CORE
Metadata, citation and similar papers at core.ac.uk
Provided by University of Richmond

University of Richmond
UR Scholarship Repository

Math and Computer Science Faculty Publications
Math and Computer Science

7-1991

Difference Sets in Abelian 2-Groups

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

Follow this and additional works at: http://scholarship.richmond.edu/mathcs-faculty-publications


Part of the Discrete Mathematics and Combinatorics Commons

Recommended Citation
Davis, James A. "Difference Sets in Abelian 2-Groups." *Journal of Combinatorial Theory, Series A* 57, no. 2 (July 1991): 262-86. doi: 10.1016/0097-3165(91)90050-Q.

This Article is brought to you for free and open access by the Math and Computer Science at UR Scholarship Repository. It has been accepted for inclusion in Math and Computer Science Faculty Publications by an authorized administrator of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.

JOURNAL OF COMBINATORIAL THEORY, Series A 57, 262–286 (1991)

Difference Sets in Abelian 2-Groups

JAMES A. DAVIS

Department of Mathematics, Lafayette College, Easton, Pennsylvania 18042

Communicated by the Managing Editors

Received September 7, 1987

Examples of difference sets are given for large classes of abelian groups of order 2^{2d+2}. This fills in the gap of knowledge between Turyn's exponent condition and Dillon's rank condition. Specifically, it is shown that $\mathbb{Z}/(2^d)\times\mathbb{Z}/(2^{d+2})$ and $\mathbb{Z}/(2^{d+1})\times\mathbb{Z}/(2^{d+1})$ both admit difference sets, and these have many implications. © 1991 Academic Press, Inc.

1. INTRODUCTION

If G is an abelian group of order v, and D is a subset of G with k elements such that every nonidentity element can be expressed λ times in the form $a-b$, where a and b are elements of D, then D is called a (v, k, λ) difference set in G. The order n of the difference set is $k-\lambda$. In this paper we consider the parameter values $v=2^{2d+2}$, $k=2^{2d+1}-2^d$, $\lambda=2^{2d}-2^d$, and $n=2^{2d}$.

The rank r of G is the minimum number of generators, and the exponent $(\exp(G)=2^e)$ is the size of the largest cyclic subgroup of G. For a given order 2^{2d+2} of G, $(2d+2)/e\leqslant r\leqslant 2d+3-e$. In terms of r and e, the current state of knowledge can be summarized as follows: (1) If $e\geqslant d+3$, then G does not have a difference set (Turyn [8]); (2) if $r\geqslant d+1$, then G does have a difference set (Dillon [2]). Graphically, see Fig. 1.

The following is a result of Turyn [8], and it will be the main tool of this paper:

THEOREM 1.1. *A subset D of an abelian group G is a difference set if and only if $|\sum_{d\in D}\chi(d)|=\sqrt{n}$ for every nonprincipal character χ, and $\sum_{d\in D}\chi(d)=k$ for the principal character. (That is, $|D|=k$.)*

Using this result, we will prove (2). The construction is due to Dillon [2], but the proof uses Theorem 1.1.

Proof of (2). Suppose G is a group with $r\geqslant d+1$. Then G has an

0097-3165/91 $3.00

Copyright © 1991 by Academic Press, Inc.
All rights of reproduction in any form reserved.

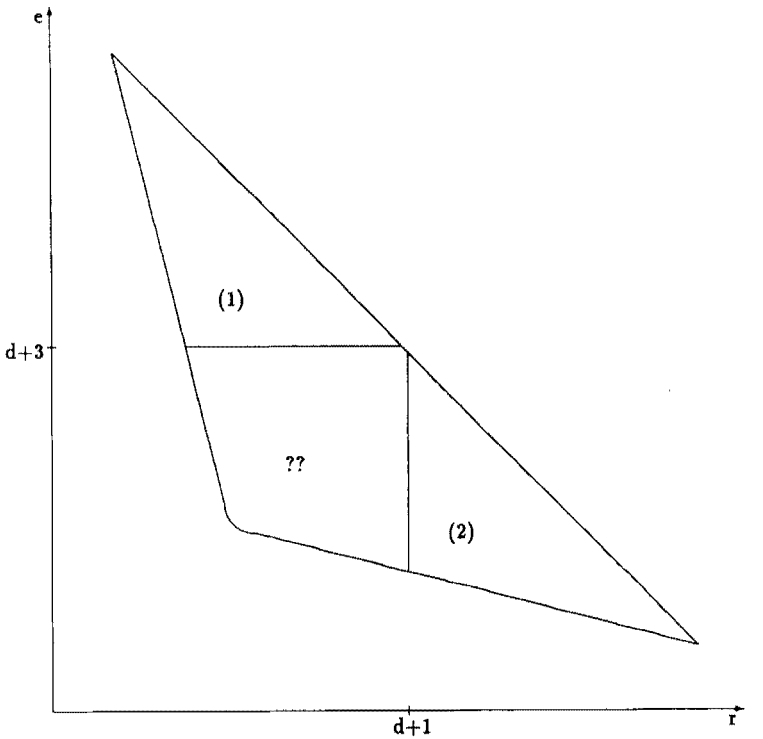

FIG. 1. Existence of difference sets Rank vs Exponent.

elementary abelian subgroup H of rank $d+1$. H has $2^{d+1}-1$ subgroups of order 2^d; call them D_i. If we consider the subset, $D=\bigcup_{i=1}^{2^{d+1}-1} g_i D_i$, where the g_i are coset representatives of H, then we claim that D is a difference set in G. For χ, a nonprincipal character on G, the character sum of Theorem 1.1 is

$$\left|\sum_{d\in D}\chi(d)\right| = \left|\sum_{k=1}^{2^{d+1}-1}\chi(g_k)\sum_{d\in D_k}\chi(d)\right|.$$

There are two cases:

(1) $\chi\in H^{\perp}$, where $H^{\perp}=\{\chi \text{ a character of } G \mid \chi(h)=1 \text{ for all } h \text{ in } H\}$. Since $D_i\subseteq H$, all have $\chi(d)=1$. Thus

$$\left|\sum_{d\in D}\chi(d)\right| = 2^d\left|\sum_{i=1}^{2^{d+1}-1}\chi(g_i)\right| = 2^d|-\chi(g_{2^{d+1}})| = 2^d=\sqrt{n}.$$

(2) $\chi\notin H^{\perp}$. Since the D_i are subgroups of H, any nonprincipal

character will be principal on exactly one of these subgroups, say D_j. The sum $\sum_{d \in D_i} \chi(d)$ for $i \neq j$ is 0. Therefore,

$$\left| \sum_{d \in D} \chi(d) \right| = |\chi(d_j)| \, |D_j| = 2^d = \sqrt{n}.$$

Thus, our nonprincipal character has the correct sum. The sum for the principal character is correct, since $|D| = 2^d(2^{d+1} - 1) = k$, so D is a difference set. ∎

This proof suggests the approach of the rest of the paper. For example, the difference sets will be written as $\bigcup_{i=1}^{2^{d+1}-1} g_i D_i$, but each D_i will be a union of cosets of subgroups of the H that we pick, not just subgroups. Moreover, we will see the same two cases, but case 2 will be more difficult.

We will use the following notation in the paper: If $G = \mathbb{Z}/(a) \times \mathbb{Z}/(b) \times \cdots \times \mathbb{Z}/(m)$, this will be abbreviated to $G = (a, b, ..., m)$. If G has a repeating factor, $G = (a, b, b, ..., b)$, then we will write $G = (a, (b)^m)$, where there are m copies of b. The elements of the group will be written $g = (g_1, g_2, ..., g_m)$. With "a" taken to be the exponent of G, characters will be written $\chi = [v_1, (a/b)\, v_2, ..., (a/m) v_m]$, where

$$\chi(g) = \xi^{v_1 g_1 + (a/b) v_2 g_2 + \cdots + (a/m) v_m g_m}$$

for ξ a primitive ath root of unity.

2. K-Matrix Structure

We need some organized method for presenting our candidate for a difference set, and we also need an easy way to check the character sum condition from Theorem 1.1. We pick a subgroup H of order 2^{d+1}, and the group can be written as $G = \bigcup_{k=1}^{2^{d+1}} g_k H$. If D is a difference set in G, it can be written $D = \bigcup_{k=1}^{2^{d+1}-1} g_k D_k$ for D_k subsets of H. These D_k use the subgroup structure of H; they will be unions of cosets of a subgroup of H.

Construction

Call two characters χ and χ' of G equivalent if both have the same kernel when they are restricted to H. This is clearly an equivalence relationship; let the class that χ belongs to be e_χ.

