacy classes of nonlinear irreducible representations for G_t. First, we list the pieces. Next, we prove that the union of the pieces is a set. Finally, we show that the representation sums are correct.

For the single conjugacy class of irreducible degree 2^t representations for G_t we set $k = 2t - 1$ in Lemma 3.1. We also select $a_{2t-1} = 2$ and $d_{2t-1} = 0$. Set $h = 2t + 1$. Then the degree 2^t piece of our difference set is

$$D_{2^t,0} = (1 + x^{2^{3t}})\left[A_{2^t}\sum_{i=0}^{2^{t-1}-1}(x^{2^h})^i\langle x^{-2^{2t+3}i}y\rangle + B_{2^t}\sum_{i=0}^{2^{t-1}-1}(x^{2^h})^i\langle x^{-2^{2t+2}(2i+1)}y\rangle\right].$$

We have written this as an element of the group ring, and we first need to establish that this group ring element is associated to a subset of G_t: namely, we need to show that $D_{2^t,0}$ has only 0 and 1 for coefficients.

LEMMA 4.1. *The group ring element $D_{2^t,0}$ is associated to a subset of G_t.*

Proof. In the definition of $D_{2^t,0}$, the expressions A_{2^t} and B_{2^t} consist of distinct powers of x which lie in distinct cosets of H_t. These obviously

won't overlap. So suppose there are elements from different cosets which are the same group element. Because all of the subgroups are generated by elements of the form $x^{-2^{2t+3}i}y$ (the $x^{-2^{2t+2}(2i+1)}y$ case is similar) and the powers of y must be the same, the two elements are of the form $(x^{2^{2t+1}})^i(x^{-2^{2t+3}i}y)^j$ and $(x^{2^{2t+1}})^{i'}(x^{-2^{2t+3}i'}y)^j x^{2^{3t}k}$ where $0 \le i, i' \le 2^{t-1} - 1$, $k = 0, 1$. Matching the exponents of x, we get that $2^{2t+1}i - 2^{2t+3}ij - 2^{2t+1}i' + 2^{2t+3}i'j \equiv 0 \mod 2^{3t}$. This implies that $(i - i')(1 - 4j) \equiv 0 \mod 2^{t-1}$, so $i = i'$. Thus, the elements were not really distinct (they are from the same coset). ▌

For future discussions, any group ring element with coefficients 0 or 1 will be considered equivalent to the subset of G_t to which it is associated. Thus, we will be able to make sense out of statements which claim that two group ring elements are disjoint. This simply means that the sets associated to those group ring elements are disjoint.

Note that there are 2^{t-1} cosets in each sum making up $D_{2^t,0}$, each with 2^t elements. The total is multiplied by $(1 + x^{2^{3t}})$, so there are 2^{2t} elements in each coset $x^k H_t$ where $k \equiv \pm 2$ and $\pm 3 \pmod 8$.

For $j = 1, \ldots, t-1$, G_t has 2^j conjugacy classes of irreducible representations of degree 2^{t-j}. There will be a piece of the difference set for each. Let $D_{2^{t-j},b}$ denote the piece of the difference set which corresponds to the conjugacy class of $\Phi_{2^{t-j},b}$. Let $A_{2^{t-j}}$ and $B_{2^{t-j}}$ be as in Lemma 3.2 where $a_{2t-2j-1} = 2^{j+1}$ and $d_{2t-1-2j} = 2^j - 1$.

When $b \neq 0$ let $b = 2^\alpha \beta$. Set

$$S_{2^{t-j},b} = \sum_{i=0}^{2^{t-1-j}-1} x^{2^{2t+1}i} \langle x^{-2^{2t+2-(j-\alpha)}(2^{j-\alpha+1}i+\beta)} y, y^{2^{t-\alpha}} \rangle$$

and

$$T_{2^{t-j},b} = \sum_{i=0}^{2^{t-1-j}-1} x^{2^{2t+1}i} \langle x^{-2^{2t+2-(j-\alpha)}(2^{j-\alpha+1}i+\beta)+2^{j-\alpha}} y, y^{2^{t-\alpha}} \rangle.$$

Then

$$D_{2^{t-j},b} = (1 + x^{2^{3t-j}}) \left[x^{2^{j+3+\alpha}} A_{2^{t-j}} S_{2^{t-j},b} + x^{-2^{j+3+\alpha}} B_{2^{t-j}} T_{2^{t-j},b} \right].$$

When $b = 0$, set

$$S_{2^{t-j},0} = \langle x^{-2^{3t+2-j}}, y \rangle + \sum_{k=1}^{t-1-j} \sum_{i=0}^{2^{k-1}-1} x^{2^{3t-j-k}(2i+1)} \langle x^{-2^{3t+2-j-k}(2i+1)} y, y^{2^k} \rangle$$

and

$$T_{2^{t-j},0} = \sum_{i=0}^{2^{t-1-j}-1} x^{2^{2t+1}i} \langle x^{-2^{2t+2}(2i+1)} y, y^{2^{t-j}} \rangle.$$

Then

$$D_{2^{t-j},0} = (1 + x^{2^{3t-j}})[A_{2^{t-j}}S_{2^{t-j},0} + B_{2^{t-j}}T_{2^{t-j},0}].$$

The union of these pieces will make up most of the different set. Of course it must be shown that the union will be disjoint so that we build a set and not a multi-set.

We first argue that the sets $D_{2^{t-j},b}$ and $D_{2^{t-j'},b'}$ will not intersect if $j \neq j'$. By Lemma 3.2 the subset $D_{2^{t-j},b}$ intersects all cosets of H_t in G_t which are labeled by powers of x whose exponents are congruent to $\pm 2^{j+1} + 2^{j+3}b$ or $\pm(2^{j+2} - 1) + 2^{j+3}b$ modulo 2^{3+2j}, and similarly for j'. Without loss of generality say $j < j'$. Then none of exponents for the coset labels for $D_{2^{t-j},b}$ are zero modulo $2^{j'+1}$ while all of them are zero for $D_{2^{t-j'},b'}$. Thus these pieces must be disjoint.

The next lemma shows that $D_{2^{t-j},b}$ and $D_{2^{t-j},b'}$ are disjoint if $b \neq b'$.

LEMMA 4.2. *Let $0 \leq j \leq t - 1$ and $b \neq b'$. The sets $D_{2^{t-j},b}$ and $D_{2^{t-j},b'}$ are disjoint.*

Proof. Suppose that there is an element g in the intersection of $D_{2^{t-j},b}$ and $D_{2^{t-j},b'}$. Write $b = 2^{\alpha}\beta$ and $b' = 2^{\alpha'}\beta'$. It suffices to consider the case where $2t + 2 - j + \min\{\alpha, \alpha'\} < 2j + 3$. Otherwise $D_{2^{t-j},b}$ will only intersect those cosets of H_t labeled by powers of x whose exponents are congruent to $2^{j+3}b \bmod 2^{2j+3}$, and $D_{2^{t-j},b'}$ will intersect cosets labeled by powers of x whose exponents are congruent to $2^{j+3}b' \bmod 2^{2j+3}$. The two cosets are disjoint, so $D_{2^{t-j},b}$ and $D_{2^{t-j},b'}$ are disjoint in this case.

