

# On Difference Sets in Certain 2-Groups

Robert A. Liebler  
Colorado State University

Kenneth W. Smith  
Central Michigan University

IN MEMORY OF MARSHALL HALL, JR.

## Abstract

A representation theoretic sieve for studying difference sets in a group  $G$  is presented. A number of results of the form: "If  $G$  is a 2-group with a difference set  $D$  having a homomorphic image  $G/N$  of the form ..., then the distribution of  $D$  among the cosets of  $N$  is ..." are proven using explicit representations over cyclotomic integers. Corollaries include a celebrated result of Turyn "If  $G$  is abelian, then it has order greater than or equal to the square of half its exponent." The (nonabelian) "modular group" of order 64 is shown to possess a difference set and thus the Turyn bound does not extend to non abelian groups. This difference set also completes the last case of Dillon's program to decide the existence of difference sets in all the groups of order 64.

## 1 Introduction

Every nontrivial symmetric design with  $v$  a power of 2 has parameters:  $v = 4u^2$ ,  $k = 2u^2 - u$ ,  $\lambda = u^2 - u$ ,  $n = u^2$ , by a theorem of Mann [[5], II.3.17]. Thus, any difference set in a 2-group has these parameters and is in the parameter family called Menon difference sets [[5], VI.6.12]. Menon difference sets are related to certain Hadamard matrices and exist in great numbers whenever  $u$  is a power of 2. In case the group  $G$  is elementary abelian, there is an affine geometry construction and in case  $G$  is homocyclic of exponent 4 there is an elegant construction based on the units in an algebraic extension of the integers modulo 4.

Dillon [3] has raised the question of which 2-groups  $G$  admit difference sets and his question has been settled for all groups of order 64 except the "modular group".

$$\langle x, y | x^{32} = y^2 = 1, yxy = x^{17} \rangle.$$

The set  $\Delta$  where

$$\sum_{g \in \Delta} g = (1 + x^{16})[1 + x^4 + y + x^{12}y + x + x^9]$$

$$+ (1 + x^8)[x^2 + x^{-2} + x^8(x^5 + x^{-5} + x^{10}y + x^{-10}y) + x^{13}y + x^{-13}y]$$

is shown in Corollary (4.8) to be a difference set in this group as announced elsewhere by the second author and contrary to earlier claims of someone else. The same methods yield stronger results of the form: If  $G$  is a 2-group with a difference set  $\Delta$  having a homomorphic image  $G/N$  of the form ..., then the distribution of  $\Delta$  among the cosets of  $N$  is ... (Propositions (4.1), (4.3), (4.6)). Results of this form strongly restrict the search space if one is seeking out "new" difference sets.

With the concept of a sufficient representation, this paper sets out a representation theoretic (NOT character theoretic) framework that can be used to efficiently seek out (rule out) combinatorial solutions to specific equations in finite group rings. We hope to return to this rich subject in the future. In case the group is solvable, this framework can be implemented as a sieve-like algorithm.

It is a pleasure to acknowledge the encouragement and helpful comments of especially J. Dillon and R. McFarland. Portions of this work was done while the first author was visiting T. U. Braunschweig, FRG and MSRI in Berkeley, California and while the second author was visiting the National Security Agency Fort Meade, Maryland. The hospitality of these institutions is gratefully acknowledged.

## 2 Sufficient Representations

In view of the relative scarcity of results on nonabelian difference sets, it seems worthwhile to point out that the problem of verifying if a subset  $\Delta$  of  $G$  is a difference set is no less tractable in case  $G$  is nonabelian. More precisely, the problem is equivalent to verifying the difference set equation in each simple ideal of the complex group algebra  $CG$  of  $G$ . If  $G$  is abelian, there are  $|G|$  simple ideals each of which is one dimensional and each verification reduces to the computation of the norm of a Gauss sum. If  $G$  is not abelian then each verification reduces to the computation of the norm of a  $d$  by  $d$  matrix whose entries are Gauss sums — but the sum of the squares of the degrees of the matrices that arise in this way is still  $|G|$ . Thus the number of equations involving Gauss sums that must be verified is always  $|G|$ .

The problem of seeking out (ruling out) difference sets in  $G$  is equivalent to classifying the subsets  $\Delta$  of  $G$  satisfying:

$$\delta\delta^{(-1)} = n1 + \lambda j \text{ in a group ring,}$$

where

$$\delta = \sum_{g \in \Delta} g, \delta^{(-1)} = \sum_{g \in \Delta} g^{-1}, j = \sum_{g \in G} g,$$

$1$  is the identity element of  $G$  and  $n, \lambda$  are the usual parameters of the design.

Call a representation  $\varphi$  of  $G$  sufficient if whenever the equation

$$\varphi(\delta)\varphi(\delta^{(-1)}) = \varphi(n1 + \lambda j)$$

holds then  $\Delta \subset G$  is a difference set. Since the group algebra itself affords the regular representation of  $G$ , the regular representation of  $G$  is sufficient. It is natural to look for minimal sufficient representations. Warning: faithful representations need not be sufficient.

**Example 1** Let  $x$  generate a cyclic group  $G$  of order 21 and let  $\varphi$  be a faithful irreducible complex representation of  $G$ . Then  $\varphi(x)$  is a complex 21-th root  $\eta$  of unity. The faithfulness of  $\varphi$  requires that no two elements of  $G$  have the same image under  $\varphi$  and is equivalent to the requirement that  $\eta$  be primitive. Let  $\Delta = \{x^{2^i} | i = 0, 1, 2, 3, 4, 5\}$  and define  $\delta$  as above. Then  $\varphi(\delta)\varphi(\delta^{(-1)}) = 2$  (proof of this is given below). If this representation were sufficient, it would follow that  $\Delta$  is a difference set. But this is impossible because the parameter condition  $20\lambda = (v - 1)\lambda = k(k - 1) = 6 \cdot 5$  arising from the trivial representation fails for  $\Delta$ . In order to compute  $\varphi(\delta)\varphi(\delta^{(-1)})$ , set  $\omega = \eta^7$ , and  $\kappa = \nu^{15} + \nu^9 + \nu^{18}$ . Then

$$\varphi(\delta) = (\eta + \eta^{16} + \eta^4) + (\eta^8 + \eta^2 + \eta^{32}) = \omega\kappa + \omega^2\kappa = -\kappa,$$

so

$$\varphi(\delta)\varphi(\delta^{(-1)}) = \kappa\bar{\kappa}.$$

The result follows from the fact that  $\kappa$  is the image under  $\varphi$  of a difference set in  $\langle x^3 \rangle$ . □

**Theorem 2.1** Let  $K$  be a splitting field of characteristic zero for  $G$ . Suppose  $\Phi$  is a set of  $KG$ -representations such that every irreducible  $KG$ -representation is algebraically conjugate to a constituent of an element of  $\Phi$ . Then  $\varphi = \sum \oplus \Phi$  is sufficient.

nb. the term algebraically conjugate is defined in [2, p 471].

