3-1992

A Generalization of Kraemer's Result on Difference Sets

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

JOURNAL OF COMBINATORIAL THEORY, Series A 59, 187–192 (1992)

A Generalization of Kraemer's Result on Difference Sets

JAMES A. DAVIS

University of Richmond, Virginia 23173

Communicated by the Managing Editors

Received July 14, 1989

Kraemer has shown that every abelian group of order 2^{2d+2} with exponent less than 2^{2d+3} has a difference set. Generalizing this result, we show that any non-abelian group with a central subgroup of size 2^{d+1} together with an exponent-like condition will have a difference set. © 1992 Academic Press, Inc.

1. INTRODUCTION

Let G be any finite group of order v: if $D \subset G$ is a subset of size k so that any nonidentity element of G can be represented λ times as differences from D, then D is called a (v, k, λ) difference set. If we look in the group ring ZG, this translates to the equation $DD^{(-1)} = k - \lambda + \lambda G$, where $D = \sum_{d \in D} d$, $D^{(-1)} = \sum_{d \in D} d^{-1}$, and $G = \sum_{g \in G} g$.

Another useful view of a difference set is its "contraction" by a normal subgroup H. This breaks the difference set up into pieces that exist in the cosets of H. If we write these pieces as $D_i \subset H$, then $D = \bigcup_{i=1}^{|G/H|} g_i D_i$, where the g_i are in distinct cosets. In the group ring,

$$DD^{(-1)} = \sum_i \sum_j g_i D_i D_j^{(-1)} g_j^{-1} = k - \lambda + \lambda \sum_k g_k H. \tag{1}$$

Characters on abelian groups can help determine the existance of a difference set. A character, χ, is a homomorphism from the abelian group G to the complex numbers. Clearly, χ must take every element of G into a 2^e root of unity if 2^e is the exponent of G. Turyn [7] shows the following.

LEMMA 1.1. *D is a $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$ difference set in an abelian group G if and only if for every nonprincipal character χ, $|\sum_{d \in D} \chi(d)| = 2^d$.*

The orthogonality relationships for characters can be used to demonstrate:

0097-3165/92 $3.00

LEMMA 1.2. *Let* $A=\sum_{g\in G} a_g g, a_g \in Z$ *be in the group ring* ZG; $\chi(A)=\sum_{g\in G} a_g \chi(g)=0$ *for every nonprincipal character* χ *if and only if* $A=cG$ *for some* c.

Proof. Suppose $A=cG=\sum_{g\in G} cg$. If χ is nonprincipal, there is a $g'\in G$ so that $\chi(g')\neq 1$. Since $g'A=A$, $\chi(g'A)=\chi(A)$. This implies that $\chi(g')\,\chi(A)=\chi(A)$, so $\chi(A)$ must be 0.

Now suppose that $\chi(A)=0$ for every nonprincipal character χ. The orthogonality relationships for characters imply that $a_g=1/|G|$, $\sum_\chi \chi(A)\,\chi^{-1}(g)=\chi_0(A)/|G|=c$ for every $g\in G$ (χ_0 is the principal character). ∎

In the constructions of Davis [2] and Kraemer [5], these character theoretic results are used to prove that there are difference sets in any abelian group of order 2^{2d+2} and exponent less than 2^{d+3}. Since we have to show that the character sums are valid for every nonprincipal character, we need to set up an equivalence relationship on the characters so we can check a whole class at once. Modifying the normal construction slightly, if χ and χ' are two characters on an abelian group H of size 2^{d+1}, then $\chi\equiv\chi'$ if $\mathrm{Kern}(\chi)=\mathrm{Kern}(\chi')$. The following lemma describes the equivalence classes of these characters (this is proved in [2]).

LEMMA 1.3. *The equivalence class for* χ, $[\chi]=\{\chi^a \mid a \text{ is odd}\}$. *If* χ' *is principal on* $\mathrm{Kern}(\chi)$ *but* $\chi'\notin[\chi]$, *then* $\chi'=\chi^{2a}$.

2. K-MATRICES

To investigate the existence of difference sets in two-groups, we need to introduce a structure called a K-matrix structure. We will essentially follow the notation of Kraemer.

Let $[\chi_0]$, $[\chi_1]$, ..., $[\chi_Q]$ be a list of the distinct equivalence classes of a subgroup H of order 2^{d+1} of an abelian group G of order 2^{2d+2}. For each $[\chi_t]$, $t\neq 0$, define the following:

(1) $K_t=\mathrm{Kern}(\chi_t)$.

(2) h_t is in $H-K_t$ so that h_tK_t generates H/K_t (recall that H/K_t is cyclic).

(3) The order of χ_t is 2^{s_t+1}.

(4) y_t and z_t are elements of G.

