ON CENTRAL DIFFERENCE SETS IN CERTAIN NON–ABELIAN 2–GROUPS

ROD GOW AND RACHEL QUINLAN

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.

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 λ be a positive integer. We say that D is a (v, k, λ)–difference set in G if for each non–identity element g in G, there are exactly λ 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. The purpose of this note is to provide, for each odd integer s, an example of a $(2^{2s}, 2^{2s-1} - 2^{s-1}, 2^{2s-2} - 2^{s-1})$ central difference set in a non–abelian 2–group of exponent 4. We remark that, up to complementation, a non-trivial difference set in a 2–group always has parameters of this form, by a theorem of H.B. Mann, [4], Theorem 1. The group which we use is a Suzuki 2–group, although we show more generally that a group of so–called Suzuki type also possesses such a central difference set. 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, [3], 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 $|C_G(x)| = 2^{s+1}$.

Our main example of a group of Suzuki type is provided by the well–known Suzuki 2–groups, which we construct in the following way. Let F be a finite field of order 2^s, where $s \geq 2$. Define a multiplication on the set $F \times F$ by putting

$$(a, b)(c, d) = (a + c, a^2c + b + d)$$

1991 *Mathematics Subject Classification.* 05B10.
Key words and phrases. central difference set, conjugacy class, non–abelian 2–group.

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 and call a Suzuki 2–group. 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 arbitary 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 Suzuki 2–group. For example, a *covering group* (or stem cover) of an elementary abelian group of order 8 is a group of Suzuki type of order 64. There are several non–isomorphic such covering groups, including the Suzuki 2–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 λ 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 χ be an irreducible complex character of G lying over λ and let R be a representation of G with character χ. 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

$$\chi(x)=\operatorname{trace}R(x)=-\operatorname{trace}R(x)=-\chi(x).$$

We deduce that $\chi(x)=0$ 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 $\chi(z)=\pm\chi(1)$ for all $z\in Z(G)$. The orthogonality relations give

$$|G|=\sum_{x\in G}|\chi(x)|^2=\sum_{z\in Z(G)}|\chi(z)|^2=|Z(G)|\chi(1)^2$$

and this implies that

$$2^s=|G:Z(G)|=\chi(1)^2.$$

This is a contradiction, since it implies that s is even. Thus H equals some H_z, as required. □

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

$$H_1, \ldots, H_{2^s-1}$$

denote the $2^s - 1$ different hyperplanes in H. Then the subset D of G defined by

$$D = \bigcup_{i=1}^{2^s-1} x_i H_i$$

is a difference set in G, [1], 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. □

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 Lemma 1 is false when s is even. We again employ a character–theoretic argument that we think may be capable of proving the non–existence of central difference sets in other situations.

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

Proof. Let χ be an irreducible complex character of G. We note that $\chi(1)^2$ divides $|G : Z(G)|$. See, for example, Problem 3.6 of [2]. It follows that $\chi(1)$ is a divisor of 2^t. Now as G is of Suzuki type it is straightforward to see that G has 2^{2t} central conjugacy classes and $2^{2t+1} - 2$ non–central conjugacy classes, each of size 2^{2t-1}. Moreover, as $G/Z(G)$ is elementary abelian of order 2^{2t}, G has at least

2^{2t} irreducible characters of degree 1. Excluding these linear characters, suppose that G has exactly u irreducible characters of degree dividing 2^{t-1} and exactly v irreducible characters of degree 2^t. Then since the number of irreducible characters of G equals the number of conjugacy classes of G, it follows that $u+v = 2^{2t+1}-2$.

Recalling that

$$|G| = 2^{4t} = \sum_{\chi} \chi(1)^2,$$

where the sum extends over all irreducible characters χ of G, we obtain the inequality

$$2^{4t} \leq 2^{2t} + u2^{2t-2} + v2^{2t}$$

and hence

$$2^{2t+2} \leq 4 + u + 4v = 2^{2t+1} + 2 + 3v.$$

This implies that $v \geq 2(2^{2t}-1)/3$, as claimed.

Finally, let χ be an irreducible character of G of degree 2^t. We noted in the proof of Lemma 1 that $\chi(z) = \pm\chi(1) = \pm 2^t$ for all $z \in Z(G)$. The orthogonality relations give

$$|G| = 2^{4t} = \sum_{z \in Z(G)} |\chi(z)|^2 + \sum_{x \notin Z(G)} |\chi(x)|^2 = 2^{4t} + \sum_{x \notin Z(G)} |\chi(x)|^2$$

and this equality clearly implies that $\chi(x) = 0$ if $x \in G - Z(G)$. It follows that χ is determined by its restriction to $Z(G)$. We may write $\chi_{Z(G)} = 2^t\lambda$ where λ is a non–trivial linear character of $Z(G)$. The kernel of χ is then the kernel of λ, which is a hyperplane of $Z(G)$. Since λ is determined by its kernel, it is clear that different such χ have different kernels. □

We return briefly to a finite multiplicatively–written group G of order v and suppose that D is a (v,k,λ)–difference set in G. Given a non-empty subset S of G, we let $\widehat{S}$ denote the sum

$$\sum_{s \in S} s$$

in $\mathbb{C}G$. The fact that D is a (v,k,λ)–difference set is expressible by the equation

$$\widehat{D}\widehat{D}^{(-1)} = \lambda\widehat{G} + n1_G,$$

where $n = k - \lambda$ is the order of D, and $\widehat{D}^{(-1)}$ is the sum of the inverses of the elements in D.