**Proof.** Suppose  $\Delta \subset G$  satisfies the required equation in  $\varphi$ . Then  $\Delta^\sigma = \Delta$  satisfies the same equation in  $\varphi^\sigma$  for each  $K$ -automorphism  $\sigma$ . It follows that  $\Delta$  satisfies the critical equation in every irreducible  $KG$ -representation, also in any representation that is a direct sum of irreducible  $KG$ -representations. By Maschke's theorem, the regular representation is of this type. □

**Corollary 2.2** The only groups for which the regular representation is (possibly) a minimal sufficient representation are the elementary abelian 2-groups.

**Proof.** A minimal sufficient representation is multiplicity free, so the regular representation is too, and  $G$  is abelian. If further, no two inequivalent representations are algebraically conjugate then the group is an elementary abelian 2-group.  $\square$

Of course all of this presumes that a candidate  $\Delta$  is in hand. The difficult problem of coming up with these candidates is being ignored. There really is no difficulty in finding solutions to the difference set equation in  $CG$ . The problem is that the solutions must represent the sum of a subset of the elements of  $G$  and so must be a "0,1" solution in  $ZG$ . It is therefore essential to keep track of which matrices represent elements of  $G$ . Perhaps the major philosophical point of the rest of this paper is that coefficient ring for the group algebra can be of great value in fingering  $\Delta$  candidates.

### 3 Cyclotomic Integers

Let  $\eta = \exp(\pi i/2^t)$  be the primitive complex  $2^{t+1}$ -th root of unity, for  $t > 0$ , and set  $\zeta = \eta^2$ . The structure of the field  $Q(\eta)$  is a classic part of algebraic number theory cf. [4, Appx E]. This section concerns primarily the ring  $Z[\eta]$  of algebraic integers in  $Q(\eta)$  [2, 21.13]. It presumes minimal familiarity with this literature and contains a crucial result Corollary (3.2) which characterizes the elements of  $Z[\eta]$  having norm a power of 2. This result actually follows from the well known theorem of Kronecker [5, p 83 line 25; 6, p 321 line 19] that the only algebraic integers all of whose conjugates are of modulus 1 are roots of unity; but an elementary direct proof of (3.2) is given here.

The minimum polynomial of  $\eta$  over the rationals is  $x^{2^t} + 1$ , and so  $\{\eta^d | d \in I\}$  is a  $Z$ -basis of  $Z[\eta]$  where  $I = I(\eta) = \{d \in Z | -2^{t-1} < d \leq 2^{t-1}\}$ . Because we are concerned with difference SETS, it is helpful to refine this  $Z$ -basis to a "natural  $N$ -basis" as follows. Write  $z \in Z[\eta]$  as:

$$z = \sum_{k \in I} z_k \eta^k$$

If the coefficient  $z_k$  is negative, we replace  $z_k \eta^k$  with  $(-z_k)(-1)\eta^k$  by setting  $z_{(k)} = 0$  and  $z_{(k \pm 2^t)} = z_k$  (where the sign is chosen so that  $|k \pm 2^t| \leq 2^t$ ). Otherwise, define  $z_{(k)}$  to be  $z_k$ . Thus  $z$  is expressed uniquely as:

$$z = \sum z_{(k)} \eta^k \text{ where } z_{(k)} \in N.$$

The strange function

$$^{(2)} : Z[\eta] \longrightarrow Z[\zeta] \text{ defined by } \sum z_{(k)} \eta^k \xrightarrow{(2)} \sum z_{(k)} \zeta^k$$

plays a role in the combinatorial representation theory of 2-groups. This map is NOT even a  $Z$ -homomorphism, but it does provide a convenient way to enumerate representations. Indeed, if  $\varphi$  is a monomial matrix representation

cf. [2, p 314] obtained by inducing a linear representation that takes values in  $Z[\eta]$ , then so is  $\varphi^{(2)}$ , where  $\varphi^{(2)}(g)$  has  $i, j$  entry the image of the  $i, j$  entry of  $\varphi$  under  $^{(2)}$ . Warning, since  $^{(2)}$  is not a ring homomorphism, this recipe works only for  $g \in G$ , NOT for arbitrary elements of  $ZG$ .

Let  $R$  denote the real elements of  $Z[\zeta]$  and  $\bar{x}$  denote the complex conjugate of  $x$ .

Denote the  $Z[\zeta]$ -ideal  $(1 - \zeta)$  by  $P$  and observe that both  $\bar{\zeta}$  and  $-\zeta$  are powers of  $\zeta$ , so  $P = \bar{P} = (\zeta + 1)$  and  $P^2 = (\zeta^2 - 1)$ , whence  $P^{2^{t-1}} = (-1 - 1) = (2)$ . For  $x \in Z[\zeta]$ , define the  $P$ -adic valuation,  $\nu(x)$  to be the largest integer  $k$  such that  $x \in P^k$ . Since  $Z[\zeta]$  is a Dedekind domain [2, §18, (21.13)], this function is a valuation [2, p 115]. Observe that whenever  $a, b, c \in Z[\zeta]$  and

$$(3.0.1) \quad a + b = c, \text{ the minimum of } \{\nu(a), \nu(b), \nu(c)\} \text{ cannot occur just once.}$$

A second simple property of this valuation that we will find useful is:

$$(3.0.2) \text{ For } x = \sum_{i \in I(\zeta)} x_i \zeta^i \in Z[\zeta], \nu(x) \geq s\nu(2) \text{ if and only if each } x_i \text{ is divisible by } 2^s.$$

In case  $\nu(x) < \nu(2)$ ,  $\nu(x)$  carries information about where  $x$  lies in the unique chain of ideals of the finite local ring  $Z[\zeta]/(2)$  and this is the basis of a type of "parity argument" that appears in the proof of Proposition (4.7).

**Lemma 3.1** *a. Each of the elements  $z \in Z[\zeta]$  for which  $z\eta$  is purely imaginary is in  $P$ .*

*b. If  $x \in R$ , then  $\nu(x)$  is even.*

*c. Suppose  $|a + b\eta| = 2^m$ , for  $a, b \in Z[\zeta]$ ,  $0 < m \in Z$ . Then  $a = 0$  or  $b = 0$ .*

**Proof Part a.** Write

$$z\eta = \sum_{k \in I} z_k \eta^k; z_k \in Z$$

as a  $Z$ -linear combination of basic powers of  $\eta$ . By hypothesis,  $z \in Z[\zeta]$ , so  $z_k$  is zero for  $k$  even and the coefficients  $z_k$  and  $z_{-k}$  sum to zero. Thus

$$z = \sum_{0 < k \in I(\eta), k \text{ odd}} z_k \eta^{-1} (\eta^k - \eta^{-k}) = \sum z_k \zeta^{-(k+1)/2} (\zeta^k - 1) \in P,$$

since  $(\zeta - 1)$  divides  $(\zeta^k - 1)$ .