LEMMA 2.1. *If χ is a character on G and $\chi \notin H^\perp$, then $e_\chi = \bigcup_{j=1}^{a/2} (\chi)^{2j-1} H^\perp$, where a is the order $\chi|_H$.*

Proof. From elementary character theory, $(\mathrm{Ker}(\chi|_H))^\perp = \langle \chi \rangle H^\perp$, and

the even powers of χ have a bigger kernel than the odd powers; only the odd powers of χ have the same kernel. ∎

To each equivalence class e_χ except $H^\perp$, the class of χ_0, we associate a K-matrix. The entries are cosets of a subgroup K of G. The K-matrix for e_χ is

$$\{a_{i,j}\} = \{(i-(2i+1)j)x + \mathrm{Ker}(\chi\,|_H)\}.$$

If L is the order of χ restricted to H, then i and j run from 0 to $L/2-1$. Each column is labeled by $y+jz$; x, y, and z all depend on χ, the character: x is in H and y and z are elements of G. The motivation for this construction is that each column will be in the piece of the difference set in a particular coset of H, determined by $y+jz$, a column marker of the K-matrix. Picking the column markers $y+jz$ is more difficult than the construction in the Introduction; these column markers have to fit together to make our character sums correct (we will make this more precise). The coset of H that would be associated to the equivalence class $H^\perp$ does not meet the difference set. We denote its coset representative g_{2^d+1}. Most importantly, we require this choice of a K-matrix structure to have the following three properties:

(i) If χ' is a character not in $H^\perp$ or in e_χ, but χ' is principal on $\mathrm{Ker}(\chi\,|_H)$ (that is, χ' is in an $H^\perp$ coset of an even power of χ), then for the matrix associated to e_χ:

$$\sum_{i=0}^{L/2-1} \chi'((i-(2i+1)j)x) = \chi'(-jx) \sum_{i=0}^{L/2-1} \chi'(i(1-2j)x) = 0;$$

that is,

$$\sum_{i=0}^{L/2-1} \chi'(i(1-2j)x) = 0$$

for every j.

(ii) If χ' is in $e_\chi \neq H^\perp$, then for the matrix associated to e_χ:

$$\begin{aligned}
&\left|\sum_{j=0}^{L/2-1} \chi'((i-(2i+1)j)x + y + jz)\right| \\
&\quad = \left|\chi'(ix+y) \sum_{j=0}^{L/2+1} \chi'((1+2i)jx + jz)\right| \\
&\quad = \left|\sum_{j=0}^{L/2-1} \chi'((1+2i)jx + jz)\right| \\
&\quad = \begin{cases} 0 & \text{for every row but one, called } i_0 \\ 2^d/|\ker(\chi\,|_H)| & \text{for row } i_0. \end{cases}
\end{aligned}$$

The idea here is to break the character sum down to a sum over the rows of the K-matrix. Every rwo sums to 0 except one, which we call i_0; i_0 may depend on χ'.

(iii) The column markers $y+jz$ are representatives of distinct cosets of H.

THEOREM 2.2. *Any group G of order 2^{2d+2} with this K-matrix structure has a difference set D.*

Proof of Theorem 2.2. If we write G as $\bigcup_{k=1}^{2^{d+1}} g_k H$, where H is a subgroup of order 2^{d+1}, then we want to write $D=\bigcup_{k=1}^{2^{d+1}} g_k D_k$ also: the D_k are subsets of H, and they are the elements of the column marked by g_k. We picked the column markers to represent distinct cosets, and the D_k are subsets of H, so this fits the model so far. Let χ' be any nonprincipal character, and consider the sum

$$\left|\sum_{d\in D}\chi'(d)\right| = \left|\sum_{k=1}^{2^{d+1}-1}\chi'(g_k)\sum_{d_k\in D_k}\chi'(d_k)\right|.$$

Case 1. χ' is in $H^{\perp}$. Then, $\sum_{d_k\in D_k}\chi'(d_k)=|D_k|$, since each D_k is in H. Now $|D_k|=|\mathrm{Ker}(\chi'\mid_H)|\ L/2=|H|/2=2^d$. Thus the sum becomes

$$2^d\left|\sum_{k=1}^{2^{d+1}-1}\chi'(g_k)\right| = 2^d\,|-\chi'(g_{2^{d+1}})| = 2^d.$$

Case 2. χ' is not in $H^{\perp}$. We first check the character sum on every K-matrix except the one associated to $e_{\chi'}$. If χ' is nonprincipal on $K=\mathrm{Ker}(\chi''\mid_H)$, where χ'' is the character associated to the K-matrix, then since $\sum_{k\in K}\chi'(k)=0$, we obtain

$$\left|\sum_{i,j}\chi'((i-(2i+1)j)x+y+jz)\sum_{k\in K}\chi'(k)\right|=0.$$

If χ' is principal on K, then when we sum only over each column in the K-matrix, we obtain the size of the kernel times:

$$\chi(y+jz)\sum_{i=0}^{L/2-1}\chi'((i-(2i+1)j)x).$$

By property (i) of the K-matrix structure, this sum is 0, so again the character sum is 0 over this whole K-matrix. We need to check what sum χ' has on its own K-matrix. The sum for a given i is

$$\left| \sum_{j=0}^{L/2-1} \chi'((i-(2i+1)j)x+y+jz) \right| |\mathrm{Ker}(\chi'|_H)|$$
$$= \begin{cases} 0 & \text{for every } i \text{ but } i_0 \\ 2^d & \text{for } i_0, \end{cases}$$

by property (ii) of the K-matrix structure. These separate sums yield

$$\left| \sum_{d \in D} \chi'(d) \right| = 2^d = \sqrt{n}.$$

Finally,

$$\sum_{d \in D} \chi_0(d) = |D_i| \sum_{i=0}^{2^{d+1}-1} \chi_0(g_i) = 2^d(2^{d+1}-1)$$
$$= 2^{2d+1} - 2^d = k.$$

Thus, by Theorem 1.1, $D = \bigcup_{k=1}^{2^{d+1}-1} g_k D_k$ is a difference set in G. ∎

3. $(2^{d+2}, 2^d)$ Case

When we consider the abelian groups of order 2^{2d+2}, the worst possible case would be $(2^{d+2}, 2^d)$, since it has the lowest possible rank (2) and the highest possible exponent (2^{d+2}) to be in the gap.

To show that we do have a difference set in this class of groups, we use the structure from the preceding section. If we can show that the group has a K-matrix structure, then the fact that it has a difference set will merely be a corollary.

Example. We start by considering (16, 4), which is a group in the gap. The first thing we need is a subgroup H of order 8, so we will use $(4, 2) = H$. Next we consider the equivalence relationship on the character group: the classes are: (1) $H^\perp$; (2) $[2, 4]\, H^\perp$; (3) $[2, 0]\, H^\perp$; (4) $[0, 4]\, H^\perp$; (5) $[1, 4]\, H^\perp \cup [3, 12]\, H^\perp$; and (6) $[1, 0]\, H^\perp \cup [3, 0]\, H^\perp$. The characters use a 16th root of unity. Attached to these equivalence classes are the following K-matrices: (1) nothing; (2) $\mathrm{Ker}([2, 4]|_H)$, $y = (1, 0)$; (3) $\mathrm{Ker}([2, 0]|_H)$, $y = (1, 1)$; and (4) $\mathrm{Ker}([0, 4]|_H)$, $y = (3, 0)$. Notice that 2, 3, and 4 are 1×1 K-matrices since the characters only have order 2 on H; 5 and 6 will be 2×2 K-matrices since the characters in those categories have order 4:

$$(5) \qquad \begin{matrix} y=(0,0) & y+z=(0,1) \\ \begin{pmatrix} (0,0)+\mathrm{Ker}([1,4]\,|_H) & (12,0)+\mathrm{Ker}([1,4]\,|_H) \\ (4,0)+\mathrm{Ker}([1,4]\,|_H) & (8,0)+\mathrm{Ker}([1,4]\,|_H) \end{pmatrix} \end{matrix}$$

$$(6) \qquad \begin{matrix} y=(2,0) & y+z=(6,1) \\ \begin{pmatrix} (0,0)+\mathrm{Ker}([1,0]\,|_H) & (12,0)+\mathrm{Ker}([1,0]\,|_H) \\ (4,0)+\mathrm{Ker}([1,0]\,|_H) & (8,0)+\mathrm{Ker}([1,0]\,|_H) \end{pmatrix} \end{matrix}$$

We need to confirm that this K-matrix structure will satisfy the three properties.

The only characters that are principal on a kernel not the one for its equivalence class make up $[2,0]\,H^{\perp}$. The characters in this class are principal on the kernels in categories 5 and 6. If we write the general character in that category as $\chi=[2,0]\,h^{\perp}$ for $h^{\perp}$ in $H^{\perp}$, then we have

$$\chi(0,0)+\chi(4,0)=1-1=0; \qquad \chi(8,0)+\chi(12,0)=1-1=0.$$

This holds true for both categories 5 and 6, so property (i) is satisfied.

Suppose χ is in category 2. Here, the $|\mathrm{Ker}(\chi\,|_H)|=4$, so we want our sum $|\sum_{j=0}^{L/2-1}\chi'((i-(2i+1)j)x+y+jz)|$ to have absolute value 1. There is only one summand, and it is a root of unity, so it has absolute value 1. The exact same reasoning works if χ is in 3 or 4.

If χ is in category 5, $\chi(4,0)=\pm i$, and $\chi(0,1)=\pm i$, so we have to consider two different cases (two others are complex conjugates of these two cases).

