Note
On central difference sets in certain non-abelian 2-groups
Rod Gow, Rachel Quinlan
Mathematics Department, University College, Belfield, Dublin 4, Ireland

Available online 2 August 2005

Received 13 July 2004

Abstract
In this note, we define the class of finite groups of Suzuki type, which are non-abelian groups of exponent 4 and class 2 with special properties. A group $G$ of Suzuki type with $|G| = 2^{2s}$ always possesses a non-trivial difference set. We show that if $s$ is odd, $G$ possesses a central difference set, whereas if $s$ is even, $G$ has no non-trivial central difference set.

© 2005 Elsevier Inc. All rights reserved.

MSC: 05B10

Keywords: Central difference set; Conjugacy class; Non-abelian 2-group

1. Introduction

Let $G$ be a finite multiplicatively written group of order $v$ and let $D$ be a $k$-subset of $G$, where $1 < k < v$. Let $\lambda$ be a positive integer. We say that $D$ is a $(v, k, \lambda)$-difference set in $G$ if for each non-identity element $g$ in $G$, there are exactly $\lambda$ ordered pairs $(a, b)$ in $D \times D$ with

$$g = ab^{-1}.$$ 

We say that $D$ is a central difference set in $G$ if it is a union of conjugacy classes in $G$. In the theory of difference sets in non-abelian groups, central difference sets seem to represent objects which are more tractable for study. We may mention in this respect a formula...
which offers the prospect of employing, for central difference sets, the character-theoretic methods which have proved to be effective in abelian difference sets [4, Theorem 12]. There is also a multiplier theorem for central difference sets, although it still awaits significant applications [1, Chapter VI, Theorem 4.14]. The purpose of this note is to construct, for each odd integer \( s \), central difference sets in certain non-abelian 2-groups of order \( 2^{2s} \) and exponent 4. The groups we use are what we call groups of Suzuki type, a family which includes the Sylow 2-subgroups of the simple Suzuki groups. While other examples of non-trivial central difference sets in non-abelian groups may be known, we note that the 1999 survey article of R. Liebler suggested that such difference sets might not exist [4, Conjectures, p. 351].

2. Groups of Suzuki type

Let \( G \) be a group of order \( 2^{2s} \), where \( s \geq 2 \) is an integer. Let \( Z(G) \) denote the centre of \( G \). We say that \( G \) is of Suzuki type if the following hold:

- \( Z(G) \) and \( G/Z(G) \) are both elementary abelian groups of order \( 2^s \).
- If \( x \) is any element of \( G - Z(G) \) and \( C_G(x) \) is the centralizer of \( x \) in \( G \), then \( |C_G(x)| = 2^{s+1} \).

Specific examples of groups of Suzuki type are provided by the Sylow 2-subgroups of the simple Suzuki groups. (We remark that there is a related concept of a Suzuki 2-group. See, for example, [3, Chapter 8, §7].) We construct these 2-groups in the following way. Let \( F \) be a finite field of order \( 2^{2s} \), where \( s \geq 2 \). Define a multiplication on the set \( F \times F \) by putting

\[(a, b)(c, d) = (a + c, a^2c + b + d)\]

for all ordered pairs \((a, b)\) and \((c, d)\) in \( F \times F \). It is straightforward to see that \( F \times F \) is a finite group of order \( 2^{2s} \), which we shall denote by \( G_s \). The identity element is \((0, 0)\) and the inverse of \((a, b)\) is \((a, a^3 + b)\). The centre \( Z(G_s) \) of \( G_s \) consists of all elements \((0, v)\) and is elementary abelian of order \( 2^s \). The quotient \( G_s/Z(G_s) \) is also elementary abelian of order \( 2^s \).

Let \( x \) be any element of \( G_s - Z(G_s) \). We may write \( x = (a, b) \), where \( a \neq 0 \). It is easy to check that \( C_{G_s}(x) \) consists of all elements \((c, d)\), where \( d \) is an arbitrary element of \( F \) and \( c = 0 \) or \( c = a \). Thus \( |C_{G_s}(x)| = 2^{s+1} \) and we see that \( G_s \) is a group of Suzuki type according to the definition above. There do, however, exist groups of Suzuki type that are not isomorphic to a group of the form \( G_s \). For instance, a Schur covering group (or stem cover) of an elementary abelian group of order 8 is a group of Suzuki type of order 64. There are 10 non-isomorphic such covering groups, including the group \( G_3 \).

Let \( G \) be a group of Suzuki type with \( |G| = 2^{2s} \). We will consider \( Z(G) \) to be a vector space of dimension \( s \) over \( \mathbb{F}_2 \). Given elements \( x \) and \( y \) in \( G \), let \([x, y] \) denote the commutator \( x^{-1}y^{-1}xy \). Since \( G \) is nilpotent of class 2, \([x, y] \in Z(G) \) and the relation

\[ [x, yz] = [x, y][x, z] \]
holds for all \( z \) in \( G \). Thus, if we fix \( x \) to be an element of \( G - Z(G) \) and let \( y \) run over \( G \), the commutators \([x, y]\) form a subgroup of \( Z(G) \). Moreover, since \([x, y] = 1\) if and only if \( y \in C_G(x) \), and \(|C_G(x)| = 2^{s+1}\), we see that there are \( 2^{s-1} \) different elements of the form \([x, y]\) and they therefore constitute a hyperplane, \( H_x \), say, of \( Z(G) \). The conjugacy class of \( x \) in \( G \) is the coset \( xH_x \).