To each $[\chi_t]$, we associate the $2^{s_t}\times 2^{s_t}$ matrix M_t with (i,j) entry $m_{i,j}=y_t z_t^j h_t^{i-(2i+1)j}$, $0\leqslant i, j\leqslant 2^{s_t}-1$. We define a group to have a *K-matrix structure* if

(1) χ is principal on K_t, but $\chi \notin [\chi_t]$ and $\chi \neq \chi_0$, then $\sum_{i=0}^{2^{s_t}-1} \chi(h_t^{i-(2i+1)j}) = 0$ for every j. (This is the character sum of the h_t values in a column of M_t.)

(2) Suppose G is abelian, and χ is a character on G. If χ restricted to H is in $[\chi_t]$, then the sum of the values of χ on any row of M_t is 0, except for one row, called i_0 (depending on χ), where the sum has magnitude 2^{s_t}.

(3) The set $y_t z_t^j$ $0 \leqslant j \leqslant 2^{s_t} - 1$, $1 \leqslant t \leqslant Q$, together with the identity constitutes a complete set of distinct coset representatives of H in G.

In Davis [2], the following is proved:

THEOREM 2.1. *Any abelian two-group with a K-matrix structure has a difference set.*

The actual difference set is constructed by defining $D_{t,j} = \bigcup_{i=0}^{2^{s_t}-1} h_t^{i-(2i+1)j} K_t$, and then $D = \bigcup_{t=1}^{Q} \bigcup_{j=0}^{2^{s_t}-1} y_t z_t^j D_{t,j}$ is the difference set. The proof involves showing that every nonprincipal character sum over D has magnitude 2^d (Lemma 1.1).

To show that any abelian group meeting the exponent bound has a difference set, Kraemer [5] had to pick the y_t and z_t to meet the K-matrix definition. The choice of the z_t is important within M_t, while the choice of the y_t is only important in satisfying condition (3) of the K-matrix structure. To pick the z_t in the abelian case, it was neccesary to have a $c \in G - H$ so that either (i) $\mathrm{ord}(c) = \mathrm{ord}(cH) \geqslant \exp(H)$ or (ii) $\mathrm{ord}(c)/2 = \mathrm{ord}(cH) \geqslant \exp(H)$. If $\mathrm{ord}(c) = 2^e$, then $z_t = c^{2^{e-s_t}} h_t$ in case (i); case (ii) is either $z_t = c^{2^{e-s_t-1}}$ (if $c^{2^{e-1}} \notin K_t$) or $z_t = c^{2^{e-s_t-1}} h_t$ (if $c^{2^{e-1}} \in K_t$).

The coset representatives for H can be written as $a_1 c$, $a_1 c^2$, ..., $a_1 c^{2^e-1}$, a_1, $a_2 c$, $a_2 c^2$, ..., a_2, ..., $a_m c^{2^e-1}$, a_m for some $a_1, a_2, ..., a_m$. To choose the y_t, Kraemer proved that the following algorithm will satisfy condition (3) of the K-matrix definition:

I. Let μ be an $m \times 2^e$ matrix of integers, each row of which contains the integers from 1 to 2^e in order, all initially unmarked.

II. Set $t = 1$.

III. Let b_t be the unmarked entry in μ of minimal value. In case of a tie, choose the entry in the row of minimal index. Mark out all entries in that row of the form $b_t + k2^{e-s_t}$, for $0 \leqslant k \leqslant 2^{s_t} - 1$. Call the row, where b_t lies, r_t.

IV. Set $y_t = a_{r_t} c^{b_t}$, where $a_m = 1$.

V. Increment t. Doing III, IV, and V constitute step t. Go to III and repeat until Q steps have occurred.

With this setup, $D = \bigcup_{t=1}^{Q} \bigcup_{j=0}^{2^{s_t}-1} y_t z_t^j D_{t,j}$ is a difference set in G. Moving back to the group ring consideration, this is

$$\sum_{t=1}^{Q}\sum_{t'=1}^{Q}\sum_{j=0}^{2^{s_t}-1}\sum_{j'=0}^{2^{s_t}-1} y_t z_t^j D_{t,j} D_{t',j'}^{(-1)} z_{t'}^{-j'} y_{t'}^{-1}$$
$$= \sum_{t=t',j=j'} D_{t,j} D_{t,j}^{(-1)} + \sum_{t=t'}\sum_{j\neq j'} z_t^{j-j'} D_{t,j} D_{t,j'}^{(-1)}$$
$$+ \sum_{t\neq t'}\sum_{j,j'} y_t z_t^j z_{t'}^{-j'} y_{t'}^{-1} D_{t,j} D_{t',j'}^{(-1)}$$
$$= k-\lambda+\lambda \sum g_i H.$$

The part of the sum where $t=t'$ is the differences within one K-matrix. The following lemma considers part of the $t=t'$ case, and it is important in generalizing the group ring equation over to the nonabelian case.