Case 1. $\chi(4,0)=\chi(0,1)=i$:

$$\text{row } i=1 \qquad |(\chi(0,0)+\chi(12,1))|=|1+1|=2$$

$$\text{row } i=2 \qquad |(\chi(4,0)+\chi(8,1))|=|i-i|=0;$$

$\chi(4,0)=\chi(0,1)=-i$ is the conjugate of this case, and its sums will be the same as those.

Case 2. $\chi(4,0)=i$; $\chi(0,1)=-i$:

$$\text{row } i=1 \qquad |\chi(0,0)+\chi(12,1)|=|1-1|=0$$

$$\text{row } i=2 \qquad |\chi(4,0)+\chi(8,1))|=|i+i|=2;$$

$\chi(4,0)=-i$; $\chi(0,1)=i$ is the conjugate of this case, and its $i=2$ sum will be $-2i$, which has absolute value 2. Thus, the sums are the same.

Thus, the sum is always $4/|\mathrm{Ker}[\chi\,|_H]|=4/2=2$ for one i and 0 for the other. This satisfies condition (ii).

The same argument works exactly the same for category 6 since, if χ is in category 6, $\chi(4, 0) = \pm i$ and $\chi(4, 1) = \pm i$; just as for category 5, the four cases satisfy condition (ii).

Finally, the coset representatives are: (2) (1, 0); (3) (1, 1); (4) (3, 0); (5) (0, 0) and (0, 1); and (6) (2, 0) and (6, 1). The cosets are distinct, which is condition (iii). Therefore, $d = 2$ has the K-matrix structure that we were looking for which implies that D is a difference set in (16, 4).

For ease of notation, we will write subgroups as $\langle\ \rangle$, where this signifies that we are considering the subgroup generated by the elements in between that symbol; also, we will write cosets of this subgroup as $g\langle\ \rangle$, even though the group is additive.

To actually see what this difference set is in G, let us write out the D_i and g:

D_1 is empty; $D_2 = \langle 4, 0\rangle$; $D_3 = \langle (8, 0), (0, 2)\rangle$;

$D_4 = \langle (4, 2)\rangle$; $D_5 = \langle 8, 2\rangle \cup (4, 0)\langle 8, 2\rangle$;

$D_5' = (12, 0)\langle 8, 2\rangle \cup (8, 0)\langle 8, 2\rangle$; $D_6 = \langle 0, 2\rangle \cup (4, 0)\langle 0, 2\rangle$;

$D_6' = (12, 0)\langle 0, 2\rangle \cup (8, 0)\langle 0, 2\rangle$.

Thus, the difference set in (16, 4) is

$$\begin{aligned} D &= (1, 0)\langle 4, 0\rangle \cup (1, 1)\langle (8, 0), (0, 2)\rangle \cup (3, 0)\langle 4, 2\rangle \cup \langle 8, 2\rangle \\ &\quad \cup (4, 0)\langle 8, 2\rangle \cup (12, 1)\langle 8, 2\rangle \cup (8, 1)\langle 8, 2\rangle \cup (2, 0)\langle 0, 2\rangle \\ &\quad \cup (6, 0)\langle 0, 2\rangle \cup (2, 1)\langle 0, 2\rangle \cup (14, 1)\langle 0, 2\rangle \\ &= \{(1, 0), (5, 0), (9, 0), (13, 0); (1, 1), (9, 1), (1, 3), (9, 3); \\ &\quad (3, 0), (7, 2), (11, 0), (15, 2); (0, 0), (8, 2); (4, 0), (12, 2); \\ &\quad (12, 1), (4, 3); (8, 1), (0, 3); (2, 0), (2, 2); (6, 0), (6, 2); \\ &\quad (2, 1)(2, 3); (14, 1), (14, 3)\}. \ \blacksquare \end{aligned}$$

We have to develop techniques to get a difference set in $(2^{d+2+1}, 2^{d+1})$ given that $(2^{d+2}, 2^d)$ has a difference set. We look at the case where d is even.

The d Even Case

We start by considering the following groups: $G = (2^{d+2}, 2^d)$, $H = (2^{(d+2)/2}, 2^{(d/2)})$; $G' = (2^{d+3}, 2^{d+1})$, and $H' = (2^{(d+2)/2}, 2^{(d+2)/2})$, for d even. If χ is a character on G, then we will write $\chi = [v, 4w]$ which maps to powers of a 2^{d+2}nd root of unity ξ; and if χ is a character on G', then write $\chi = [v', 4w']'$ mapping to powers of a 2^{d+3}th root of unity η, where this is set up so that $\eta^2 = \xi$.

The following map of G into G' and $\mathrm{char}(G)$ into $\mathrm{char}(G')$ will be very useful:

$$P\colon G \to G' \qquad \text{and} \qquad P\colon \mathrm{char}(G) \to \mathrm{char}(G')$$

defined by

$$P(g) = P(a, b) = (2a, b)' \qquad \text{for } g \text{ in } G,\ 0 \leqslant b \leqslant 2^d - 1$$

$$P(\chi) = P[v, 4w] = [v, 8w]' \qquad \text{for } \chi \text{ in } \mathrm{char}(G),\ 0 \leqslant v \leqslant 2^{d+2} - 1.$$

Note that P is not a homomorphism, but it is an injection of G into G' with several very nice properties.

LEMMA 3.1. (1) *$P(\chi)\{P(g)\} = \chi(g)$ for every χ in $\mathrm{char}(G)$, g in G. This implies that $P(\chi)^r\{sP(g)\} = \chi^r(sg)$ for any r, s.*

(2) *P restricted to H is an injection of H into H'.*

(3) *$\mathrm{ord}(P(\chi)\,|_{H'}) = \mathrm{ord}(\chi\,|_H)$ for every χ in $\mathrm{char}(G)$.*

(4) *Let g and $\hat{g}$ be in G. If $P(g) = P(\hat{g}) + h'$ for some h' in H', then $g = \hat{g} + h$ for some h in H.*

(5) *If $(h')^\perp$ is in $(H')^\perp$, and $(y + jz)$ is any column marker in G, then $(h')^\perp(P(y + jz)) = (h')^\perp(P(y))(h')^\perp(jP(z))$.*

(6) *If $(h')^\perp$ is in $(H')^\perp$, and (a, b) is any element of G, then there is an $h^\perp$ in $H^\perp$ satisfying $(h')^\perp(jP(a, b)) = h^\perp(j(a, b))$.*

Proof. (1) $g = (a, b)$; $\chi = [v, 4w]$. Then $P(\chi)\{P(g)\} = [v, 8w]'(2a, b)' = \eta^{2av + 8bw} = \eta^{2(av + 4bw)} = \xi^{av + 4bw} = [v, 4w](a, b) = \chi(g)$. Also, $P(\chi)^r\{sP(g)\} = [v, 8w]'^r\{s(2a, b)'\} = \eta^{r\{2avs + 8bws\}} = \xi^{r\{avs + 4bws\}} = [v, 4w]^r\{s(a, b)\} = \chi^r(sg)$.

(2) Every element of H is of the form $h = (a2^{(d+2)/2}, b2^{d/2})$, for a and b integers, so $P(h) = (a2^{(d+1+3)/2}, b2^{(d+1-1)/2})'$; this is in H', so since P is an injection, it is an injection of H into H'.

(3) $P(\chi)$ has the same values on the generators of H' as χ has on the generators of H (see (1)), and the order of a character is determined by the values it takes on the generators. Thus, the orders must be the same.

(4) Let $g = (a, b)$ and $g_1 = (a_1, b_1)$; $P(g) = P(g_1) + h'$, so $(2a, b)' = (2a_1, b_1)' + (c2^{d/2+2}, f2^{d/2})$ for some c, f. If this is true, then $2a \equiv 2a_1 + c2^{d/2+2} (\mathrm{mod}\ 2^{d+3})$ and $b \equiv b_1 + f2^{d/2} (\mathrm{mod}\ 2^{d+1})$. Then $a \equiv a_1 + c2^{d/2+1} (\mathrm{mod}\ 2^{d+2})$ and $b \equiv b_1 + f2^{d/2} (\mathrm{mod}\ 2^d)$. Thus, we have $(a, b) = (a_1, b_1) + (c2^{d/2+1}, f2^{d/2})$, and the second term is in H.

