1991

A Note on Nonabelian (64, 28, 12) Difference Sets

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

Recommended Citation

Davis, James A. "A Note on Nonabelian (64, 28, 12) Difference Sets." *Ars Combinatoria* 32 (1991): 311-14.

A Note on Nonabelian (64, 28, 12) Difference Sets

J.A. Davis

University of Richmond
VA 23173 U.S.A.

Abstract. The existence of difference sets in abelian 2-groups is a recently settled problem [5]; this note extends the abelian constructs of difference sets to nonabelian groups of order 64.

1. Introduction.

A difference set D in a finite group G (of order v) is a subset of size k so that every nonidentity element of G can be represented λ times as differences from elements in D. For groups of order a power of 2, the existence of difference sets in the abelian groups is a recently settled problem [5]. The nonabelian case is more difficult; this paper discusses a technique for using the structure of the abelian difference sets to obtain difference sets in nonabelian groups of order 64.

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 $DD^{(-1)} = (k - \lambda)1 + \lambda G$. In the $v = 64$ case, this is $DD^{(-1)} = 16(1) + 12G$.

All groups in this paper will be written multiplicatively, including abelian groups. Subgroups will be denoted $\langle \cdot , \cdot \rangle$, where the generators are included in the brackets.

2. The abelian case.

The abelian case $Z_{16} \times Z_4$ is discussed in [1], [2], [4].

Theorem 2.1. *$Z_{16} \times Z_4$ has a difference set.*

We will provide the difference set and leave it to the reader to verify the theorem (either by a straight check or by character theory). All elements of the group can be written as powers of a and b, where $a^{16} = b^4 = 1$. If we take the subgroup $H = \langle a^4, b^2 \rangle$, we can write $G = \cup g_i H$.

Take the following subsets of H:

$$\begin{array}{ccccccc} D_2 & D_3 & D_4 & D_5 & D_5' & D_6 & D_6' \\ \langle a^4 \rangle & \langle a^8, b^2 \rangle & \langle a^4 b^2 \rangle & \Big(\begin{smallmatrix} \langle a^8 b^2 \rangle \\ \cup a^4 \langle a^8 b^2 \rangle \end{smallmatrix} & \begin{smallmatrix} a^{12} \langle a^8 b^2 \rangle \\ \cup a^8 \langle a^8 b^2 \rangle \end{smallmatrix} \Big) & \Big(\begin{smallmatrix} \langle b^2 \rangle \\ \cup a^4 \langle b^2 \rangle \end{smallmatrix} & \begin{smallmatrix} a^{12} \langle b^2 \rangle \\ \cup a^8 \langle b^2 \rangle \end{smallmatrix} \Big) \end{array}$$

The claim is that $aD_2 \cup abD_3 \cup a^3 D_4 \cup D_5 \cup bD_5' \cup a^2 D_6 \cup a^6 b D_6'$ is a difference set in $Z_{16} \times Z_4$.

The following lemma is proved in [3].

Lemma 2.2. *If $i \neq j$, then $D_i D_j^{(-1)} = 2H$.*

This lemma excludes two important cases, which are covered in the next lemma.

Lemma 2.3.

(a) $D_5 D_5'^{(-1)} = D_5' D_5^{-1} = 4(a^8 + b^2) + 2(a^4 + a^4 b^2 + a^{12} + a^{12} b^2)$

(b) $D_6 D_6'^{(-1)} = D_6' D_6^{(-1)} = 4(a^8 + a^8 b^2) + 2(a^4 + a^4 b^2 + a^{12} + a^{12} b^2)$

(c) $D_5 D_5'^{(-1)} + b^2 D_5 D_5'^{(-1)} = 4H$

(d) $D_6 D_6'^{(-1)} + a^8 b^2 D_6 D_6'^{(-1)} = 4H$.

Notice that these lemmas can be considered in the group ring $Z[H]$ since all the D_i are subsets of H.

3. The nonabelian case.

Let $\overline{G}$ be any group of order 64 with a normal subgroup $\overline{H} \cong Z_4 \times Z_2$. We can choose an isomorphism $f: H \to \overline{H}$, where H is the $Z_4 \times Z_2$ from the abelian case. Define $\overline{D}_i = \{f(d_i) \mid d_i \in D_i\}$.

