7-1991

A Result on Dillon's Conjecture in Difference Sets

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

Recommended Citation

Davis, James A. "A Result on Dillon's Conjecture in Difference Sets." *Journal of Combinatorial Theory, Series A* 57, no. 2 (July 1991): 238-42. doi:10.1016/0097-3165(91)90047-K.

JOURNAL OF COMBINATORIAL THEORY, Series A 57, 238–242 (1991)

A Result on Dillon's Conjecture in Difference Sets

JAMES A. DAVIS

University of Richmond, Richmond, Virginia 23173

Communicated by the Managing Editors

Received January 15, 1989

Dillon has conjectured that any group of order 2^{2d+2} with a normal subgroup isomorphic to Z_2^{d+1} will have a difference set. He was able to show that this is true if the subgroup is central: this paper extends that idea to noncentral subgroups. © 1991 Academic Press, Inc.

1. INTRODUCTION

A difference set in a finite group is a subset $D \subset G$ so that every nonidentity element of G can be written as a difference of elements of D in precisely λ ways. The order of G is v and the size of D is k. These can be considered in groups of any order, but this paper will be concerned with groups of order a power of 2.

Dillon [2] provided a construction for a difference set in groups of order 2^{2d+2} if the group has a normal subgroup isomorphic to Z_2^{d+1}. He was able to show that the construction works if the subgroup is central, but difficulties arose in the general case. This paper explores cases when the subgroup is not central, and we provide a sufficient condition for the construction to work.

It is helpful to consider the ring $Z[G]$. If $A \subset G$, we will abuse notation by writing $A = \sum_{a' \in A} a'$ as an element of $Z[G]$. Also, $A^{(-1)} = \sum_{a' \in A} (a')^{-1}$. By the definition of a difference set, $D \subset G$ is a difference set iff $DD^{(-1)} = (k - \lambda)\, 1 + \lambda G$.

2. CONSTRUCTION

Let G be a group of order 2^{2d+2} with normal subgroup H isomorphic to Z_2^{d+1}. Consider the hyperplanes of H; i.e., the $2^{d+1} - 1$ subgroups of H of order 2^d (call them D_i, $i = 1, 2, ..., 2^{d+1} - 1$). Let $g_1, g_2, ..., g_{2^{d+1}-1}$ be

0097-3165/91 $3.00

elements of G in distinct cosets of H, and define $D=\bigcup_{i=1}^{2^{d+1}-1} g_iD_i$. In the group ring $Z[G]$,

$$DD^{(-1)}=\sum_i g_iD_i\sum_j D_j^{(-1)}g_j^{-1}=\sum_{i,j} g_iD_iD_j^{(-1)}g_j^{-1}.$$

In Dillon's paper, this constitutes a difference set in G if the map $\phi\colon D_i \to g_iD_ig_i^{-1}$ is a permutation of the hyperplanes. Define a non-degenerate bilinear form on H and write $D_i=\langle h_i\rangle^{\perp}$ (the form gives a polarity between the points and the hyperplanes). Thus, $g_iD_ig_i^{-1}=g_i(\langle h_i\rangle^{\perp})\,g_i^{-1} = \langle h_j\rangle^{\perp}$ for some j. If we define the product $\langle h_i\rangle^{\perp}\,\langle h_j\rangle^{\perp}=\langle h_ih_j\rangle^{\perp}$, then the set of hyperplanes together with H will form an elementary abelian group (called H'). Thus, ϕ will be a permutation of the hyperplanes if and only if $g_i\langle h_j\rangle^{\perp}\,g_i^{-1}$ is a permutation of the elements of H'.

3. Main Result

Lemma 3.1. *Consider $\sum_{i=1}^{n} a_i$, where a_i are all integral powers of 2, and $a_i \geqslant a_{i+1}$, $i=1, 2, ..., n-1$. If $a_1 \leqslant 2^s$ for some s and $\sum_{i=1}^{n} a_i \geqslant 2^s$, then there is a partial sum so that $\sum_{i=1}^{m} a_i=2^s$.*

Proof. Suppose m is the biggest number so that $\sum_{i=1}^{m-1}<2^s$: thus, $a_m \geqslant (2^s-\sum_{i=1}^{m-1} a_i)$. Since a_m is a power of 2 less than 2^s, a_m divides 2^s; also, since the sum is decreasing powers of 2, a_m divides $\sum_{i=1}^{m-1} a_i$. However, a_m cannot divide $(2^s-\sum_{i=1}^{m-1} a_i)$ if it is strictly greater than it, so $a_m=2^s-\sum_{i=1}^{m-1} a_i$. Thus, $\sum_{i=1}^{m} a_i=2^s$. ▮

