

Non-Abelian Hadamard Difference Sets

KEN W. SMITH

Central Michigan University, Mt. Pleasant, Michigan 48859

Communicated by the Managing Editors

Received December 23, 1992; revised October 20, 1993

Difference sets with parameters (v, k, λ) may exist even if there are no *abelian* (v, k, λ) difference sets; we give the first known example of this situation. This example gives rise to an infinite family of non-abelian difference sets with parameters $(4t^2, 2t^2 - t, t^2 - t)$, where $t = 2^q \cdot 3^r \cdot 5 \cdot 10^s$, $q, r, s \geq 0$, and $r > 0 \Rightarrow q > 0$. No abelian difference sets with these parameters are known. © 1995 Academic Press, Inc.

1. INTRODUCTION

A (v, k, λ) difference set is a subset A of size k in a group G of order v with the property that for every g in G , $g \neq 1$, there are exactly λ ordered pairs $(x, y) \in A \times A$ such that

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

A difference set is said to be abelian (non-abelian, cyclic) if the group is abelian (non-abelian, cyclic). If a group G has a difference set A then the set $\{gA : g \in G\}$ forms the blocks of a symmetric (v, k, λ) design with point set G . On this design G acts by left multiplication as a sharply transitive automorphism group.

Difference sets were first introduced in cyclic groups in the study of projective planes [6, 10]. Most progress in the study of difference sets has occurred in *abelian* groups; indeed the term "difference" comes from the abelian (additive) version of the formula in the definition.

Difference sets with parameters $(4t^2, 2t^2 - t, t^2 - t)$ are often called "Hadamard" difference sets or "Menon" difference sets. They are known to exist in abelian groups of the form $\mathbf{Z}_3^{2s} \times \mathbf{Z}_4^a \times \mathbf{Z}_2^{2b}$ [5, p. 628; 21]. The existence of *abelian* $(4p^2, 2p^2 - p, p^2 - p)$ difference sets for primes $p > 3$ was ruled out by McFarland [20]. The existence of $(4t^2, 2t^2 - t, t^2 - t)$ difference sets with t divisible by any prime greater than 3 were previously unknown. In this paper we construct *non-abelian* difference sets with t divisible by 5.

Little is apparently known in general about *non-abelian* difference sets [14, p. 243]. The author hopes that the discovery detailed in this paper will stimulate a search for difference sets in non-abelian groups. At the same time as this discovery, Xia announced in [24] the construction of abelian difference sets with t divisible by p^4 , p being prime congruent to 3 modulo 4. The parameters $(4t^2, 2t^2 - t, t^2 - t)$ are a fertile ground for further research into difference sets.

Let $\mathbf{Z}G$ be the integral group ring of G . Given a subset A of G , equate A with the element $\sum_{g \in A} g$ of $\mathbf{Z}G$. More generally, for an integer m , define

$$A^{(m)} := \sum_{g \in A} g^m.$$

Then a subset A of G is a difference set iff in the group ring $\mathbf{Z}G$,

$$A \cdot A^{(-1)} = (k - \lambda)1 + \lambda G. \quad (1)$$

Standard introductions to difference sets occur in [5, 11, 15]. Lander's work, [15], now out of print, is an exceptional text and we will assume some familiarity with Chapter 4 of that book.

The representation-theoretic approach to construction of a difference set requires examining Eq. (1) under the images of various irreducible representations. This approach has been promoted by Leibler (in [17, 18]) and a general attack on groups of order $4p^2$ has been initiated by Hams [12].

Call a representation ϕ of G *sufficient* if every member of $\mathbf{Z}G$ is uniquely determined by its image under ϕ (see [18]). A sufficient representation is necessarily faithful; the converse is not true. The direct sum of all the irreducible representations is a sufficient representation.