(5) Let $(h')^\perp = [v'2^{(d/2)+1}, w'2^{(d/2)+3}]'$, v' and w' are arbitrary. If $y = (a, b)$ and $z = (c, f)$, then

$$(h')^\perp(P(y + jz)) = [v'2^{d/2+1}, w'2^{d/2+3}]'(2a + 2cj, b + fj + k2^d)',$$

where k is chosen so that $0 \leqslant b + fj + k2^d \leqslant 2^{d-1}$. This idea of using k to ensure that the component is in the proper range is true for the rest of the paper, and it never affects the calculations of the characters. Thus, we will suppress the use of this from now on. This value is

$$\eta^{2^{(d/2)+2}\{(a+cj)v' + 2(b+fj)w'\}};$$

$$\eta^{2^{(d/2)+2}\{(av' + 2bw') + (cjv' + 2fjw')\}}$$

$$= [v'2^{(d/2)+1}, w'2^{(d/2)+3}]'\,(2a, b)'$$

$$\times [v'2^{(d/2)+1}, w'2^{(d/2)+3}]'\,(j(2c, f))$$

$$= h'^{\perp}(P(a, b))\, h'^{\perp}(jP(c, f)).$$

(6) Let $(h')^{\perp} = [v'2^{(d/2)+1}, w'2^{(d/2)+3}]'$ and (a, b) is an element of G. Then

$$h'^{\perp}(jP(a, b)) = [v'2^{(d/2)+1}, w'2^{(d/2)+3}]'\,(j(2a, b)')$$

$$= \eta^{2^{(d/2)+2}\{ajv' + 2bjw'\}} = \xi^{2^{(d/2)+1}\{ajv' + 2bjw'\}}$$

$$= [v'2^{(d/2)+1}, w'2^{(d/2)+2}](j(a, b)) = h^{\perp}(j(a, b)),$$

where $[v'2^{(d+2)/2}, w'2^{(d/2)+2}]$ is the $h^{\perp}$ we were looking for. ∎

We can use P to map a K-matrix in G to a K-matrix in G' as follows: if the arbitrary element of this K-matrix is $x + \mathrm{Ker}(\chi\,|_H)$, Lemma 3.1(2) ensures that $P(x)$ will be in H'. Thus, $P(x) + \mathrm{Ker}(P(\chi)\,|_{H'})$ will be the element of a K-matrix in G'. If the equivalence class of the K-matrix is e_χ, then the equivalence class associated to the K-matrix in G' will be $e_{P(\chi)}$: by Lemma 3.1(3), since these characters have the same order, the size of the matrix will be the same. If the column marker for this K-matrix is $y + jz$, then the new column marker for the K-matrix in G' is $P(y + jz)$. We can use the lemma to show that the new K-matrices will satisfy properties (i), (ii), and (iii): the one important thing to note here is that this will not be a complete K-matrix structure as defined in Section 2. In that section, every equivalence class of characters had to have a K-matrix associated to it, and here we have only defined K-matrices for characters of G' that have a preimage character in G under P. Thus, we only check characters of the form $P(\chi)$, but there are other characters of G'.

LEMMA 3.2. *If there is a K-matrix structure in G satisfying properties* (i), (ii), *and* (iii), *then the K-matrices obtained in G' by using P will also satisfy these properties.*

Proof. (i) If $\sum_{i=0}^{L/2-1} \chi((i-(2i+1)j)x)=0$, then by Lemma 3.1(1),

$$\sum_{i=0}^{L/2-1} P(\chi)((i-(2i+1)j)\,P(x))=\sum_{i=0}^{L/2-1} \chi((i-(2i+1)j)x)=0,$$

so the K-matrix in G' satisfies (i).

(ii) If

$$\left|\sum_{j=0}^{L/2-1} \chi h^{\perp}((i-(2i+1)j)x+y+jz)\right| = \begin{cases} 2^d/|\mathrm{Ker}(\chi\,|^H)| & \text{for } i=i_0 \\ 0 & \text{otherwise.} \end{cases}$$

then by properties (1), (5), and (6) of Lemma 3.1, with $h'^{\perp}\in H'^{\perp}$,

$$\begin{aligned}
&\left|\sum_{j=0}^{L/2-1} P(\chi)\,h'^{\perp}((i-(2i+1)j)\,P(x)+P(y+jz))\right| \\
&\quad=\left|\sum_{j=0}^{L/2-1} P(\chi)\,h'^{\perp}((i-(2i+1)j)\,P(x))\,P(\chi)\,h'^{\perp}(P(y+jz))\right| \\
&\quad=\left|\sum_{j=0}^{L/2-1} \chi((i-(2i+1)j)x)\,P(\chi)(P(y))\,P(\chi)(P(jz))\,h'^{\perp}(P(y+jz))\right| \\
&\quad=\left|\sum_{j=0}^{L/2-1} \chi((i-(2i+1)j)x)\,\chi(y)\,\chi(jz)\,h^{\perp}(y+jz)\right| \\
&\qquad\text{for some } h^{\perp} \text{ in } H^{\perp} \\
&\quad=\left|\sum_{j=0}^{L/2-1} \chi h^{\perp}((i-(2i+1)j)x+y+jz)\right| \\
&\quad=\begin{cases} 2^d/|\mathrm{Ker}(\chi\,|_H)| & \text{for } i=i_0 \\ 0 & \text{otherwise} \end{cases} \\
&\quad=\begin{cases} 2^{d+1}/|\mathrm{Ker}(P(\chi)|_{H'})| & \text{for } i=i_0 \\ 0 & \text{otherwise;} \end{cases}
\end{aligned}$$

so this satisfies (ii).

(iii) By Lemma 3.1(4), if $P(y+jz)=P(y_1+j'z_1)+h_1$, then $y+jz=y_1+j'z_1+h$ for some h. This implies that those two are in the same coset of H, so since all the column markers are in distinct cosets, we have that $y+jz=y+j'z_1$ are marking the same column. Thus, $P(y+jz)=P(y+j'z_1)$, so we still have distinct coset representatives. ∎

We need to realize what needs to be completed. The classes of characters that have preimages in G cover twice as many characters in G' as they did in G, since $H'^{\perp}$ is twice as big. Thus, they cover half of the characters of G', since there are four times as many of the characters of G'. Consider characters of the form $[v, 4]'$, for $0 \leqslant v \leqslant 2^{(d+2)/2} - 1$. The classes of these characters fill out the missing characters, and we need to find K-matrices associated to these classes to fill out our structure. The K-matrix associated to the class for $[v, 4]'$ is

$$\{(i-(2i+1)j)x + \mathrm{Ker}([v, 4]'|_{H'})\}; y; z;$$

where $x = (0, 2^{d/2})'$; $z = (4, 2^{d/2} - v)'$; $y = (1, v/2)'$ if v is even, $(3, (v+1)/2)'$ if v is odd; $\mathrm{ord}[v, 4]' = 2^{(d/2)+1}$, so $0 \leqslant i, j \leqslant 2^{d/2} - 1$.

LEMMA 3.3. *If d is even, then the K-matrix structure we have setup using the map P and the $[v, 4]'$ matrices satisfies properties* (i), (ii), *and* (iii) *of the K-matrix section.*

Proof. We need to check the three properties separately, but we need to notice that a lot of work has already been done in Lemma 3.2.

(i) Suppose we have a character χ that is not in $H'^{\perp}$ or in $e_{\chi'}$ for some character χ', but χ is principal on $\mathrm{Ker}(\chi'|_{H'})$. As noted before, this implies that χ is an even power of χ' (or an $H'^{\perp}$ translate of that). If χ' is in the class of a character that is an image under P, then Lemma 3.2 implies that (i) is satisfied. Thus, we only need to consider the case $\chi' = [v, 4]'$ for some v. In that case we have $\chi = [v, 4]'^{2m}$ for $m \not\equiv 0 \pmod{2^{d/2}}$, so

$$\begin{aligned}
&\sum_{i=0}^{L/2-1} [v, 4]'^{2m} h'^{\perp}((i-(2i+1)j)(0, 2^{d/2})') \\
&\quad = \sum_{i=0}^{L/2-1} [v, 4]'^{2m}((i-(2i+1)j)(0, 2^{d/2})') \\
&\quad = \sum_{i=0}^{2^{d/2}} \eta^{\{2^{d/2+2}(i-(2i+1)j)\}2m} \\
&\quad = \sum_{i=0}^{2^{d/2}-1} \eta^{\{2^{d/2+3}(i-(2i+1)j)\}m} = \sum_{i=0}^{2^{d/2}-1} \gamma^{(i-(2i+1)j)m},
\end{aligned}$$

where γ is a $2^{d/2}$ root of unity. This last sum is 0, since $(1-2j)m \not\equiv 0 \pmod{2^{d/2}}$. Thus, (i) is satisfied.

(ii) If we have any nonprincipal character χ not in $H'^{\perp}$, we want to check the sum over its associated block. Again, if χ is an image by P of a

character on G (or an $H'^{\perp}$-translate of one), then Lemma 3.2 shows us that this is satisfied. We only need to check the case of $\chi = [v, 4]'$, and $(h')^{\perp} = [a2^{(d/2)+1}, b2^{(d/2)+3}]'$,

$$\begin{aligned}
&\left| \sum_{j=0}^{L/2-1} [v, 4]'^{2m+1} h'^{\perp}((i-(2i+1)j)(0, 2^{d/2})' + y + j(4, 2^{d/2} - v)) \right| \\
&= \left| \sum_{j=0}^{2^{d/2}-1} [v, 4]'^{2m+1} ((i-(2i+1)j)(0, 2^{d/2})' \right. \\
&\quad \left. + y + j(4, 2^{d/2} - v)) h'^{\perp}(y + j(4, 2^{d/2} - v)) \right| \\
&= \left| \sum_{j=0}^{2^{d/2}-1} \eta^{((i-(2i+1)j)2^{d/2+2} + j\{4v + 2^{d/2+2} - 4v\})(2m+1) + j\{2a2^{d/2+2} + b2^{d+3} - 2bv2^{d/2+2}\}} \right| \\
&= |\eta^{i2^{d/2+2}(2m+1)}| \left| \sum_{j=0}^{2^{d/2}-1} \eta^{j2^{d/2+2}((2m+1)(-1-2i+1)+2a-2bv)} \right| \\
&= \left| \sum_{j=0}^{2^{d/2}-1} \eta^{j2^{d/2+3}((2m+1)(-i)+a-bv)} \right| \\
&= \left| \sum_{j=0}^{2^{d/2}-1} \gamma^{j((2m+1)(-i)+a-bv)} \right|,
\end{aligned}$$

where γ is a $2^{d/2}$ root of unity.