Lemma 3.2. *Let G be a group of order 2^{2d+2}, H the normal elementary abelian subgroup of order 2^{d+1}, and H' the subgroup of hyperplanes of H. Suppose that the size of the largest conjugacy class in H' is 2^t. If $|C_G(H')| = 2^{d+1+s} \geqslant 2^{d+1+t}$, then for every $h\in H'$ there is a g_h so that $g_hhg_h^{-1} \neq g_{h'}h'g_{h'}^{-1}$ when $h\neq h'$, and the g_h are in distinct cosets of H.*

Proof. Let $x_1, x_2, ..., x_{2^t}$ be a conjugacy class in H'. Pick $g\in G$: $g_{x_i}=gz_i$, where $z_i\in C_G(H')$ are all in distinct cosets (we can do this because $|C_G(H')| \geqslant 2^{d+1+t}$). Suppose $g_{x_i}x_ig_{x_i}^{-1}=g_{x_j}x_jg_{x_j}^{-1}$: this implies that

$$gz_ix_iz_i^{-1}g^{-1}=gz_jx_jz_j^{-1}g^{-1}$$

$$gx_ig^{-1}=gx_jg^{-1}$$

$$x_i=x_j.$$

Thus, this property works on this conjugacy class: we need to show that it works on all the other conjugacy classes. If we order the conjugacy classes in H by size, Lemma 3.1 implies that there will be a partial sum of these adding to 2^s. Continue the process shown above on all these classes in the partial sum. This will use all the distinct cosets represented by $C_G(H')$.

Pick a $g' \in G$ so that g' is not in any of the cosets represented thus far. Start the assigning process again on a new conjugacy class, say $y_1, y_2, ..., y_{2^r}$ so that $g_{y_i} = g'z_i$. These new representatives will all be in different cosets than the one above, since $C_G(H') \lhd G$. This can be continued on a new partial sum of conjugacy classes that adds to 2^s by Lemma 3.1. Continue this procedure until all the elements of H' are assigned representatives. This satisfies the conditions of the lemma. ▌

THEOREM 3.1. *Let G be a group of order 2^{2d+2} with a normal subgroup $H \cong Z_2^{d+1}$. If H' has conjugacy classes of size less than 2^t and $|C_G(H)| \geqslant 2^{d+1+t}$, then G has a difference set.*

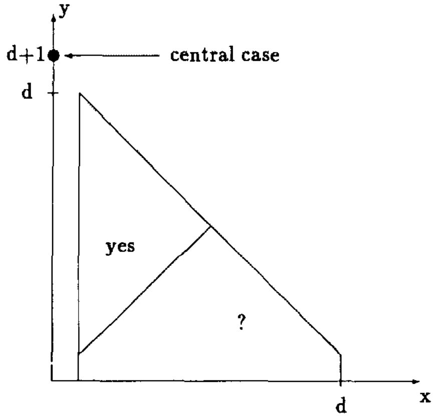
Proof. Dillon's construction will work if we can assign coset representatives to the $D_i = \langle x_i \rangle^\perp$ so that $g_i D_i g_i^{-1}$ is a permutation of the hyperplanes. Choose these representatives as in the above Lemma 3.2. ▌

A picture of this theorem can be obtained as follows: for $|G| = 2^{2d+2}$, $H \cong Z_2^{d+1}$, define

$$\psi: G \rightarrow \left(\log_2(|\text{c.c.}|), \log_2\left(\frac{|C_G(H')|}{2^{d+1}}\right)\right),$$

where |c.c.| is the size of the largest conjugacy class in H'.

Other than the case where H' is central (where the x-coordinate is 0), ψ maps the groups into a triangular shaped region in the xy-plane ($x = \log_2(|\text{c.c.}|)$ and $y = \log_2(C_G(H')/2^{d+1})$) so that $1 \leqslant x$, $y \leqslant d$. The top boundary comes from the relationship $|\text{c.c.}|\ |C_G(H')| \leqslant 2^{2d+2}$. The theorem implies that any group above the diagonal has a difference set. Pictorially,



The following corollary gives a condition which guarantees that the group will be above the diagonal.