We assume that each irreducible representation is a unitary representation, and so $\phi(g^{-1}) = \overline{\phi(g)}'$, the conjugate transpose of $\phi(g)$. If ϕ is a representation which does not have the trivial representation as a constituent then $\phi(G) = 0$. If ϕ is a non-trivial irreducible unitary representation then

$$\phi(A) \cdot \overline{\phi(A)}' = (k - \lambda) \phi(1). \quad (2)$$

(Basic material on groups representations are [4, 7, 9, Chap. 3, or 16].)

2. A SPECIAL GROUP OF ORDER 100 AND ITS LINEAR REPRESENTATIONS

For the remainder of this paper, G will be the group of order 100 with presentation

$$G = \langle a, b, c : a^5 = b^5 = c^4 = [a, b] = cac^{-1}a^{-2} = cbc^{-1}b^{-2} = 1 \rangle.$$

The unique Sylow 5-subgroup of G is the commutator subgroup $G' = \langle a, b \rangle$.

Δ will represent a subset of G of size 45.

The first step to finding a difference set is to find the irreducible representations of G . Any linear (that is, one-dimensional) representation will have the commutator subgroup G' in its kernel. In this case G/G' is isomorphic to the cyclic group of order 4 and so G has four inequivalent linear representations. The linear representations are defined by

$$\chi_j(a) = \chi_j(b) = 1, \quad \chi_j(c) = i^j$$

($i^2 = -1$) for $j = 0, 1, 2, 3$. χ_0 is the trivial representation and so $\chi_0(\Delta) = |\Delta| = 45$. If $j = 1, 2$, or 3 then by Eq. (2), $\chi_j(\Delta) \overline{\chi_j(\Delta)} = 25$ and so $\chi_j(\Delta)$ has modulus 5. The linear representation χ_1 maps Δ to a Gaussian integer of modulus 5 and so $\chi_1(\Delta) \in \{\pm 3 \pm 4i, \pm 4 \pm 3i, \pm 5, \pm 5i\}$. The linear representation χ_2 maps Δ to a rational integer of modulus 5; therefore $\chi_2(\Delta) = \pm 5$. $\chi_3(\Delta)$ is the conjugate of $\chi_1(\Delta)$.

The four cosets of G' partition Δ into four sets:

$$\Delta = \Delta_0 \cup \Delta_1 c \cup \Delta_2 c^2 \cup \Delta_3 c^3, \quad \Delta_i \in G'.$$

Or, by viewing sets as members of the group algebra, we have

$$\Delta = \Delta_0 + \Delta_1 c + \Delta_2 c^2 + \Delta_3 c^3, \quad \Delta_i \in \mathbf{Z}G'. \quad (3)$$

We apply the various linear representations χ_j , $j = 0, 1, 2$, to Eq. (3) and find

$$\chi_0(\Delta) = |\Delta_0| + |\Delta_1| + |\Delta_2| + |\Delta_3| = 45$$

$$\chi_1(\Delta) = |\Delta_0| + |\Delta_1| i - |\Delta_2| - |\Delta_3| \quad i \in \{\pm 3 \pm 4i, \pm 4 \pm 3i, \pm 5, \pm 5i\}$$

$$\chi_2(\Delta) = |\Delta_0| - |\Delta_1| + |\Delta_2| - |\Delta_3| = \pm 5.$$

This allows us to solve for $|\Delta_k| = |\Delta \cap G'c^k|$ in terms of $\chi_j(\Delta)$ and we find that the multi-set $\{|\Delta_k|\}$ is either equal to $\{15, 10, 10, 10\}$ or $\{14, 12, 11, 8\}$. This is the first combinatorial fact given by a representation and we summarize it in a lemma.

LEMMA 1. *We may assume (after translating Δ or applying a group automorphism of G/G' , if necessary) that the image of Δ under the natural homomorphism from G to G/G' is either*

- (i) $15G' + 10G'c + 10G'c^2 + 10G'c^3$,
- (ii) $14G' + 12G'c + 11G'c^2 + 8G'c^3$, or
- (iii) $14G' + 8G'c + 11G'c^2 + 12G'c^3$.