This sum is zero unless $(2m+1)(-i) + (a-bv) \equiv 0 \pmod{2^{d/2}}$, in which case the sum is $2^{d/2} = 2^d/|\mathrm{Ker}(\chi'|_{H'})|$, which is what we want. This happens when

$$\begin{aligned}
(2m+1)(-i) &\equiv (bv-a) \pmod{2^{d/2}}, \\
(-i) &\equiv (bv-a)/(2m+1) \pmod{2^{d/2}},
\end{aligned}$$

or

$$i \equiv (a-bv)/(2m+1) \pmod{2^{d/2}};$$

this is the i_0 we were looking for. Thus, (ii) is satisfied.

(iii) We need to show that the coset representatives that we get from this construction (what is being called the column markers) are distinct. If we have two that are the same, they must both be images of column markers in G, or both not images. The reason for this involves the first component of the column marker: every image from G has an even first component since P doubles the first component, and every nonimage has an odd first component by construction. Thus, these could never differ by

an element of H; so we have only these two cases to check. The first case, that of both column markers being images from G, is taken care of in Lemma 3.2. Thus, we only need check the nonimage case. They are of the form $y + jz$ and $y + j'z$. In this case, both y and y_1 must of the form $(1, v/2)$ or $(3, (v+1)/2)$, since z has first component 4 and these must agree in the first component modulo 4. Also, using the first components, we see that j must equal j': if not, then the restriction of the values for j implies that they cannot be congruent. Finally, the second component yields

$$\begin{aligned}
v/2 + j(2^{d/2} - v) &\equiv v_1/2 + j(2^{d/2} - v_1) \pmod{2^{d/2}},\\
(v - v_1)/2 + (j)(v_1 - v) &\equiv 0 \pmod{2^{d/2}},\\
(v - v_1) + (2j)(v_1 - v) &\equiv 0 \pmod{2^{d/2+1}},\\
(v - v_1)(2j - 1) &\equiv 0 \pmod{2^{d/2+1}},\\
v_1 - v &\equiv 0 \pmod{2^{d/2+1}}.\\
v_1 &\equiv v \pmod{2^{d/2+1}};\\
v_1 &= v \qquad \text{by the restrictions on } v.
\end{aligned}$$

Thus, these mark the same column, so the column markers are representatives of distinct cosets. ∎

The d Odd Case

Before we do that, we need to realize that the map P used above is only good in the d even case. We need a similar map to handle the d odd case. In the same way, use the groups: $G = (2^{d+2}, 2^d)$; $G' = (2^{d+3}, 2^{d+1})$; $H = (2^{(d+1)/2}, 2^{(d+1)/2})$; $H' = (2^{(d+3)/2}, 2^{(d+1)/2})$. Characters on G will be written $[v, 4w]$, and characters on G' will be written $[v', 4w']'$. We define P' as follows: $P'\colon G \to G'$ and $P'\colon \mathrm{char}(G) \to \mathrm{char}(G')$ by $P'(a, b) = (a, 2b)'$, $0 \leqslant a \leqslant 2^{d+2} - 1$, and $P'([v, 4w]) = [2v, 4w]'$ for ξ a 2^{d+2} root of unity and η a 2^{d+3} root of unity (again with $\eta^2 = \xi$), and $0 \leqslant w \leqslant 2^d - 1$. We also need to define a "twist" in G' to ensure ourselves of a completely analogous lemma to 3.1:

$$\begin{aligned}
f\colon G' \to G' \qquad &\text{defined by } f(2a, b)' = (2a, b)';\\
&f(2a + 1, b)' = (2a, b + 1)'.
\end{aligned}$$

We notice that every column marker z has an even first component since it is either 4 or an image by P. Thus, f does not affect z. The following discussion is completely the same as Lemmas 3.1 through 3.3, so we have not included the proofs. The only slight change is the introduction of the

map f, but it is easy to check that the character calculations still work out with f involved. We obtain the following lemma.

LEMMA 3.4. (1) $P'(\chi)[P'(g)] = \chi(g)$ *for every* g *in* G *and* χ *in* $\mathrm{char}(G)$. *Also,* $P'(\chi)^r(sP'(g)) = \chi^r(sg)$ *for any* r, s.

(2) P' *injects* H *into* H'.

(3) $\mathrm{ord}(P'(\chi)\mid_{H'}) = \mathrm{ord}(\chi\mid_H)$ *for all* χ *in* $\mathrm{char}(G)$.

(4) *Let* g, g'' *be in* G. *If* $f(P'(g)) = f(P'(g'')) + h'$ *for some* h' *in* H', *then* $g = g'' + h$ *for some* h *in* H.

(5) *If* χ' *is in* $\mathrm{char}(G')$, *and* $y + jz$ *is a column marker in a* K*-matrix in* G, *then* $\chi'(f(P'(y+jz))) = \chi'(f(P'(y)))\,\chi'(fP'(jz)))$.

(6) *If* $(h')^{\perp}$ *is in* $H'^{\perp}$, *and* $z = (2a, b)$ *is any element of* G *with even first component, then there is an* $h^{\perp}$ *in* $H^{\perp}$ *such that* $(h')^{\perp}(f(P'(jz))) = h^{\perp}(jz)$.

Using P' and f, we can get a map from a K-matrix structure in G to a K-matrix structure in G' as follows: If $x + \mathrm{Ker}(x\mid_H)$ is the arbitrary entry in the K-matrix, then $P'(x) + \mathrm{Ker}(P'(\chi)\mid_{H'})$ is the element in the K-matrix in G', the associated equivalence class of characters is $e_{P'(\chi)}$, and the column markers in the new K-matrix are $f(P'(y+jz))$.

LEMMA 3.5. *If there is a* K*-matrix structure in* G *satisfying properties* (i), (ii), *and* (iii), *then the* K*-matrix structure obtained in* G' *by using* P' *and* f *will also satisfy those properties.*

Thus, we always have a method of embedding our K-matrix structure into a higher group. This is not the complete structure: there are many characters in the higher character group that do not have a preimage character.

Just as in the even case, there are equivalence classes with representatives $[1, 4v]'$, where $0 \leqslant v \leqslant 2^{(d+3)/2} - 1$. The corresponding K-matrix is $\{(i-(2i+1)j)x + \mathrm{Ker}([1, 4v]'\mid_{H'})\}$, where $x = (2^{(d+3)/2}, 0)'$; $y = (2v+1, 0)'$; $z = (2^{(d+3)/2} - 4v, 1)'$. Notice here that the order of $[1, 4v]'$ is $2^{(d+3)/2}$, so i and j are between 0 and $2^{(d+1)/2} - 1$, and $|\mathrm{Ker}([1, 4v]'\mid_{H'})| = 2^{(d+1)/2}$.

This takes care of all the equivalence classes that were not taken care of under the P' and f maps.

LEMMA 3.6. *If* d *is odd, then the* K*-matrix structure that we have set up using* P' *and* f *will satisfy properties* (i), (ii), *and* (iii) *of the* K*-matrix section.*

Finally, we are set to state the main result. The whole reason for these lemmas was to show how to build a K-matrix structure in a larger group

given one in a smaller group. We have now shown how to do this from odd to even and even to odd, which covers all the cases.

THEOREM 3.7. *Every group of the form* $(2^{d+2}, 2^d)$ *has a K-matrix structure that satisfies properties* (i), (ii), *and* (iii) *using* $H = (2^{(d+2)/2}, {}^{d/2})$ *when d is even and* $H = ((2^{(d+1)/2})^2)$ *when d is odd.*

Proof. We will do a proof by induction, where we induct on the parameter d. The example that we gave, in (16, 4), is the $d = 2$ case, and it starts the induction. Then if the group with parameter d', $(2^{d'+2}, 2^{d'})$, has a K-matrix structure satisfying (i), (ii), and (iii), we can use either Lemma 3.3 or Lemma 3.6 to see that the group for $d'+1$ will also have a K-matrix structure satisfying those three properties. The only difference between the two is that Lemma 3.3 handles the d' even case, and Lemma 3.6 handles the d' odd case. Thus, $(2^{d'+3}, 2^{d'+1})$ also has a K-matrix structure, so the induction is done. ∎