So consider the powers of $x \bmod 2^{2j+3}$. Since $2j + 3 \leq 2t + 1$, the only terms we need worry about are the terms $x^{2^{j+3}b}$ (resp. b') and $x^{2^{2t+2-j}bk}$ (resp. $b'k'$) where k (resp. k') is the power that appears in expressing the first generator of a subgroup in the sum for $D_{2^{t-j},b}$ (resp. b'). Our concern is that two of these describe the same element g. If so, then

$$2^{j+3}(b - b') \equiv 2^{2t+2-j}(bk - b'k') \pmod{2^{2j+3}}.$$

Now since $j \leq t - 1$, $j + 3 \leq 2t + 2 - j$. The right hand side of the above congruence is $0 \bmod 2^{2t+2-j+\min\{\alpha,\alpha'\}}$, so

$$b \equiv b' \bmod 2^{2t-2j-1+\min\{\alpha,\alpha'\}}.$$

Because $2t - 2j - 1 \geq 1$, we have $b \equiv b' \bmod 2^{1+\min\{\alpha,\alpha'\}}$. Without loss of generality $\alpha \leq \alpha'$. So $b' = 2^{\alpha}\beta + r2^{1+\alpha}$ for some r. This implies that b' is divisible by 2^{α} but not by $2^{1+\alpha}$. By our convention for writing the subscripts b, we see that $\alpha = \alpha'$.

So since $b \neq b'$ it must be that $\beta \neq \beta'$. Continuing under the assumption that g is an element in both sets, we now compare the powers of y

appearing in g. Use k and k' as the powers of the first generator of the subgroups where g exists. Because $\alpha = \alpha'$, the second generators must be $y^{2^{t-\alpha}}$. Thus $y^{k+2^{t-\alpha}l} = y^{k'+2^{t-\alpha}l'}$, for some l, l'. So $k \equiv k' \bmod 2^{t-\alpha}$.

Now read the powers of x modulo 2^{2j+3}. We get

$$2^{j+3+\alpha}(\beta - \beta') \equiv 2^{2t+2-j+\alpha}(\beta k - \beta' k') \qquad (\bmod 2^{2j+3}).$$

Say $2^a \| (\beta - \beta')$ where $1 \le a \le j - \alpha - 1 < t - \alpha$. Since $k - k' \equiv 0 \pmod{2^{t-\alpha}}$, $k - k' \equiv 0 \pmod{2^a}$. Thus $\beta k - \beta' k' \equiv \beta(k - k') \equiv 0 \pmod{2^a}$. Furthermore $j \le t - 1$ implies $2t + 2 - j + \alpha + a \ge j + 4 + \alpha + a$. Then $2^{j+3+\alpha}(\beta - \beta')$ is not congruent to zero modulo $2^{j+4+\alpha+a}$ while $2^{2t+2-j+\alpha}(\beta k - \beta' k')$ is congruent to zero modulo $2^{j+4+\alpha+a}$. This contradiction demonstrates that g cannot exist. ∎

The next lemma shows that there is no internal overlap.

LEMMA 4.3. *There are exactly* $2^{2t}(|A_{2^{t-j}}| + |B_{2^{t-j}}|)$ *elements of* G_t *in* $D_{2^{t-j},b}$.

Proof. Each subgroup used to build $D_{2^{t-j},b}$ has order 2^{t+j}. There are 2^{t-j-1} subgroups attached to each of $A_{2^{t-j}}$ and $B_{2^{t-j}}$. The factor $(1 + x^{2^{3t-j}})$ doubles the number of elements from the rest of the expression, so there are $2 \cdot 2^{t+j} \cdot 2^{t-j-1} \cdot (|A_{2^{t-j}}| + |B_{2^{t-j}}|) = 2^{2t}(|A_{2^{t-j}}| + |B_{2^{t-j}}|)$ elements in the expression. To prove the lemma, we must show that there are no duplicated elements.

Suppose that there is an element $g \in G_t$ that appears twice. We consider the case that g appears in the $A_{2^{t-j}}$ piece twice (the other cases are similar), so that we can write $g = x^{a+e}y^{k+2^{t-\alpha}m} = x^{a'+f}y^{k'+2^{t-\alpha}m'}$, where both x^a and $x^{a'}$ appear in $A_{2^{t-j}}$, and

$$e = 2^{2t+1}i + 2^{2t+2-(j-\alpha)}(2^{j-\alpha+1}i + \beta)k,$$

$$f = 2^{2t+1}i' + 2^{2t+2-(j-\alpha)}(2^{j-\alpha+1}i' + \beta)k'.$$

Equate the exponents on y to see that $k \equiv k' \bmod 2^{t-\alpha}$. Write $k - k' = 2^{t-\alpha}\delta$ for some δ. Then the two expressions for g imply $a - a' \equiv e - f \pmod{2^{3t+2}}$. But $e - f$ simplifies to $2^{2t+1}(i - i') - 2^{2t+3}(ik - i'k') - \beta(2^{3t+2-j}\delta)$, and x raised to this power is seen to be in H_t. Therefore $x^{a-a'} \in H_t$. Whence $a = a'$.

Next write $i - i' = 2^\rho c$, where $0 \le \rho \le t - j - 2$, and $2^\rho \| (i - i')$ so that c is odd. We examine the exponents of x in the expressions for g modulo $2^{2t+2+\rho}$. Because $2t + 2 + \rho \le 3t - j$ the term $(1 + x^{2^{3t-j}})$ at the beginning of $D_{2^{t-j},b}$ is of no concern here. Also, the case $j = t - 1$ has one subgroup in each part of the block so there is no chance of intersection there. Therefore we are interested in those values of j between 0 and $t - 2$. (The $j = t$ case comes later.)