Any set which intersects the cosets of G' in this fashion will satisfy Eq. (1) under the image of χ_j , $j = 0, 1, 2, 3$.

The cases in Lemma 1 are distinguished by their image under χ_1 . In the first case $\chi_1(\Delta) = 5$; in the second and third cases $\chi_1(\Delta) = 3 + 4i$ and $3 - 4i$, respectively. (The author wishes to thank an anonymous referee for pointing out the existence of case iii.)

3. THE EQUATION IN $\mathbf{Z} \cdot \text{Frob}(20)$

G has 10 equivalent irreducible representations. We have found the four linear representations and now construct the nonlinear irreducible representations.

The subgroup G' is isomorphic to $\mathbf{Z}_5 \times \mathbf{Z}_5$, the noncyclic group of order 25, and has six subgroups of order 5. These are $H_j = \langle a^j b \rangle$, $j = 0, 1, 2, 3, 4$, and $H_\infty = \langle a \rangle$. Each of these is normal in G and have factor group isomorphic to $F = \langle \alpha, \beta : \alpha^5 = \beta^4 = \beta \alpha \beta^{-1} \alpha^{-2} = 1 \rangle$, the Frobenius group of order 20. F is the key to our construction of Δ . F has one irreducible complex representation ψ' of degree 4 corresponding to the representation induced by a faithful character of $\langle \alpha \rangle$. Explicitly,

$$\psi'(\alpha) = \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{pmatrix}, \quad \psi'(\beta) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

where $\zeta = e^{2\pi i/5}$.

For each subgroup H_j , $j = 0, 1, 2, 3, 4, \infty$, we may define an irreducible representation on G by $\omega'_j(x) := \psi'(H_j x)$. These representations are irreducible because ψ' is. These representations are distinguished by their characters on H_j and so they are mutually inequivalent; this completes the list of irreducible representations of G .

The minimal splitting field of the representations ψ' , ω'_j is $Q[\zeta]$. We may avoid computing in $Q[\zeta]$ by creating integral representations equivalent to ψ' , ω'_j ; unfortunately the new representations are not unitary. Instead we will create integral representations of degree 5 which are equivalent to the direct sum of a representation of degree 4 and the trivial representation. Let ψ be the natural permutation representation of F on the left cosets of the Frobenius complement $\langle \beta \rangle$ by left multiplication. (See [9, pp. 37-38 or 3, p. 190].) This will give us an integral-valued representation ψ equivalent to $\chi_0 \oplus \psi'$; explicitly, we set

$$\psi(\alpha) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \psi(\beta) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

As before, define a representation on all of G by defining $\omega_j(x) := \psi(H_j x)$ for $j = 0, 1, 2, 3, 4, \infty$. Fix $j \in \{0, 1, 2, 3, 4, \infty\}$ and Eq. (1) becomes

$$\omega_j(\Delta) \cdot \omega_j(\Delta)' = 25I_5 + 400J, \quad (4)$$

where J is the matrix of all ones. In addition, $\omega_j(\Delta)J = 45J$.

Set $M = \omega_j(\Delta) - 9J$. Then $MJ = 0$ and $MM' = 25I_5 - 5J$. This gives enough information for us to construct M and thus $\omega_j(\Delta)$.

LEMMA 2. *Let M be a 5×5 matrix with integer entries such that $MJ = 0$ and $MM' = 25I_5 - 5J$. Then, up to permutation of rows and columns, $M = \pm X_1$, or $M = \pm X_2$, where*

$$X_1 = \begin{pmatrix} -4 & 1 & 1 & 1 & 1 \\ 1 & 3 & 0 & -1 & -3 \\ 1 & 0 & -1 & -3 & 3 \\ 1 & -1 & -3 & 3 & 0 \\ 1 & -3 & 3 & 0 & -1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} -4 & 1 & 1 & 1 & 1 \\ 1 & -4 & 1 & 1 & 1 \\ 1 & 1 & -4 & 1 & 1 \\ 1 & 1 & 1 & -4 & 1 \\ 1 & 1 & 1 & 1 & -4 \end{pmatrix}.$$

Proof. Let $(m_1 m_2 m_3 m_4 m_5)$ be a row of M . Then $\sum m_j = 0$ and $\sum m_j^2 = 20$. This forces the row to be (up to permutation) either

- (i) $(-4 \ 1 \ 1 \ 1 \ 1)$,
- (ii) $(4 \ -1 \ -1 \ -1 \ -1)$, or
- (iii) $(3, 1, 0, -1, -3)$.