COROLLARY 3.8. *Every group* $(2^{d+2}, 2^d)$ *has a difference set.*

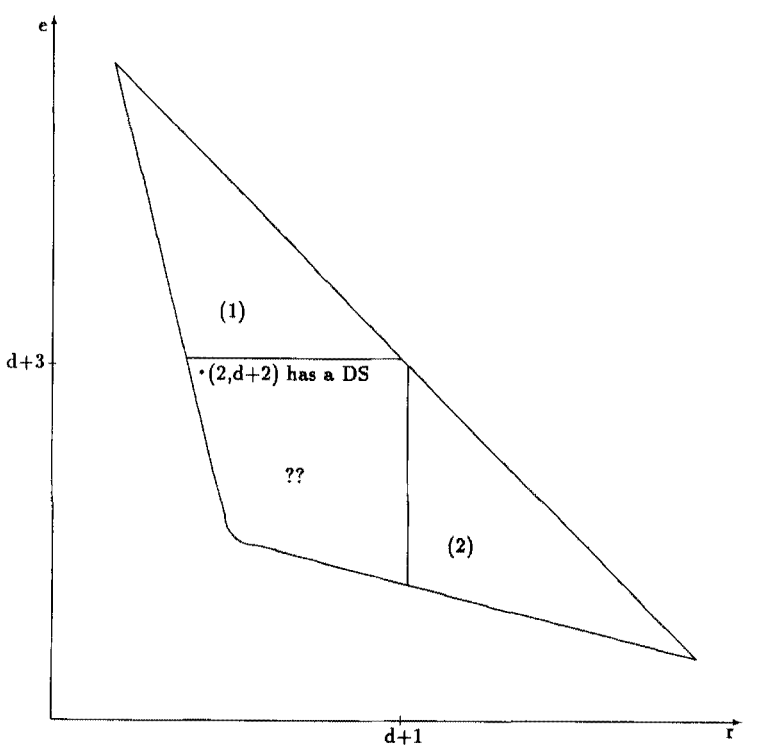

FIG. 2. Existence of rank 2 difference sets.

Proof. Combining Theorems 2.2 and 3.7, since this group has a K-matrix structure, it must have a difference set. ∎

Thus, we have accomplished what appears to be the most difficult case. Looking at the graph in Fig. 2, we see that we have filled in part of the unknown area.

4. Other Groups

We have now constructed a difference set in the difficult rank two case: we wish to obtain difference sets in other groups as a result of this finding. There are many techniques for finding these difference sets, and we will try to demonstrate several of these. The goal is to develop enough techniques to be able to answer all 2-groups.

$(2^{d+1}, 2^{d+1})$ *Case*

This is the other rank two case that meets the exponent bound. We can immediately observe that any group of this form will have the same subgroups H as the $(2^{d+2}, 2^d)$ for comparable d (depending on d even or d odd). Using the same idea that we used in the last section, we have $G = (2^{d+2}, 2^d)$, $H = (2^{(d+2)/2}, 2^{d+2})$ for d even, $(2^{(d+1)/2}, 2^{(d+1)/2})$ for d odd; $G' = (2^{d+1}, 2^{d+1})$; and H' is isomorphic to H. We need to find a map from G to G' and $\mathrm{char}(G)$ to $\mathrm{char}(G')$ will allow a transfer of the K-matrix structure. The following will work: $T: G \to G'$ defined by $T(2a, b) = (a, 2b)$ and $T(2a+1, b) = (a, 2b+1)$. $T: \mathrm{char}(G) \to \mathrm{char}(G')$ is defined as follows: let $[v, 4w]$ be any character in $\mathrm{char}(G)$, where $0 \leqslant v < 2^{d+2}$ and $0 \leqslant w < 2^d$. If $0 \leqslant v < 2^{d+1}$, then $T[v, 4w] = [v, w]'$, and if $2^{d+1} \leqslant v < 2^{d+2}$, then $T[v, 4w] = [v, w + 2^d]'$. The characters of G map to ξ, a 2^{d+2}th root of unity, while characters of G' map to δ a 2^{d+1}th root of unity. These roots of unity satisfy $\xi^2 = \delta$. We need to catalogue the properties of this map.

LEMMA 4.1. (1) *T is a bijection of G into G' and* $\mathrm{char}(G)$ *into* $\mathrm{char}(G')$.

(2) *T restricted to H is a bijection into H; moreover, if $T(p) - T(q)$ is in H in G', then $p - q$ is in H in G.*

(3) *For every χ a character on G and every g in G with even first component, $T(\chi)\, T(g) = \chi(g)$.*

(4) *If $y + jz$ is a column marker of the K-matrix structure in G, then $T(y + jz) = T(y) + jT(z)$.*

(5) $\mathrm{ord}(T(\chi)\,|_H) = \mathrm{ord}(\chi\,|_H)$ *for every* χ *in* $\mathrm{char}(G)$; *therefore,* $|\mathrm{Ker}(T(\chi)\,|_H)| = |\mathrm{Ker}(\chi\,|_H)|$.

Proof. (1) To show that T is 1–1 on G, look at arbitrary elements

$g=(a, b)$ and $k=(a''. b'')$ in G. Suppose $T(g)=T(k)$. In this case, both a and a'' must be both odd or even: if not, $T(g)$ and $T(k)$ will have opposite odd/even components in the second component, which cannot happen if they are equal. We have that either $a/2 \equiv a''/2 \pmod{2^{d+1}}$ or $(a-1)/2 \equiv (a''-1)/2 \pmod{2^{d+1}}$; both imply that $a \equiv a'' \pmod{2^{d+2}}$. Similarly, either $2b \equiv 2b'' \pmod{2^{d+1}}$ or $2b+1 \equiv 2b''+1 \pmod{2^{d+1}}$; both of these imply that $b \equiv b'' \pmod{2^d}$. Thus, $g=k$, so T is 1–1. Since these are finite, this implies that T is a bijection.

Suppose $T[v, 4w]=T[v', 4w']$. By the restriction of v, v', w, and w', we immediately obtain that $v=v'$ and $w=w'$. Thus, T is 1–1 on char(G), and is therefore a bijection.

(2) The general element of H in G can be written $h=(a2^{(d+2)/2}, b2^{d/2})$ in the d even case (the d odd case is the same). $T(h)=(a2^{d/2}, b2^{(d+2)/2})$, and this is the general element of H in G'. Thus, T maps H into H, and it inherits the bijection property.

Also, suppose $p=(a, b)$ and $q=(a'', b'')$; p and q must have both even or both first components (if not, then second components would differ in their odd components when we apply T, and would not be in H). Consider the odd case (the even is the same): $T(p)-T(q)=((a-1)/2,\ 2b+1)-((a''-1)/2,\ 2b''+1)=((a-a'')/2,\ 2(b-b''))$ is in H, so its preimage is also in H by the first part of (2). Therefore, $(a-a'', b-b'')=(a, b)-(a'', b'')$ is in H.

(3) Let $\chi=[v, 4w]$ for ξ a 2^{d+2} root of unity, and let $g=(2a, b)$ be an aribitrary element of G with an even first component. We have two cases: first, if $0 \leqslant v < 2^{d+1}$, then $T(\chi)\,T(g)=[v, w]'\ (a, 2b)=\delta^{av+2bw}=\xi^{2av+4bw}=[v, 4w](2a, b)=\chi(g)$. If $2^{d+1} \leqslant v < 2^{d+2}$, then $T(\chi)\,T(g)=[v, w+2^d]'\ (a, 2b)=\delta^{av+2bw+b2^{d+1}}=\delta^{av+2bw}=\xi^{2av+4bw}=[v, 4w](2a, b)=\chi(g)$.

(4) Every $z=(2a, b)$, for some a and b. The other part of the column markers, y, could have any values in the first component, so we break this down into two cases:

Case 1. y has even first component; $y=(2c, e)$:

$$T(y+jz)=T((2c, e)+j(2a, b))=T(2(c+ja),\ e+jb)$$
$$=(c+ja,\ 2e+2jb)=(c, 2e)+j(a, 2b)=T(y)+jT(z).$$

Case 2. y has odd first component; $y=(2c+1, e)$:

$$T(y+jz)=T(2c+1+2ja,\ e+jb)=(c+ja,\ 2e+2jb+1)$$
$$=(c, 2e+1)+j(a, 2b)=T(y)+jT(z).$$

Thus, the column markers in the new group can be written the same way as the old ones, as $T(y)+jT(z)$.

(5) By (2), T maps the generators of H to the generators of H. By (3), since every element of H has an even first component, $T(\chi)$ will have the exact same character values on the generators that χ had; thus, the order of $T(\chi)$ is the same as the order of χ. The last statement comes from the equation $|\mathrm{Ker}(\chi\,|_H)| = |H|/|\mathrm{ord}(\chi\,|_H)|$. ∎

Using this map, we can get a map from the K-matrix structure in G to a K-matrix structure in G'. If $x+\mathrm{Ker}(\chi\,|_H)$ is an arbitrary entry in a K-matrix in G, then $T(x)+\mathrm{Ker}(T(\chi)\,|_H)$ is the element in G'. The equivalence class associated to the matrix is generated by $T(\chi)$ if χ is the character in G. Finally, we use $T(y+jz)$ for the column markers for this K-matrix in G'.