COROLLARY 3.1. *Suppose that $H \lhd G$, $|G| = 2^{2d+2}$, and $H \cong Z_2^{d+1}$. Also suppose $|Z(G) \cap H'| = 2^{d+1-s}$, $0 \leqslant s \leqslant d$, and that the largest conjugacy class in H' has size at most $2(d+1)/(s+1)$. Then G has a difference set.*

Proof. Pick a generating set for H', $x_1, ..., x_s, x_{s+1}, ..., x_{d+1}$ so that $\langle x_{s+1}, ..., x_{d+1} \rangle$ generates $Z(G) \cap H'$. By the theorem, we have to show that

$$|C_G(H')| \geqslant 2^{d+1+(d+1)/(s+1)}.$$

By the product formula for subgroups, if H and K are subgroups of a group G, then

$$|H \cap K| = \frac{|H|\ |K|}{|HK|} \geqslant \frac{|H|\ |K'|}{|G|}.$$

This generalizes as follows: if $H_1, H_2, ..., H_n$ are n subgroups of G, then

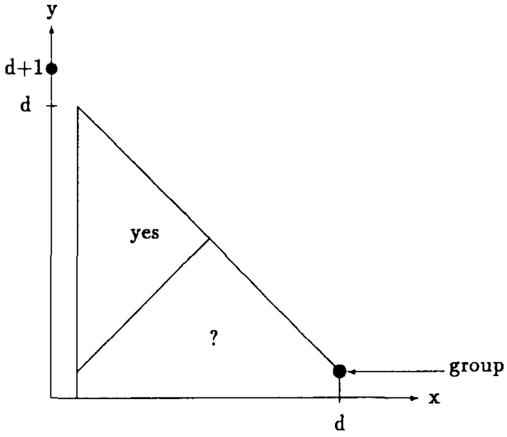
$$\begin{aligned} |H_1 \cap H_2 \cap \cdots \cap H_n| &= \frac{|H_1|\ |H_2 \cap H_3 \cap \cdots \cap H_n|}{|H_1(H_2 \cap H_3 \cap \cdots \cap H_n)|} \\ &\geqslant \frac{|H_1|\ |H_2 \cap H_3 \cap \cdots \cap H_n|}{|G|} \\ &\geqslant \cdots \\ &\geqslant \frac{|H_1|\ |H_2| \cdots |H_n|}{(|G|)^{n-1}}. \end{aligned}$$

In this situation, the subgroups of G are $C_G(x_i)$, $i = 1, 2, ..., s$. Also, $|G| = 2^{2d+2}$, and $|C_G(x_i)| = |G|/|\text{c.c.}| \geqslant 2^{2d+2-(d+1)/(s+1)}$. Thus,

$$\begin{aligned} |C_G(H')| &= |C_G(x_1) \cap C_G(x_2) \cap \cdots \cap C_G(x_s)| \\ &\geqslant \frac{|C_G(x_1)|\ |C_G(x_2)| \cdots |C_G(x_s)|}{(2^{2d+2})^{s-1}} \\ &\geqslant 2^{(2d+2-(d+1)/(s+1))s-(2d+2)(s-1)} \\ &= 2^{d+1+(d+1)/(s+1)}. \quad \blacksquare \end{aligned}$$

Remark. Using the ideas in this paper, the difficult cases occur when the subgroup H' has a large conjugacy class. One example of such a group is the semidirect product of Z_2^{d+1} with itself. This is generated by

$\langle x_1, x_2, ..., x_{d+1}, y, h_1, h_2, ..., h_d \rangle$. In this group, $H = \langle y, h_1, h_2, ..., h_d \rangle$, and the (noncommuting) relationships are $x_i y x_i^{-1} = y h_i$; $i = 1, 2, ..., d$. The conjugacy class of y has size 2^d, which is as large as possible. This would be a good group to explore when considering the generalization of Dillon's conjecture, since when we consider the picture of where ψ sends this group,



References

1. K. T. Arasu, Recent Results on Difference Sets, *in* "Proceedings, IMA, June 1988."
2. J. F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory Ser. A* **40** (1985), 9–21.
3. R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1–10.
4. J. J. Rotman, "An Introduction to the Theory of Groups," 3rd ed., Allyn & Bacon, Rockleigh, NJ, 1984.