Theorem 3.1. *A group $\overline{G}$ with a normal subgroup $\overline{H}$ isomorphic to $Z_4 \times Z_2$ has a difference set if:*

(a) *there are 4 distinct coset representatives $\overline{g}_5, \overline{g}_5', \overline{g}_6, \overline{g}_6'$ in $\overline{G}/\overline{H}$ so that $\overline{g}_5 (\overline{g}_5')^{-1} = \overline{g}_5' \overline{g}_5^{-1} (f(b^2))$ and $\overline{g}_6 (\overline{g}_6')^{-1} = \overline{g}_6' \overline{g}_6^{-1} (f(a^8 b^2))$,*

(b) $\overline{g}\,\overline{D}_i \overline{D}_i^{(-1)} \overline{g}^{-1} = \overline{D}_i \overline{D}_i^{(-1)}$ *for every $\overline{g} \in \overline{G}$,*

(c) $\overline{g}_5 \overline{D}_5 \overline{D}_5'^{(-1)} \overline{g}_5'^{-1} = \overline{g}_5 \overline{g}_5'^{-1} \overline{D}_5 \overline{D}'^{(-1)}, \overline{g}_5' \overline{D}_5' \overline{D}_5^{(-1)} \overline{g}_5^{-1} = \overline{g}_5' \overline{g}_5^{-1} \overline{D}_5' \overline{D}_5^{(-1)}$, *and the same if we replace 5 by 6.*

Proof: Pick three distinct coset representatives $\overline{g}_2, \overline{g}_3, \overline{g}_4$ in $\overline{G}/\overline{H}$ that are also distinct from $\overline{g}_5, \overline{g}_5', \overline{g}_6, \overline{g}_6'$. We claim that $\overline{D} = \overline{g}_2 \overline{D}_2 \cup \overline{g}_3 \overline{D}_3 \cup \overline{g}_4 \overline{D}_4 \cup \overline{g}_5 \overline{D}_5 \cup \overline{g}_5' \overline{D}_5' \cup \overline{g}_6 \overline{D}_6 \cup \overline{g}_6' \overline{D}_6'$ is a difference set in $\overline{G}$. Consider the group ring equation

$$\overline{D}\,\overline{D}^{(-1)} = \sum_{i,j} \overline{g}_i \overline{D}_i \overline{D}_j^{(-1)} \overline{g}_j^{-1}. \tag{1}$$

We can apply Lemmas 2.2 and 2.3 to this situation since f is a group ring isomorphism from $Z[H]$ to $Z[\overline{H}]$. If $i \neq j$, Lemma 2.2 implies

$$\overline{g}_i \overline{D}_i \overline{D}_j^{(-1)} \overline{g}_j^{-1} = \overline{g}_i (2\overline{H}) \overline{g}_j^{-1} = \overline{g}_i \overline{g}_j^{-1} (2\overline{H}). \tag{2}$$

Combining Lemma 2.3, (a), and (c),

$$\begin{aligned} &\overline{g}_5 \overline{D}_5 \overline{D}_5'^{(-1)} \overline{g}_5'^{-1} + \overline{g}_5' \overline{D}_5' \overline{D}_5^{(-1)} \overline{g}_5^{-1} \\ &= \overline{g}_5 \overline{g}_5'^{-1} \overline{D}_5 \overline{D}_5'^{(-1)} + \overline{g}_5' \overline{g}_5^{-1} \overline{D}_5' \overline{D}_5^{(-1)} \\ &= \overline{g}_5 \overline{g}_5'^{-1} \overline{D}_5 \overline{D}_5'^{(-1)} + \overline{g}_5 \overline{g}_5'^{-1} f(b^2) \overline{D}_5 \overline{D}_5'^{(-1)} \\ &= \overline{g}_5 \overline{g}_5'^{-1} (f[D_5 D_5'^{(-1)} + b^2 D_5 D_5'^{(-1)}]) \\ &= \overline{g}_5 \overline{g}_5'^{-1} (f(4H)) = \overline{g}_5 \overline{g}_5'^{-1} (4\overline{H}) \end{aligned} \tag{3}$$

$$\overline{g}_6\overline{D}_6\overline{D}_6'^{(-1)}\overline{g}_6'^{-1} + \overline{g}_6'\overline{D}_6'\overline{D}_6^{(-1)}\overline{g}_6'^{-1} = \overline{g}_6\overline{g}_6'^{-1}(4\overline{H}). \tag{4}$$