Using the fact that the inner product of two rows must be -5 , we discover that either all rows have pattern (i), all rows have pattern (ii) or there is a mixture: one row is $(-4 \ 1 \ 1 \ 1 \ 1)$ or $(4 \ -1 \ -1 \ -1 \ -1)$, and the remaining four rows are in the pattern $(3, 1, 0, -1, -3)$. These give the four cases $M = \pm X_1, \pm X_2$ in the lemma.

We have found up to permutations of rows and columns, $\omega_j(\Delta) = 9J + M$. To find a difference set we need to find $\omega_j(\Delta)$ exactly. So we view the group $F = \langle \alpha, \beta : \alpha^5 = \beta^4 = \beta\alpha\beta^{-1}\alpha^{-2} = 1 \rangle$ in several different ways. The representation ψ suggests that we view F as a particular subgroup of $\text{Sym}(5)$, the symmetric group of order 120. Explicitly the permutations $(0 \ 1 \ 2 \ 3 \ 4)$ and

(1 2 4 3) generate a subgroup of $\text{Sym}(5)$ isomorphic to F and we may equate α with (0 1 2 3 4) and β with (1 2 4 3). The representation ψ merely represents these elements as permutation matrices and we may extend ψ to permutation representation of $\text{Sym}(5)$ acting naturally on $\{0, 1, 2, 3, 4\}$.

The subgroup $\langle (0 1 2 3 4), (1 2 4 3) \rangle$ has a left transversal

$$T = \{ \pi_0 = 1, \pi_1 = (13), \pi_2 = (23), \pi_3 = (34), \pi_4 = (12), \pi_5 = (24) \}$$

in $\text{Sym}(5)$. (T has been chosen so that $T^{-1} = T$.) A matrix equivalent to $\omega_j(\Delta)$ under row and column permutations is then of the form $\psi(\pi_k) \omega_j(g \Delta h) \psi(\pi_l)$, where g and h are in F and π_k, π_l are in T . Under this correspondence there exist π_k, π_l from T such that

$$\omega_j(g \Delta h) = \psi(\pi_k)(9J \pm X_i) \psi(\pi_l) = 9J \pm \psi(\pi_k)(X_i) \psi(\pi_l).$$

We will hereafter equate a permutation π_k with its permutation matrix $\psi(\pi_k)$ and so we (somewhat sloppily) summarize the above equation as

$$\omega_j(g \Delta h) = 9J \pm \pi_k(X_i) \pi_l.$$

If Δ is a difference set in a group G then for any g in G , σ in $\text{Aut}(G)$, $g\Delta^\sigma$ is also a difference set, said to be "equivalent to Δ ." Since conjugation is an automorphism, Δ will be a difference set iff $g \Delta h$ is. So we will assume without loss of generality that $\omega_j(\Delta) = 9J \pm \pi_k(X_i) \pi_l$ ($i=1$ or 2). The matrix X_2 is in the center of $\mathbf{Z}\text{Sym}(5)$ and so we may assume further that in that case the difference set has been transformed so that $\omega_j(\Delta) = 9J \pm X_2 \pi_l$. A further simplification can be made if we note that the permutation matrix corresponding to (13)(24) commutes with X_1 . This reduces the possibilities for $\omega_j(\Delta)$ to the 48 matrices $9J \pm \pi_k X_1 \pi_l$ ($k=0, 1, 3$ and $l=0, 1, 2, 3, 4, 5$), or $9J \pm X_2 \pi_l$ ($l=0, 1, 2, 3, 4, 5$).