Since $\alpha \le j$, $t - \alpha \ge t - j$, which combined with $\rho \le t - j - 2$ implies that $t - \alpha > \rho$. Thus $k \equiv k' \bmod 2^{\rho}$. Also $i \equiv i' \bmod 2^{\rho}$, so $ik \equiv i'k' \bmod 2^{\rho}$. Therefore $(ik - i'k') \equiv 0 \bmod 2^{2t+2+\rho}$. Thus by equating exponents of x in the two expressions for g

$$2^{2t+1+\rho}c = 2^{2t+1}(i - i') \equiv 2^{2t+2-(j-\alpha)}\beta(k - k') \qquad \bmod 2^{2t+2+\rho}.$$

We first consider the case $b \neq 0$. This forces $\alpha < j$ so that $2t + 2 - (j - \alpha) \le 2t + 1 + \rho$. Divide both sides of the previous congruence by $2^{2t+2-(j-\alpha)}$ to get

$$2^{j-\alpha-1+\rho}c \equiv \beta(k - k') \qquad \bmod 2^{j-\alpha+\rho}.$$

Since β and c are odd, this implies that $k - k' \equiv 2^{j-\alpha-1+\rho} \bmod 2^{j-\alpha+\rho}$. Since $\rho \le t - j - 2$, we have that $j - \alpha + \rho \le t - \alpha - 2$, so $k - k' \equiv 2^{j-\alpha+1+\rho} + c'2^{j-\alpha+\rho} \bmod 2^{t-\alpha}$, for some c'. However, this contradicts the fact that $k - k' \equiv 0 \bmod 2^{t-\alpha}$. This establishes the lemma for $b \neq 0$.

When $b = 0$ we adapt the previous arguments to reduce to the case where g appears twice in

$$A_{2^{t-j}}\left(\langle x^{2^{3t+2-j}}, y\rangle + \left(\sum_{n=1}^{t-1-j}\sum_{i=0}^{2^{n-1}-1} x^{2^{3t-j-n}(2i+1)}\langle x^{-2^{3t+2-j-n}(2i+1)}y, y^{2^n}\rangle\right)\right).$$

Now viewing the exponents of x in two expressions for g modulo 2^{3t-j-1} shows that $k = k'$. Thus we obtain

$$2^{3t-j-n+1}(i - i') \equiv 2^{3t-j-n+2}[(2i + 1)m - (2i' + 1)m'] \bmod 2^{3t-j-n+2+\rho},$$

where ρ is as above. We argue as before to show that $im \equiv i'm' \bmod 2^{\rho}$ by using the exponents on y in the two expressions for g and restrictions on m.

Then because $m - m'$ is at most divisible by 2^{n-2} we get that $m - m' \equiv 2^{\rho-1} \bmod 2^{\rho}$ ($\rho \ge 1$) But now $n > n - 2 \ge \rho$ which implies that $m - m'$ is not zero modulo 2^n. Examination of the exponents of y in the two expressions for g shows that $m - m'$ must be zero modulo 2^n. So again we reach a contradiction.

Finally when $\rho = 0$ the above argument leads to the contradiction that $1 \equiv 0 \bmod 2$. ∎

As a consequence of Lemmas 4.1 through 4.3 we have

COROLLARY 4.1. *The set* $P := \sum_{j=0}^{t-1}\sum_{b=0}^{2^j-1} D_{2^{t-j},b}$ *intersects a coset of* H_t *in either* 2^{2t} *elements, or not at all. Moreover, the cosets of* H_t *which* P

misses are exactly those labeled by powers of x where the exponents are congruent to $0, \pm 1$ *and* 2^{t+1} *modulo* 2^{t+2}.

Proof. The choices of $a_{2t-2j-1}$ and $d_{2t-2j-1}$ yield the fact that the powers of x appearing in $A_{2^{t-j}}$ and $B_{2^{t-j}}$ are congruent to $\pm 2^{j+1}$, $\pm 2^{j+2} - 1$ modulo 2^{3+2j}, $0 \le j \le t-1$.

For the cosets which P intersects nontrivially there are two cases, namely $2t + 2 - j + \alpha \ge 2j + 3$ or $2t + 2 - j + \alpha + s = 2j + 3$ for $s \ge 1$.

In the first case, $D_{2^{t-j},b}$ fills each coset $x^k H_t$ with 2^{2t} elements where x^k appears in $x^{2^{j+3}b}A_{2^{t-j}}$ or $x^{-2^{j+3}b}B_{2^{t-j}}$.

In the second case, each subgroup used to build $D_{2^{t-j},2^{\alpha}\beta}$ is partitioned among 2^s cosets $x^{k_1}H_t, \ldots, x^k$'s H_t, where all the x^k's appear in $x^{2^{j+3+\alpha}\beta}A_{2^{t-j}}$ or they all appear in $x^{-2^{j+3+\alpha}\beta}B_{2^{t-j}}$. This is also true for $D_{2^{t-j},2^{\alpha}(\beta+r2^{j-\alpha-s})}$ for $0 \le r \le 2^s - 1$. Since the D's do not overlap, each coset $x^k H_t$ intersects P in the proper number of elements in this case.

Collectively P intersects each coset $x^k H_t$ in 2^{2t} elements where x^k appears in $x^{2^{j+3+\alpha}\beta}A_{2^{t-j}}$ or $x^{-2^{j+3+\alpha}\beta}B_{2^{t-j}}$. The cosets of H_t which do not intersect P are precisely those listed in the final claim of the corollary. ∎

We now prove that any nonlinear irreducible representation applied to P will give the proper representation sum. The next lemma shows that whenever a nonlinear irreducible representation is applied to P, it sums to zero except on its corresponding piece.

LEMMA 4.4. *Let* $\phi \in \Phi_{2^{t-j},b}$ *be a nonlinear irreducible representation for* G_t. *Then* $\phi(P) = \phi(D_{2^{t-j},b})$.

Proof. (1) First we show that if $j \ne j'$, then $\phi(D_{2^{t-j'},b'}) = 0$.

If $j < j'$ then each subgroup in the definition of $D_{2^{t-j'},b'}$ has an element of the form $(x^a y)^{2^{t-\alpha}}(y^{2^{t-\alpha}})^{-1} = x^c$, where $a = 2^{2t+2-(j'-\alpha')}(2^{t-j'-\alpha'}i + \beta')$, and $c = 2^{3t+2-j'}(2^{t-j'-\alpha'}i + \beta')$. This element is mapped by ϕ to $m_{2^{t-j}}(\zeta)$ where ζ is a primitive $2^{j'-j}$nd root of unity. By the special fact mentioned prior to Theorem 2.1, the sum of a representation over a subgroup is zero whenever there is an element of this form. Hence ϕ is zero on $D_{2^{t-j'},b'}$.

If $j > j'$, then there are two cases two consider.

First if $j = j' + 1$, then $\phi(1 + x^{3t-j'}) = (1-1)I_{2^{t-j}} = 0$. So $\phi(D_{2^{t-j'},b'}) = 0$ since $(1 + x^{3t-j'})$ is a factor of $D_{2^{t-j'},b'}$.