Putting (1), (2), (3), (4) and (b) together,

$$\begin{aligned}
&\overline{D}\,\overline{D}^{(-1)} \\
&= \Big(\sum_{i\neq j}\overline{g}_i\overline{g}_j^{-1}\Big)2\overline{H} + \sum_i \overline{g}_i\overline{D}_i\overline{D}_i^{(-1)}\overline{g}_i^{-1} + \overline{g}_5\overline{g}_5'^{-1}(4\overline{H}) + \overline{g}_6\overline{g}_6'^{-1}(4\overline{H}) \\
&= \Big(\sum_{i\neq j}\overline{g}_i\overline{g}_j^{-1}\Big)2\overline{H} + \sum_i \overline{D}_i\overline{D}_i^{(-1)} + \overline{g}_5\overline{g}_5'^{-1}(4\overline{H}) + \overline{g}_6\overline{g}_6'^{-1}(4\overline{H}).
\end{aligned} \tag{5}$$

$\overline{D}$ is a union of 7 subsets of cosets of $\overline{H}$ out of 8 possible cosets. Thus, in $\overline{G}/\overline{H}$, the coset representatives used by $\overline{D}$ form an $(8,7,6)$ difference set. Other than $\overline{H}$, each of the 7 cosets appear 6 times, and each time they are multiplied by $2\overline{H}$; therefore, each coset is covered $6(2) = 12$ times. $\overline{H}$ is covered by $\sum_i \overline{D}_i\overline{D}_i^{(-1)}$, which is the same as the abelian case. This implies

$$\overline{D}\,\overline{D}^{(-1)} = 16\,\overline{1} + 12\overline{G}, \tag{6}$$

so $\overline{D}$ is a difference set in $\overline{G}$. ∎

Corollary 3.2. *The following groups have difference sets as defined in the proof of Theorem 3.1; the groups are defined by their generators, followed by the isomorphism f and $\overline{g}_5, \overline{g}_5', \overline{g}_6, \overline{g}_6'$.*

1.	$\bar{a}^{16} = \bar{b}^4 = 1$,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^3$;	$f\colon a^4 \to \bar{a}^4,\ b^2 \to \bar{b}^2$;	$(1, \bar{b}, \bar{a}^2, \bar{a}^4\bar{b})$
2.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^5$;	" ;	$(1, \bar{b}, \bar{a}^2, \bar{a}^6\bar{b})$
3.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^7$;	" ;	$(1, \bar{b}, \bar{a}^2, \bar{a}^3\bar{b})$
4.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^9$;	" ;	$(1, \bar{b}, \bar{a}^2, \bar{a}^6\bar{b})$
5.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^{11}$;	" ;	$(1, \bar{b}, \bar{a}^2, \bar{a}^4\bar{b})$
6.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^{13}$;	" ;	$(1, \bar{b}, \bar{a}^2, \bar{a}^6\bar{b})$
7.	$\bar{a}^{16} = \bar{b}^8 = 1$,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^7,\ \bar{a}^8 = \bar{b}^4$;	$f\colon a^4 \to \bar{a}^4,\ b^2 \to \bar{a}^4\bar{b}^2$;	$(\bar{a}^6\bar{b}, \bar{a}^2, 1, \bar{b})$
8.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^9,\ \bar{a}^8 = \bar{b}^4$;	" ;	$(\bar{a}^2, \bar{a}^6\bar{b}, 1, \bar{b})$
9.	" ,	$\bar{b}\bar{a}\bar{b}^{-1} = \bar{a}^{-1},\ \bar{a}^8 = \bar{b}^4$;	" ;	$(\bar{a}^6\bar{b}, \bar{a}^2, 1, \bar{b})$

Remarks.

(1) Not all groups which contain $Z_4 \times Z_2$ will have difference sets; $Z_{32} \times Z_2$ does not have a difference set, nor does the group defined by $a^{16} = b^4 = 1$, $bab^{-1} = a^{-1}$. Condition 3.1(a) fails in these cases, and that condition appears to be the most difficult of the three to satisfy.

(2) Theorem 3.1 can probably be generalized, but analogies would be needed for Lemma 2.3 and Condition 3.1(a).

(3) Groups 3.2.2, 3.2.4, and 3.2.6 are contained in [3]; they are included here for completeness.

References

1. J. Davis, *Difference sets in abelian 2-groups*, Ph.D. Dissertation (1987), University of Virginia.
2. J. Davis, *Difference sets in abelian 2-groups.* (to appear).
3. J. Davis, *Difference sets in nonabelian 2-groups*, IMA Proceedings (June, 1988).
4. J.F. Dillon, *Difference sets in abelian 2-groups*, Proc. Amer. Math. Soc. (1988).
5. R.G. Kraemer, *Proof of a conjecture on Hadamard 2-groups.* (to appear).
6. E.S. Lander, *Symmetric designs: an algebraic approach*, London Math Society Lecture Note Series **74** (1983).