THEOREM 4.2. *Every group* $(2^{d+1}, 2^{d+1})$ *has a K-matrix structure satisfying* (i), (ii), *and* (iii), *and therefore has a different set.*

Proof. Take the K-matrix structure found by using T on the K-matrix structure of Theorem 3.7:

(i) If χ' is not in $H^\perp$ or in e_χ for some χ, but χ' is principal on $\mathrm{Ker}(\chi\,|_H)$, then $\sum_{i=0}^{L/2-1} \chi'((i-(2i+1)\,j)x)=0$, $\chi'=T(\chi'')$ for some χ'' in $\mathrm{char}(G)$. Thus, by (3) of Lemma 4.1, since x is in H and therefore has even first component,

$$\sum_{i=0}^{L/2-1} T(\chi'')((i-(2i+1)\,j)\,T(x)) = \sum_{i=0}^{L/2-1} \chi''((i-(2i+1)\,j)x)=0,$$

since we have this property in G.

(ii) If χ' is not in $H^\perp$, then on the K-matrix associated to χ',

$$\left|\sum_{j=0}^{L/2-1} \chi'((-1-2i)\,jx+jz)\right| = \begin{cases} 2^d/|\mathrm{Ker}(\chi'\,|_H)| & i_0 \\ 0 & \text{otherwise.} \end{cases}$$

By (1) and (2) of Lemma 4.1, there is a χ'' in $\mathrm{char}(G)$ so that $T(\chi'')=\chi'$. Thus, since x is in H and has even first component, and z is defined to have an even first component, we can use Lemma 4.1(3) to show

$$\left|\sum_{j=0}^{L/2-1} T(\chi'')((-1-2i)\,jT(x)+jT(z))\right|$$
$$=\left|\sum_{j=0}^{L/2-1} \chi''((-1-2i)\,jx+jz)\right|$$
$$=\begin{cases}2^d/|\mathrm{Ker}(\chi'|_H)| & i_0\\ 0 & \text{otherwise,}\end{cases}$$

since this is true in G.

(ii) By property (2) of Lemma 4.1, if $T(y+jz)-T(y_1+j'z_1)$ is in H, then $y+jz-(y_1+j'z_1)$ is in H, so these are equal, and thus the column markers are in distinct cosets in H. ∎

So that we have a concrete example of this theorem, we look at the (8, 8) case. Using the maps T on the (16, 4) case, we get the following setup:

$$D_2=\langle 2,0\rangle;\ D_3=\langle (4,0),(0,4)\rangle;$$
$$D_4=\langle 2,4\rangle;$$
$$D_5=\langle 4,4\rangle\cup(2,0)\langle 4,4\rangle;$$
$$D_5'=(6,0)\langle 4,4\rangle\cup(4,0)\langle 4,4\rangle;$$
$$D_6=\langle 0,4\rangle\cup(2,0)\langle 0,4\rangle;$$
$$D_6'=(6,0)\langle 0,4\rangle\cup(4,0)\langle 0,4\rangle.$$

Also, $g_2=(0,1)$; $g_3=(0,3)$; $g_4=(1,1)$; $g_5=(0,0)$; $g_5'=(0,2)$; $g_6=(1,0)$; $g_6'=(3,2)$. By Theorem 4.2,

$$D=(0,1)\langle 2,0\rangle\cup(0,3)\langle (4,0),(0,4)\rangle\cup(1,1)\langle 2,4\rangle$$
$$\cup\langle 4,4\rangle\cup(2,0)\langle 4,4\rangle\cup(6,2)\langle 4,4\rangle\cup(4,2)\langle 4,4\rangle$$
$$\cup(1,0)\langle 0,4\rangle\cup(3,0)\langle 0,4\rangle\cup(1,2)\langle 0,4\rangle\cup(7,2)\langle 0,4\rangle$$

is a difference set in (8, 8), or

$$D=\{(0,1),(2,1),(4,1),(6,1);(0,3),(4,3),(0,7),(4,7);$$
$$(1,1),(3,5),(5,1),(7,5);(0,0),(4,4);(2,0),(6,4);$$
$$(6,2),(2,6);(4,2),(0,6);(1,0),(1,4);(3,0),(3,4);$$
$$(1,2),(1,6);(7,2),(7,6)\}.$$

Again, looking at our graph in Fig. 3, we have filled in another hole.

We can use this same methodology on the groups $(2^{d+1}, 2^d, 2)$; $((2^d)^2, 4)$; and $((2^d)^2, (2)^2)$, but that is as far as it goes using that same

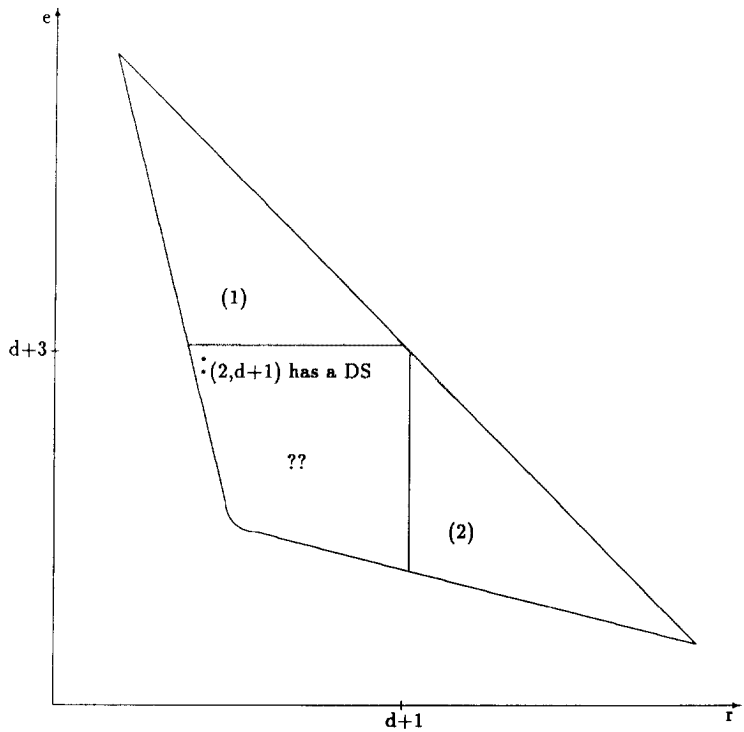

FIG. 3. Existence of rank 2 difference sets.

exact K-matrix structure. There is a far superior method for establishing the existence of difference sets in these groups, and it is due to Dillon [4]. We tackle this approach now, without giving proofs.

THEOREM 4.3. *If G and G' have order a power of 2, with the property thnat they admit difference sets, then $G'' = G \times G'$ also admits a difference set.*

THEOREM 4.4. *If G has a Hadamard difference set, then so does every group of the form $((2)^s, K)$, where K is any group containing G as a subgroup of index 2^s.*

These two results are not limited to the abelian case, so they yield some nice results in the nonabelian groups of this order. In this paper, we are solely interested in abelian groups.

LEMMA 4.5. *For every d and everyh $0 \leqslant e \leqslant d-1$, the following groups have difference sets*:

(i) $(2^{d+2}, 2^{d-e-1}, (2)^{e+1})$,
(ii) $(2^{d+1}, 2^{d-e}, (2)^{e+1})$,
(iii) $(2^{d}, 2^{d-e-1}, 4, (2)^{e+1})$.

Proof. We do induction on d. If $d=1$, then $e=0$ and these three cases are merely: (i) (8, 2); (ii) (4, 2, 2); and (iii) (2, 4, 2). All of these have difference sets, so this is true for $d=1$.

Suppose that the lemma is true for $d-1$. From her we only consider (i), since (ii) and (iii) are very similar.

(i) The group $G=(2^{d+1}, 2^{d-1})$ has a difference set by Corollary 3.8; choosing $K=(2^{d+2}, 2^{d-1})$ and applying Theorem 4.4, we see that $(2^{d+2}, 2^{d-1}, 2)$ has a difference set, and this is the $e=0$ case

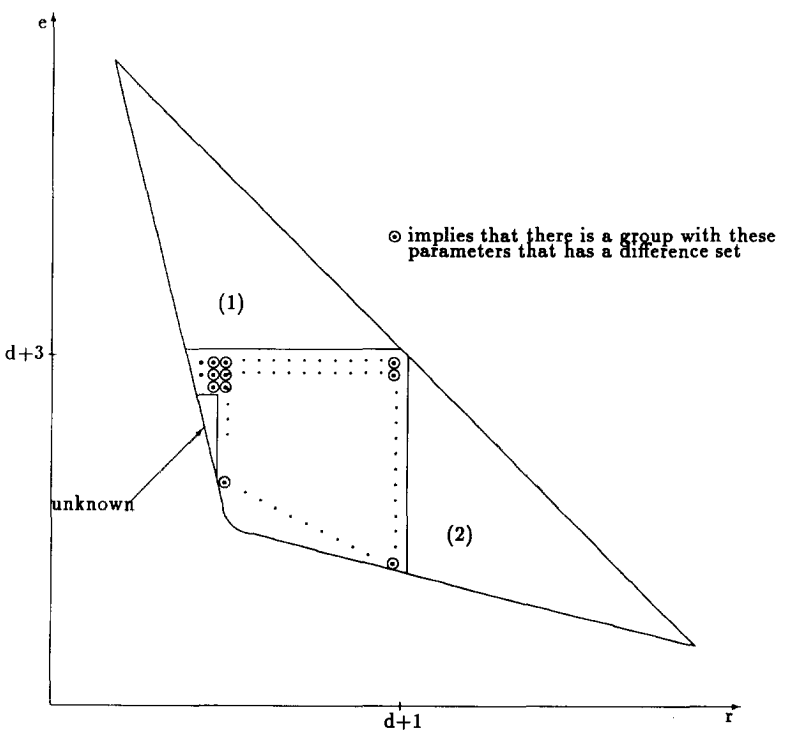

FIG. 4. Existence of difference sets.