**Proof Part b.** follows if it is established that any real element  $w$  of  $P^{2^k-1}$  is also in  $P^{2^k}$ . Write  $w = (1 - \zeta)^{2^k-1} u z$ , where  $u$  is the unit  $\bar{\zeta}^{k-1}$  in  $Z[\zeta]$ . Then, by choice of  $u$ ,  $z\eta$  is

**Proof Part c.** Now argue part c by contradiction, and assume  $a \neq 0 \neq b$ . Observe that  $\bar{\eta} = \eta\bar{\zeta}$ , so

$$2^{2^m} - a\bar{a} - b\bar{b} = (\bar{a}b + a\bar{b}\bar{\zeta})\eta.$$

If  $\bar{a}b + \bar{a}b\bar{\zeta} \neq 0$ , then this equation implies that  $\eta$  is in the quotient field  $\mathbf{Q}(\zeta)$  of  $\mathbf{Z}[\zeta]$ . But the minimal polynomial  $x^{2^t} + 1$  of  $\eta$  has degree greater than the dimension of  $\mathbf{Q}(\zeta)$  over  $\mathbf{Q}$ . Thus  $\bar{a}b + \bar{a}b\bar{\zeta} = 0$ . This implies that  $\bar{a}b\eta$  is purely imaginary and so  $\bar{a}b = (1 - \bar{\zeta})w$  for some nonzero  $w \in \mathbf{Z}[\zeta]$ , by part a. Moreover  $w \in \mathbf{R}$ , so  $\nu(w)$  is even by part b.

Consider the values of  $\nu(x)$  for each of the three terms of the equation:

$$2^{2m} = a\bar{a} + b\bar{b}.$$

Since both terms on the right hand side are positive numbers in  $\mathbf{R}$ , neither is divisible in  $\mathbf{R}$  by  $2^{2m}$ . The term on the left hand side generates  $P^s$ , where  $s = (2m)(2^{t-1})$ , so this implies that the highest value of  $\nu$  occurs on the left hand side. By (3.0.1), the two terms on the right hand side have the same value of  $\nu$ . And, since  $P = \bar{P}$ ,  $\nu(a) = \nu(\bar{a}) = \nu(b) = \nu(\bar{b})$ . Therefore  $\nu(\bar{a}b)$  is even, whence  $w$  in the last paragraph has  $\nu(w)$  odd. This contradiction establishes the lemma.  $\square$

**Corollary 3.2** *If  $z \in \mathbf{Z}[\eta]$  has length  $2^n$ ,  $n > 0$ , then  $z = 2^n \eta^k$  for some  $k$ .*

**Proof.** Write  $z = a + b\eta$  for  $a, b \in \mathbf{Z}[\zeta]$ . By Lemma (3.1 c) either  $a$  or  $b$  is zero. Multiply  $z$  by  $\eta$  if necessary so that  $b = 0$  and appeal to induction on  $t$  if  $t > 1$ .  $\square$

### 4 Homomorphic Images of Difference Sets

One of the the reasons the study of difference sets requires techniques apart from standard group theory is that it is not inductive. Just because a group has a difference set is no guarantee that your favorite subgroup or homomorphic image has one too. This section shows that careful attention to the ring of coefficients can mitigate this difficulty.

**Proposition 4.1** *Let  $G$  be a 2-group of order  $4u^2 > 4$  that possesses a difference set  $\Delta$ . Suppose  $N \leq H$  are normal subgroups of  $G$  such that*

$$G/N = A \times H/N \text{ and } H/N \text{ is cyclic of order } 2^{t+1} \text{ and generated by } x.$$

*Assume that  $A$  is abelian of exponent  $\leq 2^{t+1}$ . Let  $K = N \cup Nz$  where  $z = x^{2^t}$ . If  $|A| < u$ , then  $|Kg \cap \Delta|$  is even for each  $g \in G$ .*

**Proof.** Let  $\eta$  be a primitive  $2^{t+1}$ -th root of unity and  $I = I(\eta)$  the basic index set for  $\eta$ . By assumption, all absolutely irreducible  $G/N$ -representations in characteristic 0 may be written over  $\mathbf{Z}[\eta]$ . Let  $\chi$  be a character of  $A$  and consider the tensor product  $\chi \otimes \eta$  character of  $G$  defined by

$$\chi \otimes \eta(g) = \eta^{k(g)} \chi(a(g))$$

where  $a(g) \in A$  and  $k(g) \in I(\eta)$  are defined by  $Ng = x^{k(g)}a(g)$ . Then

$$\chi \otimes \eta(\delta) = \sum_{g \in \Delta} \eta^{k(g)} \chi(a(g)) = \sum_{a \in A} \chi(a) \sum_{k \in I(\eta)} \{|\Delta \cap x^k a| - |\Delta \cap zx^k a|\} \eta^k.$$

Since  $\eta$  is primitive,  $\chi \otimes \eta$  is not the trivial character of  $G$ . It therefore satisfies:

$$u^2 = \chi \otimes \eta(\delta) \chi \otimes \eta(\delta^{-1}) = \chi \otimes \eta(\delta) \overline{\chi \otimes \eta(\delta)}.$$

By Corollary (3.2)

$$\chi \otimes \eta(\delta) = u\eta^s \text{ for some } s,$$

whence

$$\chi \otimes \eta(\delta) \equiv 0 \pmod{u}$$

in  $\mathbf{Z}[\eta]$ . Now consider the system of linear congruences:

$$\sum_{a \in A} \chi(a) \sum_{k \in I(\eta)} \{|\Delta \cap x^k a| - |\Delta \cap zx^k a|\} \eta^k \equiv 0 \pmod{u}$$

as  $\chi$  takes all values. This system of linear congruences has the character table  $\text{Ch}(A)$  of  $A$  as its coefficient matrix and the expressions  $\{|\Delta \cap x^k a| - |\Delta \cap zx^k a|\} \eta^k$  as variables. By the orthogonality relations cf. [2, 31.15 p 221] for group characters,  $|A| \text{Ch}(A)^{-1}$  has coefficients in  $\mathbf{Z}[\eta]$ . It follows that

$$\sum_{k \in I(\eta)} \{|\Delta \cap x^k a| - |\Delta \cap zx^k a|\} \eta^k \equiv 0 \pmod{u/|A|}$$

in  $\mathbf{Z}[\eta]$ , for all  $a \in A$ . Now 2 divides  $u/|A|$ , by hypothesis, so the  $\mathbf{Z}$ -independence of  $\{\eta^k | k \in I(\eta)\}$  implies:

$$(4.1.1) \quad |\Delta \cap Ng| - |\Delta \cap Ngz| \equiv 0 \pmod{2}$$

for all  $g \in G$ . Finally,

$$|\Delta \cap Kg| = |\Delta \cap Hg| + |\Delta \cap Hzg| \equiv |\Delta \cap Hg| - |\Delta \cap Hgz|, \pmod{2}$$

and the proof is complete.  $\square$

It seems plausible that the assumptions that  $A$  is abelian of exponent... might be omitted by working with the group algebra of  $A$  and not just with characters.