Second, if $j \ge j' + 2$, then we consider cosets of two subgroups used to define $D_{2^{t-j'},b'}$ which are indexed by i and i' where $i - i' = 2^{t-j}$. ($j \ge j' + 2$ implies $t - j \le t - j' - 2$ so we can do this.) For the subgroups involved the second generators are the same, so ϕ maps those generators to the same matrix. The first generators differ by x^e where $e =$

$2^{2t+2-(j'-\alpha')+(j'-\alpha'+1)+t-j} = 2^{3t+3-j}$. This group element is mapped to the identity matrix by ϕ, so ϕ takes the same value on the first generators. Since ϕ takes the same values for both generators of the subgroups, the sum over the two subgroups must be the same. The coset representatives of the subgroups differ by x^p, where $p = 2^{3t+1-j}$. So the representation sum of the two cosets collectively is zero, since $\phi(x^p) = -I_m$.

All subgroups are paired in this manner. The sum of the cosets of the subgroups under ϕ is zero, which implies that the sum of $D_{2^{t-j'},b'}$ under ϕ is zero.

(2) Now suppose that $j = j'$ and $b \neq b'$. Write $b = 2^{\alpha}\beta$ and $b' = 2^{\alpha'}\beta'$. Let $K = \langle h, g \rangle$ be a subgroup used to define $D_{2^{t-j},b'}$, where $h = x^a y$, $g = y^{2^{t-\alpha}}$ and $a = -2^{2t+2-j+\alpha}(2^{j-\alpha+1}i + \beta)$. There are three cases to consider.

(a) If $\alpha > \alpha'$, then $\phi(h^{2^{t-j}}) = m_{2^{t-j}}(\zeta)$, where ζ is a primitive $2^{j-\alpha'}$nd root of unity. Using the special fact prior to Theorem 2.1, this implies that $\phi(K) = 0$, so $\phi(D_{2^{t-j},b'}) = 0$.

(b) If $\alpha < \alpha'$, set $a = 2^{\alpha'-\alpha-1}$. Then $\phi(g^a) = (-1)^n I_{2^{t-j}}$ for some odd n. Summing over the powers of g in K we get $\phi(K) = 0$, so again $\phi(D_{2^{t-j},b'}) = 0$.

(c) When $\alpha = \alpha'$ but $\beta \neq \beta'$, write $\beta - \beta' = 2^{\delta}\rho$, where ρ is odd. By the restrictions on β we get that $0 \leq \delta \leq j - \alpha - 1$. Set $c = 2^{2t+2+\alpha}(2^{j-\alpha+1}i + \beta')$, $a = -2^{2t+2-(j-\alpha)}(2^{j-\alpha+1}i + \beta')$, and $e = -2^{2t+2+\alpha}(2^{j-\alpha+1}(i'-i) + 2^{\delta}\rho)$. Then

$$\phi(x^a y) = \left(\eta^{2^j}\right)^a \eta^c m_{2^{t-j}}(0,1,0,\ldots,0) = \eta^e m_{2^{t-j}}(0,1,0,\ldots,0).$$

The 2^{t-j}nd power of this matrix is a diagonal matrix. The j, j entry will be η^f, where $f = -2^{3t+2+\alpha+\delta-j}\rho$. Since $\delta \leq j - \alpha - 1$, $3t + 2 + \alpha + \delta - j \leq 3t + 1$. As in the previous cases, this combined with the special fact prior to Theorem 2.1 implies that the representation sum over K yields zero. So once again we get $\phi(D_{2^{t-j},b'}) = 0$. ∎

The last lemma of this section shows that the remaining representation sums are correct.

LEMMA 4.5. *Let $\phi \in \Phi_{2^{t-j},b}$ be a nonlinear irreducible representation for G_t. Then $M := \phi(D_{2^{t-j},b})$ satisfies $M\overline{M}^t = 2^{4t}I_{2^{t-j}}$.*

Proof. It suffices to show that M corresponds to $2^j(1 + \sqrt{-1})S$ where S is as in Lemma 3.2, with $k = 2t - 2j - 1$.

First, by construction $\phi(A_{2^{t-j}}) = m_{2^{t-j}}(\gamma_{2t-2j-1})$. Similarly we see that $\phi(B_{2^{t-j}}) = m_{2^{t-j}}(\overline{\gamma_{2t-2j-1}}^{\tau_j})$. Next, the elements $x^{2^{j+3+\alpha}\beta}x^{2^{2t+1}k}$ correspond to the numbers $(\eta^{2^{s-t}})^{y_j}$. Third, $\phi(1 + x^{3t-j}) = (1 + \sqrt{-1})I_{2^{t-j}}$.

Finally, each subgroup K of G_t used in the definition of $D_{2^{t-j},b}$ gets mapped by ϕ to 2^jE_m for some m. Moreover each 2^jE_m has a subgroup K as pre-image in $D_{2^{t-j},b}$, $m = 0, 1, \ldots, 2^{t-j} - 1$. ∎

4.2. *The Linear Piece*

In this section we define the part of the difference set which corresponds to the linear representations for G_t (i.e., those of degree 1).

We begin with some remarks on the behavior of the characters. First, when m is odd, $\chi_{m,\alpha,\beta}(x^{2^{2t+1}}) = -1$ and when m is even, $\chi_{m,\alpha,\beta}(x^{2^{2t+1}}) = 1$. Second, the linear representations of G_t which are not principal on H_t fall into conjugacy classes. These classes are indexed by their shared kernels when viewed as characters of H_t.

For convenience we set $p(m)$ to be the remainder of m after dividing by 2. The kernel of $\chi_{m,\alpha,\beta}$ restricted to H_t is denoted by $K_{p(m),\alpha}$. For $\alpha \le t-1$ this is the group generated by $x^{2^{2t+1}}y^{2^{t-\alpha-p(m)}}$ and $y^{2^{t-\alpha}}$. When $\alpha = t$, we have $K_{1,t} = \langle x^{2^{2t+2}}, y\rangle$, and $K_{0,t} = H_t$.

For each $(p(m), \alpha) \neq (0, t)$ we define a subset $\Delta_{p(m),\alpha}$. This is the piece of our difference set which corresponds to the conjugacy class of linear representations indexed by $K_{p(m),\alpha}$.

These subsets are defined as

$$\Delta_{1,\alpha} = K_{1,\alpha} \sum_{0 \le i,j \le 2^{t-\alpha-1}-1} x^{j\cdot 2^{t+2+\alpha}} y^{i+(2i-1)j}$$

and

$$\Delta_{0,\alpha} = K_{0,\alpha} \sum_{0 \le i,j \le 2^{t-\alpha-1}-1} x^{j\cdot 2^{t+2+\alpha}} y^{i+(2-2i)j}.$$

There are referred to as K-matrices in the literature [3]. We stress the fact that these are sets. Also we note that $\Delta_{0,t}$ is defined to be empty (if we chose it to be H_t, then the corresponding subset would be the complement of a Hadamard difference set as defined in the Introduction).