Finally, for $1 \leqslant e \leqslant d$ (or $0 \leqslant e-1 \leqslant d-1$), use Theorem 4.4 on the following groups G and K, where G is written to satisfy the inductive hypothesis, so that it has a difference set:

$$\text{(i)} \qquad G = (2^{d+1}, 2^{d-e-1}, (2)^e)$$
$$= (2^{(d-1)+2}, 2^{(d-1)-(e-1)-1}, (2)^{(e-1)+1});$$
$$K = (2^{d+2}, 2^{d-e-1}, (2)^e).$$

These imply that $(2^{d+2}, 2^{d-e-1}, (2)^{e+1})$ has a difference set. ▮

This lemma shows that for the exponent 2^{d+2}, 2^{d+1}, and 2^d cases, there is a group of order 2^{2d+2} of every rank that has a difference set. This does not answer every group with those exponents, but it does fill in a large part of the unknown gap.

TABLE I

d	Group in Gap	Exist?	Reason	
2	(16,4)	yes	Cor. 3.8	
	(8,8)	yes	Thm. 4.2	
3	(32,8)	yes	Cor. 3.8	
	(16,16)	yes	Thm. 4.2	
	(32,4,2)	yes	Thm. 4.4	K = (32,4); G = (16,4)
	(16,8,2)	yes	Thm. 4.4	K = (16,8); G = (16,4)
	(16,4,4)	yes	Thm. 4.3	K = (16,4)×(4)
	(8,8,4)	yes	Thm. 4.3	K = (8,8)×(4)
4	(64,16)	yes	Cor. 3.8	
	(32,32)	yes	Thm. 4.2	
	(64,8,2)	yes	Thm. 4.4	K = (64,8); G = (32,8)
	(64,4,2,2)	yes	Thm. 4.4	K = (64,4,2); G = (64,4)
	(32,16,2)	yes	Thm. 4.4	K = (32,16); G = (16,16)
	(32,8,2,2)	yes	Thm. 4.4	K = (32,8,2); G = (32,8)
	(32,8,4)	yes	Thm. 4.3	(32,8)×(4)
	(32,4,4,2)	yes	Thm. 4.3	(32,4,2)×(4)
	(16,16,4)	yes	Thm. 4.3	(16,16)×(4)
	(16,16,2,2)	yes	Thm. 4.3	(16,16)×(2,2)
	(16,8,4,2)	yes	Thm. 4.3	(16,4)×(8,2)
	(16,4,4,4)	yes	Thm. 4.3	(8,8)×(8,2)
	(8,8,8,2)	yes	Thm. 4.3	(8,8)×(8,2)
	(8,8,4,4)	yes	Thm. 4.3	(8,8)×(4,4)
	(16,8,8)	?		
	(64,4,4)	?		

Table continued

TABLE I—*Continued*

d	Group in Gap	Exist?	Reason	
5	(128,32)	yes	Cor. 3.8	
	(64,64)	yes	Thm. 4.2	
	(128,16,2)	yes	Thm. 4.4	K = (128,16); G = (64,16)
	(128,8,4)	?		
	(128,8,2,2)	yes	Thm. 4.4	K = (128,8,2); G = (64,8,2)
	(128,4,4,2)	?	(if (64,4,4) has one, so does this)	
	(128,4,2,2,2)	yes	Thm. 4.4	K = (128,8,2); G = (64,4,2,2)
	(64,32,2)	yes	Thm. 4.4	K = (64,32); G = (32,32)
	(64,16,4)	yes	Thm. 4.3	K = (64,16)×(4)
	(64,16,2,2)	yes	Thm. 4.3	K = (64,16); G = (2,2)
	(64,8,8)	?	(similar to the two d = 4 unknowns)	
	(64,8,4,2)	yes	Thm. 4.4	K = (64,8,4); G = (32,8,4)
	(64,8,2,2,2)	yes	Thm. 4.4	K = (64,8,2,2); G = (32,8,2,2)
	(64,4,4,4)	?	(if (64,4,4) has one, so does this)	
	(64,4,4,2,2)	yes	Thm. 4.4	K = (64,4,4,2); G = (32,4,4,2)
	(32,32,4)	yes	Thm. 4.3	(32,32)×(4)
	(32,32,2,2)	yes	Thm. 4.3	(32,32)×(2,2)
	(32,16,8)	?		
	(32,16,4,2)	yes	Thm. 4.4	K = (32,16,4); G = (16,16,4)
	(32,16,2,2,2)	yes	Thm. 4.4	K = (32,16,2,2); G = (16,16,2,2)
	(32,8,8,2)	yes	Thm. 4.3	(32,8)×(8,2)
	(32,8,4,2,2)	yes	Thm. 4.3	(32,8)×(4,2,2)
	(32,8,4,4)	yes	Thm. 4.3	(32,8)×(4,4)
	(32,4,4,4,2)	yes	Thm. 4.4	K = (32,4,4,4); G = (16,4,4,4)
	(16,16,16)	?		
	(16,16,8,2)	yes	Thm. 4.3	(16,16)×(8,2)
	(16,16,4,4)	yes	Thm. 4.3	(16,16)×(4,4)
	(16,16,4,2,2)	yes	Thm. 4.3	(16,16)×(4,2,2)
	(16,8,8,4)	yes	Thm. 4.3	(16,4)×(8,8)
	(16,8,8,2,2)	yes	Thm. 4.3	(16,2,2)×(8,8)
	(16,8,4,4,2)	yes	Thm. 4.3	(16,4,4)×(8,2)
	(16,4,4,4,4)	yes	Thm. 4.3	(16,4,4)×(4,4)
	(8,8,8,8)	yes	Thm. 4.3	(8,8)×(8,8)
	(8,8,8,4,2)	yes	Thm. 4.3	(8,8,4)×(8,2)
	(8,8,4,4,4)	yes	Thm. 4.3	(8,8)×(4,4,4)

THEOREM 4.6. *For a given d, every element of the unknown area of the graph (except possibly those of the form* $(3, e)$ *for* $e < d$*) has a preimage group that has a difference set. Graphically, see Fig.* 4.

Proof. Lemma 4.5 takes care of all the cases (r, e), where e is d, $d+1$, or $d+2$. Thus, the only case to check is (r, e), where $r \geqslant 4$ and $e < d$. In the $r = 4$ case, $G = (2^e, 2^e)$ and $G' = (2^{d-e+1}, 2^{d-e+1})$ have difference

sets by Theorem 4.2, so $(2^e, 2^e, 2^{d-e+1}, 2^{d-e+1})$ has a difference set by Theorem 4.3. Again, using Lemma 4.5 on G and G', we can get groups of exponent 2^e and any rank that we want having a difference set. This fills in the remaining cases. ∎

This still leaves a gap, and there are still a lot of unknown groups. The main thing that is missing is the rank three cases for $e < d$. Table I explains what is known in groups that are in the small cases. Table I could be continued but the pattern of unknown cases has been established. These cases do not have a $\mathbb{Z}/(2)$ component, or Theorem 4.4 would be used to get the result; they are not a direct product of groups with difference sets, or Theorem 4.3 would yield an answer. It is not clear how to attack these groups in a general way; the results of this paper seem to indicate that a character theoretic approach would answer these groups individually, but they do not seem to organize themselves in any generalizable pattern.

It does appear that all groups of order 2^{2d+2} which have exponent less than 2^{d+3} will have a difference set. The worst of the problem seems to be done, but a general construction is still out of reach. This certainly is one direction that this research should lead. Other questions of interest include the following:

(1) How can these results answer questions in the nonabelian case?

(2) How can this construction be used in abelian groups other than 2-groups?

(3) Are there other ways to view this construction besides the cumbersome block notation?

(4) Since there are difference sets in these 2-groups, how many are there (up to isomorphism)?

(5) What kinds of codes to these difference sets contain?

REFERENCES

1. C. W. CURTIS AND I. REINER, "Representations of Finite Groups and Associative Algebras," Interscience, New York, 1962.
2. J. F. DILLON, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory Ser. A* **40**, No. 1 (1980), 9–21.
3. J. F. DILLON, Elementary Hadamard difference sets, *in* "Proceedings, 6th SCCGTC Congressurs Numeration XIV, 1975."
4. J. F. DILLON, On Hadamard difference sets, *Ars Combin.* **1** (1976), 275–279.
5. N. JACOBSON, "Basic Algebra II," Freeman, San Francisco, 1986.
6. R. E. KIBLER, A summary of noncyclic difference sets, $K < 20$, *J. Combin. Theory Ser. A* **25** (1978), 62–67.
7. E. S. LANDER, "Symmetric Designs: An Algebraic Approach," London Mathematical Society Lecture Note Series, Vol. 74, Cambridge Univ. Press, London, 1983.
8. R. J. TURYN, Character sums and difference sets, *Pac. J. Math.* **15**, No. 1 (1965), 319–346.