**Corollary 4.2** *(Turyn [6, Corollary 2 p 333; 4, 4.34(1)]) If  $G$  is an abelian 2-group with a nondegenerate difference set  $\Delta$  and with order  $4u^2$ , then  $\exp(G) \leq 4u$ .*

**Proof** Suppose not, and let  $H$  be a maximal cyclic subgroup of  $G$  and observe that the hypotheses of Proposition (4.1) are met with  $N = 1$ . By (4.1.1),  $g \in \Delta$  if and only if  $gz \in \Delta$ . Whence  $z$  appears as a difference  $|\Delta|$  times and the design is degenerate.  $\square$

A construction of Dillon shows that the abelian 2-group with elementary divisors 4,1,1, has a difference set, so the hypothesis  $|A| < u$  cannot be relaxed and our Proposition (4.7) shows that the abelian hypothesis is essential to this result.

**Proposition 4.3** *Let  $G$  be a 2-group of order  $4u^2 > 4$  that possesses a difference set  $\Delta$ . Suppose  $N$  is a normal subgroup of  $G$  such that  $G/N = \langle x, y | x^{2m} = y^2 = 1, yxy = x^{-1} \rangle$  is dihedral of order  $4m$ . Then there is  $h \in G$  such that  $|\Delta \cap Nhg| - |\Delta \cap Nhg^m|$  equals  $u$  or  $0$  depending on whether  $g \in N$  or not. In particular,  $|N| \geq u$ .*

**Proof.** Take  $\delta$  and  $\delta^{(-1)}$  as in section 2, let  $\eta$  be a primitive  $2m$ -th root of unity and set  $I = I(\eta)$ ,  $\zeta = \eta^2$  as in section 3. Consider the representation of  $G$  over  $\mathbf{Z}[\eta]$  defined by:

$$\varphi(xh) = \begin{pmatrix} \eta & 0 \\ 0 & \bar{\eta} \end{pmatrix}, \varphi(yh) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; h \in N.$$

Observe that the kernel of  $\varphi$  is  $N$ , so  $\varphi$  is also a representation of  $G/N$ . Identify each  $gN/N \in G/N$  with the associated  $N$ -coset  $gN$  in  $G$ , so that the elements of  $G/N$  are subsets of  $G$ . Define  $a, b \in \mathbf{Z}[\eta]$  by:

$$a = \sum |\Delta \cap x^i | \eta^i, b = \sum |\Delta \cap x^i y | \eta^i.$$

Then

$$\varphi(\delta) = \begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix}$$

and

$$\varphi(\delta^{(-1)}) = \sum |\Delta \cap x^i | \varphi(x^{-1}) + \sum |\Delta \cap x^i y | \varphi(yx^{-1}) = \begin{pmatrix} \bar{a} & \bar{b} \\ b & a \end{pmatrix}.$$

The difference set equation  $u^2 I_2 = \varphi(\delta)\varphi(\delta^{(-1)})$  has (1,2) entry  $0 = 2ab$ .

Whence, by (3.2),  $\{a, b\} = \{0, u\eta^k\}$  for some  $k$ . Choose  $h \in G$  so that  $\varphi(\delta) = u\varphi(h)$ . The claim follows from the independence  $\{\eta^d | d \in I\}$  as in Proposition (4.1).  $\square$

The following notation will hold for the rest of this paper. The group  $G$  is a 2-group of order  $4u^2$  having a difference set  $\Delta$  and  $N$  is normal in  $G$  where

$$G/N = \langle x, y | x^{4f} = y^2 = 1, yxy = x^{1+2f} \rangle; f = 2^{t-1}, t \geq 3.$$

Let  $\delta, \delta^{(-1)}$  be as in section 2 and take  $t, \eta, \zeta, I$ , and  $(2)$  as in section 3. Again identify elements of  $G/N$  with the associated  $N$ -coset in  $G$ . Define

subgroups of  $G$  by  $H_k = \langle x^{2^k} \rangle N$  for  $k = 0, 1, \dots, t+1$ . Abuse notation so that  $H_k$  also denotes the sum  $\sum_{g \in H_k} g$ . Since  $H_k$  is normal in  $G$ ,

$$H_k \delta = \delta H_k = \sum_{g \in G/H_k} |\Delta \cap H_k g | g H_k.$$

Finally, for each  $g \in G$ , set  $g_k = |\Delta \cap H_k g|$ .

It seems plausible that knowledge of the structure of  $G/N$  (but no hypothesis on  $N$ ) is strong enough to determine  $\Delta/N$ . Our goal is more limited and is to obtain information about the numbers  $\{g_k\}$  from the representation theory of  $G/H_k$ .

**Lemma 4.4** *Define  $\varphi : G \rightarrow \text{Mat}(2, \mathbf{Z}[\eta])$  by  $\varphi(xh) = \begin{pmatrix} \eta & 0 \\ 0 & -\eta \end{pmatrix}$ ,  $\varphi(yh) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ;  $h \in N$ . Then the direct sum*

$$\varphi \oplus \varphi^{(2)} \oplus \dots \oplus \overbrace{\varphi^{(2)} \cdots (2)}^{t+1}$$

is a sufficient representation for  $G/N$ .

**Proof.** By Theorem (2.3) it is enough to show that every complex irreducible representation of  $G/N$  has an algebraic conjugate as a constituent of this direct sum. The representation  $\varphi \otimes \mathbf{C}$  is an irreducible representation of  $G/N$  over  $\mathbf{C}$ , and it has  $f$  algebraic conjugates. The sum of the minimal two-sided ideals in  $\mathbf{C}\bar{G}$  associated with algebraic conjugates of  $\varphi$  has dimension  $2^2(f)$ . The dimension of the sum of the minimal two sided ideals in  $\mathbf{C}G$  associated with all other  $G/N$ -representations is  $|G/N| - 2^2(f) = 4f$ , which happens to be  $|\frac{G/N}{(G/N)^r}|$ . All remaining irreducible  $G/N$ -representations are linear.