LEMMA 2.1. $\sum_{j=0}^{2^{s_t}-1-f} D_{t,j} D_{t,j+f}^{(-1)} + \sum_{j=2^{s_t}-f}^{2^{s_t}-1} z_t^{2^{s_t}} D_{t,j} D_{t,j+f-2^{s_t}}^{(-1)} = 2^{s_t+d-1}H$ *for every* $1 \leqslant f \leqslant 2^{s_t}-1$.

Proof. Consider all pairs $y_{t'} z_{t'}^{j'}$ and $y_{t''} z_{t''}^{j''}$ so that $y_{t'} z_{t'}^{j'} z_{t''}^{-j''} y_{t''}^{-1} = h_{t',t''} z_t^f$, for some $h_{t',t''}$. Notice that the sum in the statement of this lemma comes from all the pairs within the K-matrix M_t whose difference of y's and z's is in the coset of z_t^f. Because D is a difference set, we must have

$$z_t^f\left[\sum_{j=0}^{2^{s_t}-1-f} D_{t,j} D_{t,j+f}^{(-1)} + \sum_{j=2^{s_t}-f}^{2^{s_t}-1} z_t^{2^{s_t}} D_{t,j} D_{t,j+f-2^{s_t}}^{(-1)} + \sum_{pairs} h_{t',t''} D_{t',j'} D_{t'',j''}^{(-1)}\right]$$
$$= z_t^f\,[\lambda H].$$

Consider the sums without the z_t^f; we will use both directions of Lemma 1.2 to analyze the sum in this lemma. If χ is any nonprincipal character on H, the sum of the character values on the right-hand side is 0. Thus, the sum on the left-hand side must also be 0. There are two cases: first, suppose that $\chi \in [\chi_t]$. $\chi(D_{t',j'}) = \sum_{d\in D_{t',j'}} \chi(d) = 0$ whenever $t \neq t'$ (this is a general property of K-matrices: either part (1) of the definition or χ nonprincipal on K_t will be true, and that gives a sum of 0). The third sum on the left-hand side has the property that each term contains at least one $D_{t',j'}$ where $t\neq t'$. Thus, each term is 0, so the sum must be 0. Therefore, the character sum over the first two sums on the left-hand side must also be 0. Now suppose that $\chi \notin [\chi_t]$, $\chi \neq \chi_0$. Just as above, $\chi(D_{t,j}) = 0$, so again the first two sums on the left-hand side must have character sum of 0. Thus, those two always have a character sum of 0, so by the reverse of Lemma 1.2, those must be a multiple of H. A counting argument yields the multiple to be 2^{s_t+d-1}. ∎

The key observation to make here is that if $\chi \in [\chi_t]$, then $\chi(z_t^{2^{s_t}}) = -1$. This is because $z_t^{2^{s_t}} \in H - K_t$, but $z_t^{2^{s_t}+1} \in K_t$. This observation will be used in the nonabelian case.

We end this section with another application of Lemma 1.2.

LEMMA 2.2. *If $t \neq t'$, then $D_{t,j} D_{t',j'}^{(-1)} = 2^{d-1} H$.*

Proof. Every nonprincipal character χ is in an equivalence class, say t'': t'' is different from at least one of t or t', so χ of that D will be 0. Thus, $\chi(D_{t,j} D_{t',j'}^{(-1)}) = 0$ for every χ. By Lemma 1.2, it must be a constant multiple of H, and a counting argument gives a constant of 2^{d-1}. ∎

3. THE NONABELIAN CASE

For this section, let G be a group of order 2^{2d+2} with a central subgroup H of order 2^{d+1}. Also, suppose that there is a $c \in G - H$, so that $\text{ord}(c) = \text{ord}(cH) \geqslant \exp(H)$ or $\text{ord}(c)/2 = \text{ord}(cH) \geqslant \exp(H)$. Since H is abelian, consider the equivalence classes of characters $[\chi_0], [\chi_1], ..., [\chi_Q]$ on H, as in Section 2. For each $[\chi_t]$ define the K-matrix M_t as follows:

(a) $h_t K_t$ is a generator of H/K_t, where $K_t = \text{Kern}(\chi_t)$.

(b) Pick z_t exactly as in the abelian case (either $h_t c^{2^{e-s_t}}$, $h_t c^{2^{e-s_t-1}}$, or $c^{2^{e-s_t-1}}$).

(c) Pick the y_t using the algorithm of Section 2 (the coset representatives for H can be written $a_1 c, a_1 c^2, ..., a_m c^{e-1}, a_m$, and the same algorithm can be applied to this list as in the abelian case).