Suppose now that D is central in G. Let R be a non–trivial irreducible complex representation of G with character χ. We may extend R to a representation of $\mathbb{C}G$, also denoted by R, and in this extended representation, $R(\widehat{D})$ clearly commutes with the elements $R(g)$ for all $g \in G$. Schur's Lemma implies that $R(\widehat{D}) = \mu I$ for some scalar μ. Since $R(\widehat{G}) = 0$, we obtain

$$R(\widehat{D})R(\widehat{D}^{(-1)}) = \mu\overline{\mu}I = \lambda R(\widehat{G}) + nI = nI,$$

so that the scalar μ satisfies $|\mu|^2 = n$. As D is central, it is the union of r, say, conjugacy classes $K_1, \ldots, K_r$. Each element $R(\widehat{K_i})$ is a scalar multiple of the identity, say $\mu_i I$, and

$$\mu_1 + \cdots + \mu_r = \mu.$$

By a well known theorem of Frobenius,

$$\mu_i = \frac{|K_i|\chi(g_i)}{\chi(1)},$$

where g_i is a representative of K_i. Moreover, each μ_i is an algebraic integer. Let $Z(\mathbb{C}G)$ denote the centre of $\mathbb{C}G$. The character χ determines a so–called central character ω_χ, which is a homomorphism $Z(\mathbb{C}G) \to \mathbb{C}$ given by

$$\omega_\chi(\widehat{K_i}) = \frac{|K_i|\chi(g_i)}{\chi(1)}.$$

Thus the scalar μ_i equals $\omega_\chi(\widehat{K_i})$ and

$$|\omega_\chi(\widehat{K_1}) + \cdots + \omega_\chi(\widehat{K_r})|^2 = n$$

for all non–principal irreducible characters χ.

We note also the following elementary property of the central characters.

Lemma 3. *Let G be a finite group and let N be a normal subgroup of G. Let ψ be an irreducible complex character of G that does not contain N in its kernel. Then $\omega_\psi(\widehat{N}) = 0$.*

Proof. We first note that N is a union of conjugacy classes of G, so $\widehat{N} \in Z(\mathbb{C}G)$. Suppose that $\omega_\psi(\widehat{N}) \neq 0$. It follows that

$$\sum_{g \in N} \psi(g) \neq 0.$$

This implies that the restriction of ψ to N contains the principal character 1_N of N. The irreducibility of ψ, together with Clifford's theorem, imply that N is contained in the kernel of ψ, contrary to assumption. Thus $\omega_\psi(\widehat{N}) = 0$. □

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 $|D| < |G|/2$. Thus Mann's theorem implies that $|D| = 2^{2s-1} - 2^{s-1}$ and the order of D is 2^{2s-2}. Let $s = 2t$, where t is a positive integer and let χ 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 $K_1, \ldots, K_r$ of G. We may assume that the classes $K_1, \ldots, K_c$ are central and the remaining classes are non–central. Since χ vanishes outside $Z(G)$, we have

$$\omega_\chi(\widehat{K_i}) = \begin{cases} \varepsilon_i = \pm 1, & \text{if } 1 \leq i \leq c; \\ 0, & \text{if } i > c. \end{cases}$$

It follows that

$$\omega_\chi(\widehat{D}) = \varepsilon_1 + \cdots + \varepsilon_c = \pm 2^{s-1},$$

since $\omega_\chi(\widehat{D})$ is clearly an integer. We note also that $|K_i| = 2^{s-1}$ 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 we have

$$\omega_\chi(\widehat{D}) = \omega_\chi(\widehat{Z(G)}) = 0$$

by Lemma 3, since $Z(G)$ is not contained in the kernel of χ. This 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 K_1 to be the identity class. We now have

$$\omega_\chi(\widehat{D}) = \varepsilon_1 + \cdots + \varepsilon_{2^{s-1}} = \pm 2^{s-1},$$

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 χ. However, Lemma 2 shows that the kernel of each character χ is a hyperplane in $Z(G)$. Comparing orders, we deduce that $D \cap Z(G) = \ker \chi$. Since different characters χ have different kernels, and there are at least two different χ, by Lemma 2, we have a contradiction. Thus G has no central difference set when s is even.

□

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, [1], 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 examples of central difference sets in non–abelian 2–groups using the examples described in Theorem 1.

References

[1] J.F. Dillon, *Variations on a scheme of McFarland for noncyclic difference sets*, J. Combin. Theory Ser. A **40** (1985), 9–21.

[2] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York–San Francisco–London, 1976.

[3] R.A. Liebler, *Constructive representation theoretic methods and non–abelian difference sets*, in *Difference Sets, Sequences and their Correlation Properties* (Bad Winsheim, 1998), 331–352. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542. Kluwer Acad. Publ., Dordrecht, 1999.

[4] H.B. Mann, *Difference sets in elementary abelian groups*, Illinois J. Math. **9** (1965), 212–217.

Mathematics Department, University College, Belfield, Dublin 4, Ireland
E-mail address: rod.gow@ucd.ie, rachel.quinlan@ucd.ie