The coset representatives $x^{j\cdot 2^{t+2+\alpha}}y^{i+(2i-1)j}$ form a relative difference set in the quotient group $\langle x^{2^{t+2+\alpha}}, y\rangle / K_{p(m),\alpha}$ relative to $\langle y^{2^{t-\alpha-1}}K_{p(m),\alpha}\rangle$ with parameters $(2^{2t-2-2\alpha}, 2, 2^{2t-2-2\alpha}, 2^{2t-3-2\alpha})$. This leads to the following lemma concerning linear representation sums of the $\Delta_{p(m),\alpha}$'s.

LEMMA 4.6. *Let $\chi := \chi_{m,\alpha,\beta}$ be a linear representation for G_t which is not principal on H_t. Then*

$$\left|\chi(\Delta_{p(m'),\alpha'})\right| = \begin{cases} 2^{2t} & \text{if } p(m) = p(m') \text{ and } \alpha = \alpha' \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We prove the last part of the lemma first.

(1) To begin with let us suppose that $p(m) \neq p(m')$. We show the argument for the case where $p(m) = 0$ and $p(m') = 1$. The case where $p(m) = 1$ and $p(m') = 0$ is similar.

The first generator of $K_{p(m'),\,\alpha'} = K_{1,\,\alpha'}$ is $x^{2^{2t+1}} y^{2^{t-\alpha'-1}}$. If $\alpha \leq \alpha'$, then $\chi(x^{2^{2t+1}}) = 1$ but $\chi(y^{2^{t-\alpha'-1}}) \neq 1$. So χ is nonprincipal on $K_{p(m'),\,\alpha'}$ and therefore $\chi(\Delta_{p(m'),\,\alpha'}) = 0$. If $\alpha > \alpha'$, then χ is principal on $K_{p(m'),\,\alpha'}$. The corresponding representation on the quotient group $\langle x^{2^{t+2+\alpha'}}, y\rangle / K_{1,\,\alpha'}$ is principal on the forbidden subgroup $\langle y^{2^{t-\alpha'-1}} K_{1,\,\alpha'}\rangle$. Therefore

$$\chi\left(\sum_{0 \leq i,\, j \leq 2^{t-\alpha-1}-1} x^{j \cdot 2^{t+2+\alpha}} y^{i+(2-2i)j}\right) = 0.$$

(2) Secondly, let us suppose that $p(m) = p(m')$ and $\alpha < \alpha'$. Then $\chi(y^{2^{t-\alpha'}}) = \eta^{2^{3t+2+\alpha-\alpha'}\beta}$. This is a primitive $2^{\alpha'-\alpha}$nd root of unity. So χ is nonprincipal on $K_{p(m'),\,\alpha'}$. Thus $\chi(\Delta_{p(m'),\,\alpha'}) = 0$.

(3) Next, let us suppose that $p(m) = p(m')$ and $\alpha > \alpha'$. If $p(m') = 1$, then $\chi(x^{2^{2t+1}} y^{2^{t-\alpha'-1}}) = -1$. Therefore $\chi(K_{1,\,\alpha'}) = \chi(\Delta_{p(m'),\,\alpha'}) = 0$. If $p(m') = 0$, then χ is principal on $K_{0,\,\alpha'}$. We now consider the corresponding representation on the quotient group $G_t / K_{0,\,\alpha'}$. In particular we focus on the restriction of the corresponding representation to the subgroup $\langle x^{2^{t+2+\alpha}}, y\rangle / K_{0,\,\alpha'}$. Since $\alpha > \alpha'$, χ is principal on $\langle y^{2^{t-\alpha'-1}}\rangle$. So the fact that we have a relative difference set in the quotient group implies that the representation sum will be zero. (This corresponds to saying that the representation sums to zero down a column of the K-matrix.)

(4) Finally, if $p(m) = p(m')$ and $\alpha = \alpha'$, then χ is by construction principal on $K_{p(m'),\,\alpha'}$. Moreover the corresponding representation on the quotient group in this case is nonprincipal on the forbidden subgroup. The existence of our relative difference set assures us that $\chi(\Delta_{p(m'),\,\alpha'})$ has the proper modulus. ∎

Our difference set D will be the union of P from Corollary 4.1 and shifts of the subsets $\Delta_{p(m),\,\alpha}$. It remains to be shown that this union will be disjoint. We must also prove that $\chi(P) = 0$ for any linear representation of G_t that is nonprincipal on H_t and that $\phi(\Delta_{p(m),\,\alpha}) = 0$ for any nonlinear irreducible representation ϕ and any subset $\Delta_{p(m),\,\alpha}$. That is the subject of the following two lemmas.

LEMMA 4.7. *Let $\phi \in \Phi_{2^{t-j},\,b}$ be an irreducible representation for G_t of degree 2^{t-j}, where $0 \leq j < t$. Then $\phi(\Delta_{p(m),\,\alpha}) = 0$ for any $\Delta_{p(m),\,\alpha}$.*

Proof. Each subgroup $K_{p(m),\alpha}$ contains the element $g = x^{2^{2t+2}}$, where $\phi(x^{2^{2t+2}}) = m_{2^{t-j}}(\eta^{2^{2t+2+j}})$. Since $j < t$ this is a diagonal matrix with entries which are primitive 2^{t-j}nd roots of unity. By the special fact prior to Theorem 2.1, this implies that the representation sum over the subgroups is 0 for each $K_{p(m),\alpha}$. This implies the lemma. ∎

LEMMA 4.8. *Let $\chi := \chi_{m,\alpha,\beta}$ be a linear representation for G_t which is nonprincipal on H_t. Also let $D_{2^{t-j},2^{\alpha'}\beta'}$ be a subset associated to a conjugacy class of irreducible nonlinear representations for G_t as in Subsection* 4.1. *Then either $\chi(D_{2^{t-j},2^{\alpha'}\beta'}) = 0$ or for some β'', $\chi(D_{2^{t-j},2^{\alpha'}\beta'} + D_{2^{t-j},2^{\alpha'}\beta''}) = 0$.*

Proof. The proof naturally breaks into cases.

(1) If $p(m) = 1$, then the argument will be similar to that for the previous lemma. If $j = t - 1$, then $\chi(1 + x^{2^{2t+1}}) = 0$ and we're done. So suppose that $j < t - 1$. For a fixed α' and β', χ is either principal on each of the subgroups used to define $D_{2^{t-j},2^{\alpha'}\beta'}$ or it is principal on none of them. When χ is nonprincipal on each subgroup, then clearly $\chi(D_{2^{t-j},2^{\alpha'}\beta'}) = 0$. If χ is principal on each subgroup, the image of any subgroup under χ is its size 2^{t+j}. In this case $\chi(x^{2^{2t+1}}) = -1$. The sum over the subgroups is zero under χ, so $\chi(D_{2^{t-j},2^{\alpha'}\beta'}) = 0$.