The  $(t+1) - t h^{(2)}$ -power of  $\varphi$  takes  $x$  to the identity matrix and has two linear representations ( $x \rightarrow 1, y \rightarrow 1$ ;  $x \rightarrow 1, y \rightarrow -1$ ) as constituents and no algebraic conjugates. For  $k \leq t$ , the  $k - t h^{(2)}$ -power,  $\varphi^{(2)^k}$  of  $\varphi$  has the form:

$$\varphi(x) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \quad \varphi(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where  $\alpha = \eta^{(2)^k}$  is a primitive  $2^{t-k} - t h$  root of unity. It has two linear representations

$$x \rightarrow \alpha, y \rightarrow 1; x \rightarrow \alpha, y \rightarrow -1$$

as constituents and has (Euler phi function)  $\varphi(2^{t+1-k}) = 2^{t-k}$  algebraic conjugates. Thus the indicated direct sum accounts for

$$2 \left[ \overbrace{2^{(t-1)}}^{k=1} + \overbrace{2^{(t-2)}}^{k=2} + \dots + \overbrace{1}^{k=t} + \overbrace{1}^{k=t+1} \right] = 4f$$

distinct linear representations of  $\bar{G}$ .  $\square$

**Lemma 4.5** a. The  $(t + 1) - th^{(2)}$ -power  $\rho$  of  $\varphi$  satisfies:

$$\rho(\delta) = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ where } \{a, b\} = \{u^2, u^2 - u\}.$$

b.  $1 \leq k \leq t$ , and the  $k - th^{(2)}$ -power,  $\varphi^{(2)^k}$  of  $\varphi$ ,

$$\varphi^{(2)^k}(\delta) = \frac{u}{2} \begin{pmatrix} \alpha^p + \alpha^q & \alpha^p - \alpha^q \\ \alpha^p - \alpha^q & \alpha^p + \alpha^q \end{pmatrix},$$

for  $\alpha = \eta^{2^k}$  and some integers  $p, q$ .

c. By replacing  $\delta$  with  $\delta g$  for some  $g \in G$  we may suppose  $\det\varphi(\delta) = u^2$ . Then the difference set equation for  $\varphi$  is equivalent to:

$$a = \bar{a}, b = -\bar{b}, c\zeta = -\bar{c}, d\zeta = \bar{d}, \text{ and } u^2 = a^2 - b^2 - c^2\zeta + d^2\zeta.$$

where

$$a = \sum |\Delta \cap x^{2k}| \zeta^k, b = \sum |\Delta \cap x^{2k}y| \zeta^k, \\ c = \sum |\Delta \cap x^{2k+1}| \zeta^k, d = \sum |\Delta \cap x^{2k+1}y| \zeta^k.$$

**Proof.** In case a.,  $a = |\Delta \cap \langle x \rangle| = 1_0$  and  $b = |\Delta \cap \langle x \rangle y| = y_0$ , in the notation introduced just before lemma (4.4). The result follows from the difference set equation

$$u^2 I_2 + (2u^2 - u)2u^2 J_2 = \rho(\delta)\rho(\delta^{(-1)}) \text{ and } a + b = |\Delta| = 2u^2 - u.$$

In case b., set  $\rho = \varphi^{(2)^k}$  and observe that

$$\rho(\delta) = \begin{pmatrix} s & t \\ t & s \end{pmatrix} \text{ where } s = \sum_{x^i \in \Delta} \alpha^i, t = \sum_{x^i y \in \Delta} \alpha^i \in \mathbf{Z}[\alpha].$$

Since  $\rho$  does not have the trivial representation as a constituent, the difference set equation  $u^2 I_2 = \rho(\delta)\rho(\delta^{(-1)})$  is equivalent to:

$$s\bar{s} + t\bar{t} = u^2, s\bar{t} + \bar{s}t = 0.$$

By Corollary (3.2) twice,

$$s + t = u\alpha^p, s - t = u\alpha^q$$

for some integers  $p$  and  $q$ .

In case c., observe that  $\varphi(\delta) = \begin{pmatrix} a + c\eta & b + d\eta \\ b - d\eta & a - c\eta \end{pmatrix}$ . Since  $\det\varphi(\delta) \in \mathbf{Z}[\zeta]$  and

$$\det(u^2 I_2) = \det\varphi(\delta)\varphi(\delta^{(-1)}) = \det\varphi(\delta) \det \overline{\varphi(\delta)},$$

Corollary (3.2) implies that  $\det\varphi(\delta)$  has the form  $u^2\zeta^k$  for some  $k$ . Replace  $\Delta$  by  $(xy)^{-k}\Delta$ . Then  $\Delta$  remains a difference set but  $\det \varphi(\delta) = u^2$ . Now the difference set equation implies

$$\begin{pmatrix} \bar{a} + \bar{c}\eta & \bar{b} - \bar{d}\eta \\ \bar{b} + \bar{d}\eta & \bar{a} - \bar{c}\eta \end{pmatrix} = \varphi(\delta^{(-1)}) = u^2 \varphi(\delta)^{-1} = \begin{pmatrix} a - c\eta & -b - d\eta \\ -b + d\eta & a + c\eta \end{pmatrix}$$

by the cofactor expansion of the inverse of a 2 by 2 matrix. Comparison of the entries in this matrix equation yields a linear system having the first four equations as solution. The final equation is the determinant of  $\varphi(\delta)$ .  $\square$

In case  $N = 1$ , Lemma (4.4) and the definition of sufficient representation, imply that  $\Delta$  is a difference set in  $G$  if and only if  $\delta$  simultaneously satisfies all of the conditions of Lemma (4.5). In order to construct  $\Delta$ , it is natural to work one's way from  $k = e + 1$  down to  $k = 1$ . This seems to lead a to a proliferation of cases and does not seem to be the best organization. This organizational issue is the starting point of "The inversion formula" a forthcoming manuscript by the first author. We give a non-existence result rather like Proposition (4.3)

**Proposition 4.6** Let  $G$  be a 2-group of order  $4u^2$  having a difference set  $\Delta$ . Suppose  $N$  is normal in  $G$  and

$$G/N = \langle x, y | x^{4f} = y^2 = 1, yxy = x^{1+2f} \rangle; f = 2^{t-1}, t \geq 3.$$

Then  $u/2$  divides  $|\Delta \cap gN\langle x^{2f} \rangle| - |\Delta \cap gx^f N\langle x^{2f} \rangle|$  for each  $g \in G$ . In particular,  $|N| \geq u/4$ .