The key point for the existence of a central difference set in \( G \) is the parity of \( s \). The next lemma holds only when \( s \) is odd.

**Lemma 1.** Let \( G \) be a group of Suzuki type with \(|G| = 2^{2s}\), where \( s \) is odd. Then each hyperplane of \( Z(G) \) is equal to some \( H_x \).

**Proof.** We give a character-theoretic proof. Suppose that there is a hyperplane \( H \) of \( Z(G) \) not equal to any \( H_z \), where \( z \) runs over the elements of \( G \). Let \( \lambda \) be a complex linear character of \( Z(G) \) whose kernel is \( H \). Let \( x \) be any element of \( G - Z(G) \). Since \( H_x \neq H \), there is some \( y \) in \( G \) with \( \lambda([x, y]) = -1 \). Let \( \gamma \) be an irreducible complex character of \( G \) lying over \( \lambda \) and let \( R \) be a representation of \( G \) with character \( \gamma \). Since \([x, y] \in Z(G)\), we have

\[
R([x, y]) = \lambda([x, y])I = -I.
\]

It follows then that

\[
R(y)^{-1}R(x)R(y) = -R(x).
\]

Taking traces, we obtain

\[
\gamma(x) = \text{trace } R(x) = -\text{trace } R(x) = -\gamma(x).
\]

We deduce that \( \gamma(x) = 0 \) for all \( x \in G - Z(G) \). On the other hand, since \( Z(G) \) is an elementary abelian 2-group, Schur’s Lemma implies that \( \gamma(z) = \pm \gamma(1) \) for all \( z \in Z(G) \). The orthogonality relations give

\[
|G| = \sum_{x \in G} |\gamma(x)|^2 = \sum_{z \in Z(G)} |\gamma(z)|^2 = |Z(G)|\gamma(1)^2
\]

and this implies that

\[
2^s = |G : Z(G)| = \gamma(1)^2.
\]

This is a contradiction, since it implies that \( s \) is even. Thus \( H \) equals some \( H_z \), as required. \( \square \)

3. Construction of a central difference set for odd \( s \)

Here, we show the existence of a central difference set in a group \( G \) of Suzuki type and order \( 2^{2s} \) whenever \( s \geq 3 \) is an odd integer. We make use of a very flexible construction due to J.F. Dillon. Let \( G \) be a group of order \( 2^{2s} \), where \( s \geq 1 \). Suppose that \( G \) contains
a central elementary abelian subgroup \(H\) of order \(2^s\). Let \(x_0, \ldots, x_{2^s-1}\) be a set of coset representatives for \(H\) in \(G\), with \(x_0 \in H\). Let
\[
P_1, \ldots, P_{2^s-1}
\]
denote the \(2^s - 1\) different hyperplanes in \(H\). Then the subset \(D\) of \(G\) defined by
\[
D = \bigcup_{i=1}^{2^s-1} x_i P_i
\]
is a difference set in \(G\) [2, p. 14].

**Theorem 1.** Let \(s \geq 3\) be an odd integer. Let \(G\) be a group of Suzuki type with \(|G| = 2^{2s}\). Then \(G\) contains a central difference set.

**Proof.** Let
\[
x_1, \ldots, x_{2^s-1}
\]
be a system of representatives for those cosets of \(Z(G)\) different from \(Z(G)\), as defined above. Let \(H_i\) denote the hyperplane \(H_{x_i}\). Since any element of \(G - Z(G)\) has the form \(x_i z\) for some index \(i\) and some \(z \in Z(G)\), it follows from Lemma 1 that the hyperplanes \(H_i\), where \(1 \leq i \leq 2^s - 1\), constitute all the hyperplanes of \(Z(G)\). Thus, following Dillon’s construction:
\[
D = \bigcup_{i=1}^{2^s-1} x_i H_i
\]
is a difference set in \(G\), and it is a union of conjugacy classes, since \(x_i H_i\) is the conjugacy class of \(x_i\). We have thus constructed a central difference set in \(G\). \(\Box\)

**4. Non-existence of a central difference set for even \(s\)**

We intend to show in this section that, although Dillon’s construction gives many difference sets in a group \(G\) of Suzuki type, there is no *central* difference set when \(|G| = 2^{2s}\) and \(s\) is even. Thus central difference sets are not as ubiquitous as might be inferred. We employ a character-theoretic argument that we think may be capable of proving the non-existence of central difference sets in other situations.

The following result is easily proved and we omit the details.