(2) Suppose that $p(m) = 0$. Since χ is nonprincipal on H_t, $\chi(y) \neq 1$. As before χ is either principal on all the subgroups defining $D_{2^{t-j},2^{\alpha'}\beta'}$ or nonprincipal on them all.

(a) If χ is nonprincipal on a subgroup, that subgroup maps to zero. So $D_{2^{t-j},2^{\alpha'}\beta'}$ would map to zero.

(b) If χ is principal on all of the subgroups, each subgroup under χ gets sent to 2^{t+j}. Moreover $\chi(x^{2^{2t+1}}) = 1$. We turn our attention to $x^{2^{2j+3}s}$ where $0 \leq s \leq 2^{2(2-j-1)} - 1$. These group elements are the powers of x which separate elements of $A_{2^{t-j}}$ and $B_{2^{t-j}}$. There are now three cases to consider.

(i) If $\chi(x^{2^{2j+3}}) \neq 1$ then $\chi(A_{2^{t-j}}) = \chi(B_{2^{t-j}}) = 0$. So $\chi(D_{2^{t-j},2^{\alpha'}\beta'}) = 0$.

(ii) If $\chi(x^{2^{2j+3}}) = 1$ and $2j + 3 \leq 2t + 2 - j + \alpha'$, then the first generator of every subgroup used to define $D_{2^{t-j},2^{\alpha'}\beta'}$ will get sent to $\chi(y) \neq 1$. Thus the subgroup will go to zero under χ.

(iii) If $\chi(x^{2^{2j+3}}) = 1$ and $2j + 3 > 2t + 2 - j + \alpha'$, then the only subgroups which do not map to zero under χ are those for which $\chi(x^{2^{2t+2-j+\alpha'}}) = \chi(y)(\neq 1)$.

Note that since $j \leq t - 1$, that $j + 3 + \alpha' < 2t + 2 - j + \alpha'$. Therefore $\chi(x^{2^{j+3+\alpha'}}) \neq 1$. Let s be the power of this group element which gets mapped to -1 under χ. (This group element is the separator for the

elements appearing in $A_{2^{t-j}}$ and $B_{2^{t-j}}$ for any subset $D_{2^{t-j},2^{\alpha'}\omega}$ as ω varies.) Let β'' satisfy $\beta' - \beta'' = s$ (read modulo $2^{j-\alpha'}$).

Next consider the behavior of χ on the subgroups used to define $D_{2^{t-j},2^{\alpha'}\beta''}$. The first generator of a subgroup here differs from a first generator of a subgroup for $D_{2^{t-j},2^{\alpha'}\beta'}$ by $x^{2^{2t+2-j+\alpha'}s}$. Since $\chi(x^{2^{j+3+\alpha'}s}) = -1$ and $2t + 2 - j + \alpha' > j + 3 + \alpha'$ we see that $\chi(x^{2^{2t+2-j+\alpha'}s}) = 1$. The second generators of any subgroup have the same image under χ because α' has been fixed. Therefore for any subgroup used to define $D_{2^{t-j},2^{\alpha'}\beta'}$ there is a corresponding subgroup used to define $D_{2^{t-j},2^{\alpha'}\beta''}$ which has the same image under χ. Thus the fact that $\beta' - \beta'' = s$ implies that $\chi(D_{2^{t-j},2^{\alpha'},\beta'} + D_{2^{t-j},2^{\alpha'},\beta''}) = 0$. ∎

Next we describe how to shift the subsets $\Delta_{p(m),\alpha}$ to ensure their disjointness from P and subsequently to ensure that the representation sums will be correct for all linear representations of G_t which are principal on H_t.

The conclusion of Corollary 4.1 says that the cosets of H_t in G_t which are labeled by powers of x whose exponents are congruent to 0, ± 1, and 2^{t+1} modulo 2^{t+2} do not intersect P. We shift the $\Delta_{p(m),\alpha}$'s to fill each of these cosets with 2^{2t} elements of the difference set, with one exception which is empty. We can do this by multiplying $\Delta_{0,0}$ by 1, $\Delta_{1,0}$ by $x^{2^{t+1}}$, $\Delta_{0,1}$ by x^1, $\Delta_{1,1}$ by $x^{2^{t+2}+1}$, $\Delta_{0,2}$ by x^{-1}, and $\Delta_{1,2}$ by $x^{-1+2^{t+3}}$. Finally, for $3 \le \alpha \le t$ set $\varsigma_\alpha = \sum_{i=0}^{\alpha-3} 2^{t+2+i}$ and multiply $\Delta_{p(m),\alpha}$ by $x^{-1+p(m)2^{t+\alpha+1}+\varsigma_\alpha}$.

LEMMA 4.9. *If $p(m) \neq p(m')$ or $\alpha \neq \alpha'$, then $x^{-1+p(m)2^{t+\alpha+1}+\varsigma_\alpha}\Delta_{p(m),\alpha}$ and $x^{-1+p(m')2^{t+\alpha'+1}+\varsigma_{\alpha'}}\Delta_{p(m'),\alpha'}$ have empty intersection.*

Proof. We show only the case where $p(m) = p(m') = 1$. The other cases are similar. Also without loss of generality we take $\alpha < \alpha'$. The set $x^{-1+p(m)2^{t+\alpha+1}+\varsigma_\alpha}\Delta_{p(m),\alpha}$ contains elements from the cosets of H_t whose representatives are powers of x whose exponents are

$$-1 + \varsigma_\alpha + 2^{t+\alpha+1} + 2^{t+2+\alpha}j$$

for $0 \le j \le 2^{t-1-\alpha} - 1$. For the second set these exponents are

$$-1 + \varsigma_{\alpha'} + 2^{t+\alpha'+1} + 2^{t+2+\alpha'}j'$$

for $0 \le j' \le 2^{t-1-\alpha'} - 1$.

The nonzero part of the first set modulo $2^{t+\alpha+1}$ is $-1 + \varsigma_\alpha$ which clearly cannot equal $-1 + \varsigma_{\alpha'}$ (modulo $2^{t+\alpha+1}$). So the two sets never lie in the same coset of H_t in G_t. Therefore they are disjoint. ∎

4.3. *The Main Theorem*

Now let us define the linear part of D to be

$$L := \left[\Delta_{0,0} + x^{2^{t+1}}\Delta_{1,0} + x\Delta_{0,1} + x^{1+2^{t+2}}\Delta_{1,1} + x^{-1}\Delta_{0,2} + x^{-1+2^{t+3}}\Delta_{1,2} + \sum_{p(m)=0}^{1}\sum_{\alpha=3}^{t} x^{-1+p(m)2^{t+\alpha+1}+\varsigma_\alpha}\Delta_{p(m),\alpha}\right].$$

THEOREM 4.1. *The set* $D := P + L$ *is a* $(2^{4t+2}, 2^{2t}(2^{2t+1}-1), 2^{2t}\cdot(2^{2t}-1), 2^{4t})$ *Hadamard difference set in* G_t.