**Proof.** Observe that

$$\varphi^{(2)}(\delta) = \begin{pmatrix} A + C\zeta & B + D\zeta \\ B + D\zeta & A + C\zeta \end{pmatrix},$$

where

$$A = \sum_{x^{2k} \in \Delta} \zeta^{2k}, B = \sum_{x^{2k}y \in \Delta} \zeta^{2k}, C = \sum_{x^{2k+1} \in \Delta} \zeta^{2k}, D = \sum_{x^{2k+1}y \in \Delta} \zeta^{2k}.$$

Lemma 4.5b, asserts that there exist integers  $p, q$  such that

$$A + C\zeta = \frac{u}{2}(\zeta^p + \zeta^q), B + D\zeta = \frac{u}{2}(\zeta^p - \zeta^q).$$

It follows that  $u/2 ||\Delta \cap gN\langle x^{2f} \rangle| - |\Delta \cap gx^f N\langle x^{2f} \rangle|$ .  $\square$

**Proposition 4.7** Suppose  $N = 1$  and  $u = 4$  in a group  $G$  as in (4.6). Then there exists  $g \in G, z_1, z_2 \in Z(G) = \langle z := x^{16} \rangle$  and integers  $p, q, u, j, t$  such that

$$\delta g = (1 + x^{16})[x^p + x^q + x^p y + x^{q+8} y + (1 + x^8)x^u] +$$

$$(x^{-4} + x^4)[x^{2j}(1 + z_1y) + x^{-2j}(1 + z_1zy) + x^{2t+1}(z_2 + y) + x^{-2t-1}(zz_2 + y)].$$

Moreover

$$j \equiv 1 \pmod{2}$$

and

$$\{p, q, u\} \equiv \{2t + 1, 2t - 1, 2 \pm 2\} \text{ or } \{2t \pm 1, 0, 4\}. \pmod{8}$$

Conversely, each solution to this system of congruences for which  $\delta$  is a sum over a subset of  $G$  gives rise to a difference set  $\Delta$  in  $G$ .

**Proof.** Recall  $H_k = \langle x^{2^k} \rangle$  and that  $H_k$  also denotes  $\sum_{g \in H_k} g$ ,  $k = 0 \dots 4$ . Moreover

$$H_k \delta = \sum_{g \in G/H_k} g_k(gH_k), \text{ where } g_k = |\Delta \cap H_k g|.$$

By Lemma (4.5 a),  $1_0 = |\Delta \cap H_0|$  is 16 or 12 and any set satisfying this condition solves the difference set equation for  $\rho$ .

As in the proof of (4.6), the case  $k = 1$  of Lemma (4.5 b) reads:

$$\left( \begin{array}{c} \sum_{i=0}^7 [x^i_4 - x^{i+8}_4] \zeta^i \\ \sum_{i=0}^7 [x^i y_4 - x^{i+8} y_4] \zeta^i \end{array} \right) = \varphi^{(2)}(\delta) = 2 \begin{pmatrix} \zeta^p + \zeta^q & \zeta^p - \zeta^q \\ \zeta^p - \zeta^q & \zeta^p + \zeta^q \end{pmatrix},$$

for some integers  $p, q$ . Since  $2 = |H_4| \geq g_4 \geq 0$ , for all  $g \in G$ ,  $p \neq q$  and this implies:

$$\begin{aligned} 2 &= x^p_4 = x^q_4 = x^p y_4 = x^{q+8} y_4 \\ (4.7.1) \quad 0 &= x^{p+8}_4 = x^{q+8}_4 = x^{p+8} y_4 = x^q y_4 \\ g_4 &= x^8_4 g \text{ for all other } g \in G/H_4. \end{aligned}$$

The first four equalities imply that  $\Delta \supset x^p H_4 \cup x^q H_4 \cup x^p y H_4 \cup x^{q+8} y H_4$ ; the second four equalities imply that  $\phi = \Delta \cap (x^{p+8} H_4 \cup x^{q+8} H_4 \cup x^{p+8} y H_4 \cup x^q y H_4)$ ; and the last equality of (4.7.1) implies:

If  $g \in \Delta$  then exactly one of  $gx^8$  or  $gx^8 x^{16} = gx^{-8}$  is too.

Therefore there is a set  $\Gamma'$  of 10 elements of  $G$  such that:

$$\delta = (1 + x^{16})(x^p + x^q + x^p y + x^{q+8} y) + (x^4 + x^{-4}) \left( \sum_{g \in \Gamma'} g \right).$$

But the element  $x^{16}$  of  $G$  appears as a difference of elements of  $\Delta$  exactly 12 (the design parameter  $\lambda$ ) times. Thus there are 6  $H_4$ -cosets contained in

$\Delta$ . It follows that 2 of the elements of  $\Gamma$  form an  $H_4$ -coset. Thus there exist  $u, v$  and 8 elements  $\Gamma$  of  $G$  such that

$$\delta = (1 + x^{16})[x^p + x^q + x^p y + x^{q+8} y + (1 + x^8)x^u y^v] + (x^4 + x^{-4})\gamma,$$

where  $\gamma = \left( \sum_{g \in \Gamma} g \right)$ .

Note that all 12  $\cdot 2$  differences of elements of  $\Delta$  that equal elements of  $H_3 - H_4$  are now accounted for by  $(1 + x^{16})(1 + x^8)x^u y^v + (x^4 + x^{-4})\gamma$ , and consequently:

NO TWO ELEMENTS OF  $\Gamma$  ARE IN THE SAME  $H_3$ -COSET.

Now  $|H_0 \cap \Delta| = 12$  or 16, by the first paragraph of the proof and any such  $\delta$  of the form

$$\delta = (1 + x^{16})[x^p + x^q + x^p y + x^{q+8} y + (1 + x^8)x^u y^v] + (x^4 + x^{-4})\gamma$$

satisfies the difference set equation for  $\rho \oplus \varphi^{(2)}$ .

Since  $\varphi(x^8) = iI_2$ ,  $\varphi(\delta) = 0 + (\zeta^2 + \zeta^{-2})\varphi(\gamma)$ . Replace  $\Delta$  with  $\Delta g$  as in Lemma (4.5.c), so that  $\det \varphi(\delta) = 16$ . Next replace  $\Delta$  by  $\Delta x^8 y$  if necessary so that

$$v = 0$$

and note that  $\det \varphi(\delta)$  is unchanged and that  $|H_0 \cap \Gamma|$  is 2 or 4. We have:

$$\begin{pmatrix} a + c\eta & b + d\eta \\ b - d\eta & a - c\eta \end{pmatrix} = \varphi(\delta) = (\zeta^2 + \zeta^{-2})\varphi(\gamma) = (\zeta^2 + \zeta^{-2}) \begin{pmatrix} A + C\eta & B + D\eta \\ B - D\eta & A - C\eta \end{pmatrix},$$

and

$$A = \sum_{x^{2^k} \in \Gamma} \zeta^k, B = \sum_{x^{2^k} y \in \Gamma} \zeta^k, C = \sum_{x^{2^k+1} \in \Gamma} \zeta^k, D = \sum_{x^{2^k+1} y \in \Gamma} \zeta^k.$$

Since  $\zeta^2 + \zeta^{-2}$  is real, the complex numbers denoted by upper and lower case letters  $a, b, c, d$  have the same argument. Thus, the first equation of Lemma (4.5 c) leads to  $A = \bar{A}$  and so,  $x^{2^k} \in \Gamma \Rightarrow x^{-2^k} \in \Gamma$ ; or  $\zeta^k \in A \Rightarrow \zeta^{-k} \in A$ , where  $\zeta^k \in A$  is to be read " $\zeta^k$  appears in the sum  $A$ ".