**Lemma 2.** Let \(G\) be a group of Suzuki type with \(|G| = 2^{2s}\) and suppose that \(s = 2t\) is an even positive integer. Then \(G\) has at least \(2(2^{2t} - 1)/3\) irreducible complex characters \(\chi\) of degree \(2^t\) which vanish on all elements outside \(Z(G)\). The kernel of each such \(\chi\) is a hyperplane of \(Z(G)\) and different \(\chi\) have different kernels.

We can now prove our non-existence theorem for central difference sets in groups of Suzuki type when \(s\) is even.
Theorem 2. Let \( s \geq 2 \) be an even integer. Then a group \( G \) of Suzuki type with \( |G| = 2^{2s} \) contains no non-trivial central difference set.

Proof. Suppose on the contrary that \( G \) contains a non-trivial central difference set \( D \). Since the complement of \( D \) is also central, we may assume that \( |D| < |G|/2 \). Then it follows from a theorem of Mann’s that \( |D| = 2^{2s-1} - 2^{s-1} \) and the order of \( D \) is \( 2^{2s-2} \) [5]. Let \( s = 2t \), where \( t \) is a positive integer and let \( \chi \) be an irreducible character of \( G \) of degree \( 2^t \), whose existence is guaranteed by Lemma 2. Let \( c = |D \cap Z(G)| \) and let \( D \) be the union of \( r \) conjugacy classes \( C_1, \ldots, C_r \) of \( G \). We may assume that the classes \( C_1, \ldots, C_c \) are contained in \( Z(G) \) and the remaining classes are not contained in \( Z(G) \). Let \( g_i \) be a representative of \( C_i \) for \( 1 \leq i \leq r \). Since \( \chi \) vanishes outside \( Z(G) \) and takes the value \( \pm \chi(1) \) on any element of \( Z(G) \), we have

\[
\frac{|C_i| \chi(g_i)}{\chi(1)} = \begin{cases} 
\varepsilon_i = \pm 1 & \text{if } 1 \leq i \leq c, \\
0 & \text{if } i > c.
\end{cases}
\]

It follows from Theorem 12 of Liebler [4] that

\[
\varepsilon_1 + \cdots + \varepsilon_c = \pm 2^{s-1}
\]

(in the final line of the statement of Theorem 12 in [4], the order \( n \) of \( D \) should be replaced by \( \sqrt{n} \)). We note also that \( |C_i| = 2^{s-1} \) for \( i > c \). Since \( D \) is a union of conjugacy classes, it follows that \( c \) is divisible by \( 2^{s-1} \). However, since \( |Z(G)| = 2^s \), we see that \( c \) is either \( 2^{s-1} \) or \( 2^s \). Now the equality \( c = 2^s \) implies that \( Z(G) \) is contained in \( D \). We claim that this is impossible. For suppose that \( Z(G) \) is contained in \( D \). Then, since \( Z(G) \) is not contained in the kernel of \( \chi \), elementary character theory shows that

\[
\sum_{g \in Z(G)} \chi(g) = 0
\]

and hence

\[
\varepsilon_1 + \cdots + \varepsilon_c = 0,
\]

which is a contradiction. Thus \( c = 2^{s-1} \) and we deduce that \( |D \cap Z(G)| = 2^{s-1} \).

Let \( z \) be any element of \( D \cap Z(G) \). It is clear that \( z^{-1}D \) is also a central difference set containing the identity. Replacing \( D \) by \( z^{-1}D \) if necessary, we may assume that the identity of \( G \) is in \( D \) and we may set \( C_1 \) to be the identity class. We now have

\[
\varepsilon_1 + \cdots + \varepsilon_{2^{s-1}} = \pm 2^{s-1},
\]

where each \( \varepsilon_i = \pm 1 \) and \( \varepsilon_1 = 1 \). It must be the case that each \( \varepsilon_i = 1 \) and hence \( D \cap Z(G) \) is contained in the kernel of \( \chi \). However, Lemma 2 shows that the kernel of each character \( \chi \) is a hyperplane in \( Z(G) \). Comparing orders, we deduce that \( D \cap Z(G) = \ker \chi \). Since different characters \( \chi \) have different kernels, and there are at least two different \( \chi \), by Lemma 2, we have a contradiction. Thus \( G \) has no central difference set when \( s \) is even. \( \square \)
5. Construction of central difference sets in direct products

We end this note by making a simple observation that shows how to construct further examples of central difference sets in non-abelian 2-groups. Let $G_1$ and $G_2$ be finite groups which contain Hadamard difference sets $D_1$ and $D_2$, respectively. Then

$$D = D_1(G_2 - D_2) \cup (G_1 - D_1)D_2$$

is a Hadamard difference set in $G_1 \times G_2$. See, for example, [2, p. 13]. It is easy to see that $D$ is central if $D_1$ and $D_2$ are central. Now, any non-trivial difference set in a finite 2-group is Hadamard by Mann’s theorem. Thus, we see that the class of 2-groups possessing a central difference set is closed under direct products and we may therefore construct further central difference sets in non-abelian 2-groups using the building blocks described in Theorem 1.

References