Proof. The previous lemma shows that, after these shifts, only the coset of H_t labeled by $x^{-1+2^{2t+1}-2^{t+2}}$ has trivial intersection with all of the sets we have defined for $t \geq 3$. Every other coset of H_t in G_t intersects the union of our sets in exactly 2^{2t} elements. Since there are 2^{2t+1} cosets of H_t in G_t, we have that $|D| = k = 2^{2t}(2^{2t+1}-1)$.

Let ϕ be any representation from our complete list of distinct, inequivalent, irreducible representations for G_t.

If $\phi \in \Phi_{2^{t-j},b}$ is nonlinear, then $\phi(D) = \phi(D_{2^{t-j},b})$ by Lemmas 4.4 and 4.7. $\phi(D_{2^{t-j},b})$ satisfies the difference set equation under ϕ by Lemma 4.5.

If $\phi = \chi_{m,\alpha,\beta}$ is nonprincipal on H_t, then by Lemma 4.8, $\phi(P) = 0$. Lemma 4.6 implies that $|\phi(D)| = |\phi(\Delta_{p(m),\alpha})| = 2^{2t}$ as required.

Finally, if $\phi = \chi_{m,\alpha,\beta}$ is principal on H_t, then $\phi(D)$ has proper modulus because D intersects every coset of H_t in 2^{2t} elements with one exception, so the character sum has modulus 2^{2t}.

In all cases the representation sums are correct. Therefore by Theorem 2.1 D is a difference set. ∎

Note that the order of the group G_t is 2^{4t+2} and the exponent is 2^{3t+2}. Asymptotically, this demonstrates that the exponent of the group can be at least $|G|^{3/4}$ as claimed in the abstract.

5. EXAMPLES

5.1. $t = 1$

When $t = 1$, $G_1 = \langle x, y \mid x^{32} = y^2 = 1, yxy = x^{17}\rangle$ the modular group of order 64. In our construction of a (64, 28, 12)-difference set in this group we use $H_1 = \langle x^8, y\rangle$. We get

$$D = (1+x^8)(x^2+x^3)\langle y\rangle + (1+x^8)(x^{30}+x^{13})\langle x^{16}y\rangle + \langle x^8\rangle + x^4\langle x^8y\rangle + x^9\langle x^{16}, y\rangle.$$

Note here that $\Delta_{0,1}$ is empty, and that $|D \cap x^7 H_1| = 0$. This is similar to the difference set found by Liebler and Smith [15].

5.2. $t = 2$

When $t = 2$, $G_2 = \langle x, y \mid x^{256} = y^4 = 1, yxy^{-1} = x^{65} \rangle$ and $H_2 = \langle x^{32}, y \rangle$.

For the degree 4 part of the difference set

$$A_4 = x^2 + x^{131} + x^{170} + x^{171} + x^{82} + x^{211} + x^{122} + x^{123}$$

$$B_4 = x^{254} + x^{253} + x^{86} + x^{213} + x^{174} + x^{173} + x^{134} + x^5$$

and $D_{4,0} = (1 + x^{64})[\{A_4[\langle x^{128} y \rangle + x^{32} \langle y \rangle]\} + \{B_4[\langle x^{64} y \rangle + x^{32} \langle x^{192} y \rangle]\}]$.

For the degree two part of the difference set

$$A_2 = x^4 + x^7 \qquad \text{and} \qquad B_2 = x^{252} + x^{185}.$$

So $D_{2,0} = (1 + x^{32})[A_2 \langle x^{64} y, y^2 \rangle + B_2 \langle x^{128}, y \rangle]$ and

$$D_{2,1} = (1 + x^{32})\left[x^{16} A_2 \langle x^{32} y \rangle + x^{240} B_2 \langle x^{96} y \rangle\right].$$

The linear part of the difference set is

$$L = (x^8 + x^{24}) \langle x^{32} y^2 \rangle (1 + y) + (1 + x^{16} y^3) \langle x^{32} \rangle (1 + y)$$
$$+ x^{31} \langle x^{64}, y \rangle + x^{17} \langle x^{32} y, y^2 \rangle + x \langle x^{32}, y^2 \rangle.$$

Note that $\Delta_{0,2}$ is empty, and that $|D \cap x^{15} H_2| = 0$.

Here $P = D_{4,0} + D_{2,0} + D_{2,1}$ and $D = P + L$.

5.3. $t = 3$

When $t = 3$, $G_3 = \langle x, y \mid x^{2048} = y^8 = 1, yxy^{-1} = x^{257} \rangle$ and $H_3 = \langle x^{128}, y \rangle$.

For the degree eight part of the difference set we put $h = 1024$.

$$A_8 = x^2 \sum_{l=0}^{15} x^{h q_5(l)} (x^{72})^l (1 + x^{h(l-1)} x)$$

$$B_8 = x^{-2} \sum_{l=0}^{15} x^{h q_5(l)} (x^{-72})(1 + x^{hl} x),$$

where $q_5 = 0111101101110100$ and $x^{2048} = 1$.

$$D_{8,0} = (1 + x^{512})\Big\{A_8\big[\langle y \rangle + x^{128} \langle x^{-512} y \rangle + x^{256} \langle x^{-1024} y \rangle + x^{384} \langle x^{-1536} y \rangle\big]$$
$$+ B_8\big[\langle x^{-256} y \rangle + x^{128} \langle x^{-768} y \rangle + x^{256} \langle x^{-1284} y \rangle + x^{384} \langle x^{-1796} y \rangle\big]\Big\}.$$

The degree four part of D uses

$$A_4 = x^4 + x^{519} + x^{324} + x^{839} + x^{676} + x^{679} + x^{484} + x^{487}$$
$$B_4 = x^{2044} + x^{1017} + x^{1724} + x^{697} + x^{1372} + x^{857} + x^{1564} + x^{1049}.$$

This part consists of

$$D_{4,0} = (1 + x^{256})\{A_4[\langle x^{1024}, y\rangle + x^{128}\langle x^{-512}y, y^2\rangle] + B_4[\langle x^{-256}y, y^4\rangle + x^{128}\langle x^{-768}y, y^4\rangle]\}$$

and

$$D_{4,1} = (1 + x^{256})\{x^{16}A_4[\langle x^{-128}y\rangle + x^{128}\langle x^{-640}y\rangle] + x^{2032}B_4[\langle x^{-384}y\rangle + x^{128}\langle x^{-896}y\rangle]\}.$$