Similarly, the next three equations of Lemma (4.5 c) give:  $B = -\bar{B}$  and so  $x^{8+2^k} y \in \Gamma \Rightarrow x^{8-2^k} y \in \Gamma$ ; or  $i\zeta^k \in B \Rightarrow i\zeta^{-k} \in B$ .  $\zeta C = -\bar{C}$  and so  $x^{8+2^k+1} \in \Gamma \Rightarrow x^{8-2^k-1} \in \Gamma$ ; or  $i\zeta^k \in C \Rightarrow i\zeta^{-k-1} \in C$ .  $\zeta D = \bar{D}$  and so  $x^{2^k+1} y \in \Gamma \Rightarrow x^{-2^k-1} y \in \Gamma$ ; or  $\zeta^k \in D \Rightarrow \zeta^{-k-1} \in D$ .

The ideals  $(1 - \zeta)^{10}$  and  $(2 + 2\zeta^2)$  are equal. Consequently the ring  $R = \mathbb{Z}[\zeta]/(2 + 2\zeta^2)$  is of order  $2^{10}$  and has characteristic 4 ( $\nu(4) = 16 > 10$ ). Further,  $R$  has the endearing feature that no two distinct powers of  $\zeta$  are equal in  $R$ . We will use  $R$  as the setting for a parity argument to show that each of the sums  $A, B, C, D$  has exactly 2 terms.

Since, for example

$$[(\zeta^a + \zeta^{-a-1}) + (\zeta^b + \zeta^{-b-1})]^2$$

$$= \zeta^{2a} + \zeta^{-2a-2} + \zeta^{2b} + \zeta^{-2b-2} + 4\zeta^{-1} + 2(\zeta^a + \zeta^{-a-1})(\zeta^b + \zeta^{-b-1}) \\ \equiv \zeta^{2a} + \zeta^{-2a-2} + \zeta^{2b} + \zeta^{-2b-2} \pmod{2 + 2\zeta^2}$$

the last equation of Lemma (4.5 c)

$$16/2 = (a^2 - b^2 - c^2\zeta + d^2\zeta)/2 = (\zeta^2 + \zeta^{-2})(A^2 - B^2 - C^2\zeta + D^2\zeta)$$

reduces to

$$0 \equiv (\zeta^2 A)^2 - (\zeta^2 B)^2 - (\zeta^2 C)^2\zeta + (\zeta^2 D)^2\zeta \pmod{8} \\ 0 \equiv \sum \zeta^{2j} + \zeta^{-2j} + \sum \zeta^{2j+1} + \zeta^{-2j-1} \pmod{2 + 2\zeta^2}$$

where the first summation arises from terms appearing in the sum A or B and the second summation arises from terms appearing in C or D.

The first sum has only even powers of  $\zeta$  while the second sum has only odd powers of  $\zeta$ , so the two sums must be each equal 0 in R. Moreover, no two powers  $\zeta^a, \zeta^b$  arising from the same element of  $\{A, B, C, D\}$  can have quotient  $\pm 1$ , since no two elements of  $\Gamma$  are in the same  $H_3$ -coset.

The sum arising from A and B cannot have terms of the form  $\zeta^4 + \zeta^{-4} \equiv 0 \in R$ . The first sum must therefore have four terms and be of the form  $(\zeta^2 + \zeta^{-2}) + (\zeta^6 + \zeta^{-6})$ . If one of A, B is an empty sum, then the other sum contains distinct powers of  $\zeta$  whose quotient is  $\pm 1$ , so both A and B have two terms and:

$$(A)^2 \equiv \pm(B)^2 \equiv \pm(\zeta^2 + \zeta^{-2}). \pmod{2 + 2\zeta^2}$$

It follows that  $\{x^{2j}, x^{-2j}, x^{2k}x^8y, x^{-2k}x^8y\} \subset \Gamma$  for some odd  $j, k$ . The equality

$$8 = (\zeta^2 + \zeta^{-2})(A^2 - B^2 - C^2\zeta + D^2\zeta)$$

is not satisfied unless  $j \equiv k + 4 \pmod{8}$  too. Thus, for some odd  $j$  and,

$$z_1 := x^{2k+8-2j} (\in \langle x^{16} \rangle),$$

the set

$$\{x^{2j}, x^{-2j}, x^{2j}z_1y, x^{-2j}z_1zy\} \text{ is in } \Gamma.$$

The sum arising from C and D must have the other four terms and be the sum of two expressions of the form  $\pm(\zeta + \zeta^{-1})$  or  $\pm(\zeta^3 + \zeta^{-3})$ . If one of the sums C, D is empty, then both forms appear and they cannot sum to zero. Thus

$$(\zeta^2 C)^2\zeta = -(\zeta^2 D)^2\zeta \in \{\pm(\zeta + \zeta^{-1}), \pm(\zeta^3 + \zeta^{-3})\}. \pmod{2 + 2\zeta^2}$$

It follows that  $\{x^{2s+1}x^8, x^{-2s-1}x^8, x^{2t+1}y, x^{-2t-1}y\} \subset \Gamma$  where  $s \equiv t + 4 \pmod{8}$ . And, for  $z_2 := x^{2s+8-2t} (\in \langle x^{16} \rangle)$ , the set  $\{x^{2t+1}z_2, x^{-2t-1}z_2y, x^{2t+1}y, x^{-2t-1}y\}$  is in  $\Gamma$ .

The difference set  $\Delta$  is now normalized so that  $\delta$  has exactly the form claimed in the proposition. Moreover any  $\Delta$  of this form for which  $j$  is odd satisfies the difference set equation for  $\varphi \oplus \varphi^{(2)} \oplus \rho$ .