THEOREM 3.1. *Suppose G is a group of order 2^{2d+2} with a central subgroup of order 2^{d+1}; if there is a $c \in G - H$ so that* (i) $\text{ord}(c) = \text{ord}(cH) \geqslant \exp(H)$ *or* (ii) $\text{ord}(c)/2 = \text{ord}(cH) \geqslant \exp(H)$, *then $D = \bigcup_{t=1}^{Q} \bigcup_{j=0}^{2^{s_t}-1} y_t z_t^j D_{t,j}$ is a difference set in G.*

Proof. Since H is a central subgroup, the coset representatives will commute with the $D_{t,j}$. Thus, the group ring sum reduces to

$$\sum_{t,t',j,j'} y_t z_t^j z_{t'}^{-j'} y_{t'}^{-1} D_{t,j} D_{t',j'}^{(-1)}$$

$$= \sum_{t,j} D_{t,j} D_{t,j'}^{(-1)} + \sum_t y_t \left[\sum_{j \neq j'} z_t^{j-j'} D_{t,j} D_{t',j'}^{(-1)} \right] y_t^{-1}$$

$$+ \sum_{t \neq t',j,j'} y_t z_t^j z_{t'}^{-j'} y_{t'}^{-1} D_{t,j} D_{t',j'}^{(-1)}.$$

The first sum on the right-hand side is the same as the sum in the abelian case, which is $k-\lambda+\lambda H$. Lemma 2.1 applies to the second sum because $\chi_t(z_t^{2^{s_t}})=-1$ (notice that $z_t^{2^{s_t}}\in H-K_t$, but $z_t^{2^{s_t+1}}\in K_t$); thus, the second sum is $\sum_{t=1}^{Q} y_t[\sum_{f=1}^{2^{s_t}-1} 2^{d-1+s_t} z_t^f H]\, y_t^{-1}$. The fact that H is central implies that this sum is $\sum_{t=1}^{Q}\sum_{f=1}^{2^{s_t}-1} 2^{d-1+s_t} y_t z_t^f y_t^{-1} H$. Finally, the third sum has each term as a coset representative times $2^{d-1}H$, by Lemma 2.2. Since the coset representatives form a $(2^{d+1}, 2^{d+1}-1, 2^{d+1}-2)$ difference set, each coset is in this sum $2^{d-1}(2^{d+1}-2)=2^{2d}-2^d=\lambda$ times. ∎

Example. Let a_1, a_2, a_3, and a_4 be the generators of G with $a_1^{2^n}=a_2^{2^n}=a_3^{2^n}=a_4^{2^n}=1$, $a_2^{-1}a_1a_2=a_1^{2^r+1}$. If $r\geqslant n/2$, then choose $H=\langle a_1^{2^{n-r}}, a_2^{2^{n-r}}, a_3^{2^{2r-n}}\rangle$ as a central subgroup of size 2^{2^n}. If we choose $c=a_4$, it is easy to see that the conditions of the theorem have all been met. Thus, these groups all have difference sets.

4. Questions

This generalization leads to two functions:

1. Suppose for every $1\leqslant t\leqslant Q$, we can find a z_t so that $\operatorname{ord}(z_t H)=2^{s_t}$, and $\chi_t(z_t^{2^{s_t}})=-1$; does this imply that G has a difference set? This is what makes Lemma 2.1 true in the nonabelian case, and it will make the K-matrices work if we can choose the y_t to satisfy the definition.

2. What can we do with the K-matrix structure if H is a normal abelian subgroup of order 2^{d+1} (not neccessarily central)? This is the K-matrix question related to Dillon's conjecture, which has to do with normal elementary abelian subgroups. This would be a very powerful result, because all 56,092 groups of order 256 have a normal abelian subgroup of order 16 (see [4]), so we could attack the existence of difference sets in every group of order 256 with K-matrices.

References

1. K. T. Arasu, Recent results in difference sets, "Coding and Design Theory, Part II," The IMA Volumes (21), Springer-Verlag, 1990.
2. J. Davis, Difference sets in abelian 2-groups, *J. Comb. Theory Ser. A*, July, 1991.
3. J. F. Dillon, Difference Sets in 2-Groups, Proc. Amer. Math. Soc., to appear.
4. B. Huppert, "Endliche gruppen I," Springer-Verlag, New York/Berlin, 1967.
5. R. G. Kraemer, Proof of a conjecture on Hadamard 2-groups, submitted.
6. E. S. Lander, "Symmetric Designs: An Algebraic Approach," London Math. Society Lecture Note Series, Vol. 74, Cambridge Univ. Press, Cambridge/New York, 1983.
7. R. Turyn, Character sums and difference sets, *Pacific J. Math.* (1965), 319–346.