The degree two part consists of $A_2 = x^8 + x^{15}$, $B_2 = x^{2040} + x^{1777}$

$$D_{2,0} = (1 + x^{128})\{A_2\langle x^{512}, y\rangle + B_2\langle x^{-256}y, y^2\rangle\}$$
$$D_{2,1} = (1 + x^{128})\{x^{32}A_2\langle x^{-64}y\rangle + x^{-32}B_2\langle x^{-320}y\rangle\}$$
$$D_{2,2} = (1 + x^{128})\{x^{64}A_2\langle x^{-128}y, y^4\rangle + x^{-64}B_2\langle x^{-384}y, y^4\rangle\}$$
$$D_{2,3} = (1 + x^{128})\{x^{96}A_2\langle x^{-192}y\rangle + x^{-96}B_2\langle x^{-448}y\rangle\}.$$

The linear part of D consists of $x^{159}\Delta_{1,3} = x^{31}\langle x^{256}, y\rangle$

$$x^{2047}\Delta_{0,2} = x^{63}\langle x^{128}, y^2\rangle$$
$$x^{63}\Delta_{1,2} = x^{95}\langle x^{128}y, y^2\rangle$$
$$x\Delta_{0,1} = x\langle x^{128}, y^4\rangle(1 + y + x^{64}y^2 + x^{64}y)$$
$$x^{33}\Delta_{1,1} = x^{33}\langle x^{128}y^2, y^4\rangle(1 + y + x^{64}y^7 + x^{64}y^2)$$
$$\Delta_{0,0} = \langle x^{128}\rangle(1 + y + y^2 + y^3 + x^{32}y^2 + x^{32}y + x^{32} + x^{32}y^7 + x^{64}y^4 + x^{64}y + x^{64}y^6 + x^{64}y^3 + x^{96}y^6 + x^{96}y + x^{96}y^4 + x^{96}y^7)$$
$$x^{16}\Delta_{1,0} = x^{16}\langle x^{128}y^4\rangle(1 + y + y^2 + y^3 + x^{32}y^7 + x^{32}y^2 + x^{32}y^5 + x^{32} + x^{64}y^6 + x^{64}y^3 + x^{64} + x^{64}y^5 + x^{96}y^5 + x^{96}y^4 + x^{96}y^3 + x^{96}y^2).$$

The coset $x^{95}H_3$ does not intersect any of the sets listed above.

Here follows the intersection pattern of D with cosets of H_3 labeled by the powers of x, $x^0, \ldots, x^{127}$. Each entry signifies which part of the

difference set intersects the coset. A negative sign indicates that the part of the difference set which intersects the coset comes from a $B_{2^{t-j}}$ part. The subscript denotes the conjugacy class. So -4_1 in the position labeled by x^j will denote that a coset representative of H_3x^j appears in the B_4 piece of $D_{4,1}$.

Cosets $x^0, \ldots, x^{15}$ and $x^{64}, \ldots, x^{79}$

1_{00}	1_{01}	8	8	4_0	-8	-8	4_0	2_0	-4_1	8	8	-4_1	-8	-8	2_0
1_{00}	1_{01}	8	8	4_0	-8	-8	4_0	2_2	-4_1	8	8	-4_1	-8	-8	2_2

Cosets $x^{16}, \ldots, x^{31}$ and $x^{80}, \ldots, x^{95}$

1_{10}	-2_3	8	8	4_1	-8	-8	4_1	-2_3	-4_0	8	8	-4_0	-8	-8	1_{13}
1_{10}	-2_1	8	8	4_1	-8	-8	4_1	-2_1	-4_0	8	8	-4_0	-8	-8	

Cosets $x^{32}, \ldots, x^{47}$ and $x^{96}, \ldots, x^{111}$

1_{00}	1_{01}	8	8	4_0	-8	-8	4_0	2_1	-4_1	8	8	-4_1	-8	-8	2_1
1_{00}	1_{01}	8	8	4_0	-8	-8	4_0	2_3	-4_1	8	8	-4_1	-8	-8	2_3

Cosets $x^{48}, \ldots, x^{63}$ and $x^{112}, \ldots, x^{127}$

1_{10}	-2_2	8	8	4_1	-8	-8	4_1	-2_2	-4_0	8	8	-4_0	-8	-8	1_{12}
1_{10}	-2_0	8	8	4_1	-8	-8	4_1	-2_0	-4_0	8	8	-4_0	-8	-8	1_{02}

REFERENCES

1. M. Aschbacher, ''Finite Group Theory,'' Cambridge Univ. Press, Cambridge, England, 1986.
2. C. W. Curtis and I. Reiner, ''Representation Theory of Finite Groups and Associative Algebras,'' Wiley, New York, 1988.
3. J. A. Davis, Difference set in abelian 2-groups, *J. Combin. Theory Ser. A* **57** (1991), 262–286.
4. J. A. Davis, A generalization of Kraemer's result on difference sets, *J. Combin. Theory Ser. A* **57** (1991), 187–192.
5. J. A. Davis, A note on nonabelian (64, 28, 12)-difference sets, *Ars Combin.* **32** (1991), 311–314.
6. J. A. Davis and K. W. Smith, A construction of difference sets in high exponent 2-groups using representation theory, *J. Algebraic Combin.* **3** (1994), 137–151.

7. J. F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory Ser. A* **40** (1980), 9–21.
8. J. F. Dillon, A survey of difference sets in 2-groups, *in* "Coding Theory, Design Theory, Group Theory: Proc. of the Marshall Hall Conf." (Dieter Jungnickel, Ed.), Wiley, New York, 1992.
9. J. Jedwab, "Perfect Arrays, Barker Arrays, and Difference Sets," Ph.D. thesis, University of London, London, England, 1991.
10. R. E. Kibler, A summary of noncyclic difference sets, $k < 20$, *J. Combin. Theory Ser. A* **25** (1978), 62–67.
11. R. Kraemer, A result on Hadamard difference sets, *J. Combin. Theory Ser. A* **63** (1993), 1–10.
12. E. S. Lander, "Symmetric Designs: An Algebraic Approach," London Mathematical Society Lecture Notes Series, Vol. 74, Cambridge Univ. Press, Cambridge, England, 1983.
13. W. Ledermann, "Introduction to Group Characters," Cambridge Univ. Press, Cambridge, England, 1977.
14. R. A. Liebler, The inversion formula, *J. Combin. Math. Combin. Comput.* **13** (1993), 143–160.
15. R. A. Liebler and K. W. Smith, On difference sets in certain 2-groups, *in* "Coding Theory, Design Theory, Group Theory: Proc. of the Marshall Hall Conf." (Dieter Jungnickel, Ed.), Wiley, New York, 1992.
16. S. L. Ma, Partial difference sets, submitted for publication.
17. R. L. McFarland, A family of difference sets in noncyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1–10.
18. R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.