Consider next  $\varphi^{(4)}$ . Since  $\varphi^{(4)}(x^4) = -I, \varphi^{(4)}(z_i) = 1$ , and

$$\varphi^{(4)}(\delta) = 2\varphi^{(4)}[(x^p + x^q)(1+y) + 2x^u] - 2\varphi^{(4)}[(x^{2j} + x^{-2j} + x^{2t+1} + x^{-2t-1})(1+y)].$$

But  $j$  is odd, so  $\varphi^{(4)}(x^{2j} + x^{-2j}) = 0$ . Lemma (4.5.b) implies that there is  $e, f$  such that

$$\begin{pmatrix} \zeta^{2e} + \zeta^{2f} & \zeta^{2e} - \zeta^{2f} \\ \zeta^{2e} - \zeta^{2f} & \zeta^{2e} + \zeta^{2f} \end{pmatrix} = \frac{1}{2}\varphi^{(4)}(\delta) \\ = \begin{pmatrix} \zeta^{2p} + \zeta^{2q} + 2\zeta^{2u} & \zeta^{2p} + \zeta^{2q} \\ \zeta^{2p} + \zeta^{2q} & 2\zeta^{2u} + \zeta^{2p} + \zeta^{2q} \end{pmatrix} + i^t\zeta^2(1-i) \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Compare the sum of the entries in the first column of these matrices,

$$(4.7.2) \quad \zeta^{2e} = \zeta^{2p} + \zeta^{2q} + \zeta^{2u} + i^t\zeta^2(1-i), \text{ for some } e.$$

The difference set equation for  $\varphi^{(4)}$  is satisfied only with  $f = u$  and with any solution of this equation. Therefore any  $\Delta$  for which  $\delta$  has the claimed form with  $j$  odd that also satisfies (4.7.2), in fact satisfies the difference set equation for  $\varphi \oplus \varphi^{(2)} \oplus \varphi^{(4)} \oplus \rho$ .

In a similar manner  $\varphi^{(8)}(x^2) = -I$ , so

$$\varphi^{(8)}(x^{2t+1} + x^{-2t-1}) = 0 \text{ and } \varphi^{(8)}(x^{2j} + x^{-2j}) = -2I,$$

since  $j$  is odd. Lemma (4.5.b) implies that there is  $f, g$  such that

$$\begin{pmatrix} i^f + i^g & i^f - i^g \\ i^f - i^g & i^f + i^g \end{pmatrix} = \frac{1}{2}\varphi^{(8)}(\delta) \\ = \begin{pmatrix} i^p + i^q + 2i^u & i^p + i^q \\ i^p + i^q & 2i^u + i^p + i^q \end{pmatrix} + \begin{pmatrix} -2 & -2 \\ -2 & -2 \end{pmatrix}.$$

Comparison of the sum of the first columns of these matrices leads to:

$$(4.7.3) \quad i^f = i^p + i^q + i^u - 2, \text{ for some } f.$$

The difference set equation for  $\varphi^{(8)}$  is satisfied only with  $g = u$  and with any solution of this equation. Therefore any  $\Delta$  for which  $\delta$  has the claimed form with  $j$  odd that also satisfies (4.7.2), and (4.7.3), in fact satisfies the difference set equation for  $\varphi \oplus \varphi^{(2)} \oplus \varphi^{(4)} \oplus \varphi^{(8)} \oplus \rho$ .

The sum of the first columns of the two expressions for  $\varphi^{(16)}(\delta)$  that arise from Lemma (4.5 b) yields

$$(4.7.4) \quad (-1)^g = (-1)^p + (-1)^q + (-1)^u, \text{ for some } g.$$

Any solution of this equation extends to a solution of the difference set equation for  $\varphi^{(16)}$ . Therefore any  $\Delta$  for which  $\delta$  has the claimed form with  $j$  odd also satisfying (4.7.2), (4.7.3), and (4.7.4), satisfies the difference set equation for  $\varphi \oplus \varphi \oplus \varphi^{(2)} \oplus \varphi^{(4)} \oplus \varphi^{(8)} \oplus \varphi^{(16)} \oplus \rho$ . By Lemma (4.4) this is sufficient.

Condition (4.7.4) is satisfied whenever  $p, q, u$  do not all have the same parity and condition (4.7.3) has a solution of this type if and only if the multiset

$$\{i^p, i^q, i^u\} = \{1, 1, i^k\} \text{ or } \{1, i^k, -i^k\},$$

for some integer  $k$ . (To see this easily, observe that  $i^p + i^q + i^u$  is a Gaussian integer at distance 1 from 2, so we seek "walks on a grid" of length 3 joining the origin to 2.) The condition (4.7.2) may be rewritten:

$$\zeta^{2e} = \zeta^{2p} + \zeta^{2q} + \zeta^{2u} + \sqrt{2} i^t,$$

for some  $e$  and has general solution:

$$\{\zeta^{2p}, \zeta^{2q}, \zeta^{2u}\} = \{i^t \zeta^2, i^t \zeta^{-2}, \zeta^{2k}\} \text{ or } \{i^t \zeta^2 \text{ or } i^t \zeta^{-2}, \zeta^{2k}, -\zeta^{2k}\},$$

for some integer  $k$ . The simultaneous solutions to (4.7.2)-(4.7.4) are of two types:

$$\{p, q, u\} \equiv \{2t + 1, 2t - 1, 4k\}, \{2t \pm 1, 0, 4\} \pmod{8}$$

for some integer  $k$ .  $\square$

**Corollary 4.8** *Let  $G$  be the "modular group"*

$$\langle x, y | x^{32} = y^2 = 1, yxy = x^{17} \rangle.$$

*Then the set  $\Delta$  is a difference set, where*

$$\sum_{g \in \Delta} g = (1 + x^{16})[1 + x^4 + y + x^{12}y + x + x^9] \\ + (1 + x^8)[x^2 + x^{-2} + x^8(x^5 + x^{-5} + x^{10}y + x^{-10}y) + x^{13}y + x^{-13}y].$$

**Proof.** Set  $p = -4, q = 0, u = -3, j = 1, t = 6, z_1 = z_2 = 1$  in Proposition (4.7) and multiply the result by  $x^4$  on the left.  $\square$

## References

- [1] Beth, T. D. Jungnickel and H. Lenz. Design Theory. Cambridge University Press, (1986).
- [2] Curtis, C. W. and I. Reiner. Representation theory of finite groups and associative algebras. Interscience, (1962).
- [3] Dillon, J. F. "A Survey of difference sets in 2-groups" (Proceedings for the Conference honoring Marshall Hall Jr., Burlington Vermont September 1990).

- [4] Lander, E. S. Symmetric designs: an algebraic approach. London Mathematical Society LNS 74, Cambridge University press, (1983).
- [5] Mann, H. B. Addition Theorems: the addition theorems of group theory and number theory. Interscience, (1965).
- [6] Turyn R. J. "Character sums and difference sets" Pac. J. Math. 15, 319-346 (1965).