Given a particular 5×5 matrix $\omega_j(\Delta)$, we still face the difficulty of constructing the corresponding element in $\mathbf{Z}F$. Our viewpoint, so far, implies that the rows and columns of the representation ψ are indexed by $\{0, 1, 2, 3, 4\} = \mathbf{Z}_5$ and therefore the coordinates of the 5×5 matrix may be viewed as points of the affine plane $AG(2, 5)$. We push this further. $\psi(\alpha)$ is the characteristic function of the line $y = x + 1$ and $\psi(\beta)$ is the characteristic function of the line $y = 2x$. More generally $\psi(\alpha^s \beta^t)$ is the characteristic function of the line $y = 2^t x + s$ in $AG(2, 5)$ and we have an injection from the 20 members of F into the 30 lines of $AG(2, 5)$. This map misses the "horizontal" and "vertical" lines of $AG(2, 5)$; these correspond to the rows and columns of the 5×5 matrix. This correspondence equates a member of $\mathbf{Z}F$ with the collection of all functions from the lines of $AG(2, 5)$ to \mathbf{Z} which map the horizontal and vertical lines to zero. The (y, x) coordinate of $\omega_j(\Delta) = \omega_j(\sum_{g \in F} \alpha_g g)$ is the sum of the α_g for all "lines" g on the "point" (y, x) .

We may use a form of "Möbius inversion" [1, Section IV.2] to invert the map ω_j to reconstruct the image of Δ in \mathbf{ZF} . More generally, let f be a function from the lines of an affine plane of order q into the integers \mathbf{Z} . Define a function \hat{f} on points by

$$\hat{f}(p) := \sum_{L \text{ on } p} f(L).$$

It is also advantageous to define a second function \hat{f} on lines

$$\hat{f}(L) := \sum_{p \in L} \hat{f}(p)$$

and to extend f to the parallel classes of the plane by defining, for parallel class Π ,

$$f(\Pi) := \sum_{L \in \Pi} f(L).$$

Then for a fixed line L in a parallel class Π ,

$$\hat{f}(L) = \sum_{p \in L} \sum_{L' \text{ on } p} f(L') = q \cdot f(L) - f(\Pi) + \sum_{\text{all lines } L'} f(L').$$

Given $\hat{f}(L)$, $f(\Pi)$ and the sum $k = \sum_{\text{all lines } L'} f(L')$, we may retrieve the original function f on the line L :

$$f(L) = \{\hat{f}(L) - k + f(\Pi)\}/q. \quad (5)$$

In our case, the lines are members of F and our six parallel classes are the four cosets of $\langle \alpha \rangle$ along with the rows and columns of our 5×5 matrix. We have $k = \sum_{\text{all lines } L'} f(L') = |\Delta| = 45$ and $f(\Pi)$ is either one of $\{15, 10, 10, 10\}$ (case i of Lemma 1), or one of $\{14, 12, 11, 8\}$ (cases ii and iii). The order of the plane, q , is 5. If p is the point (y, x) in the affine plane then $\hat{f}(p)$ is the (y, x) coordinate of the matrix $\omega_j(\Delta)$ and $\hat{f}(L)$ is the sum of the coordinates corresponding to the points on L . Given any matrix $\omega_j(\Delta)$ we can use (5) to solve for $f(L)$.

$$f(L) = \{\hat{f}(L) - 45 + f(\Pi)\}/5 = \{\hat{f}(L) + f(\Pi)\}/5 - 9. \quad (6)$$

Now $f(L)$ is the cardinality of the intersection of Δ and a coset of H_j and so it must be a nonnegative integer no larger than 5. In particular $\{\hat{f}(L) + f(\Pi)\}$ is one of $\{45, 50, 55, 60, 65, 70\}$. This severely restricts the possible values of $f(L)$. For many of the 84 cases mentioned earlier, there are lines L of the matrix (affine plane) such that $f(L)$ is not integral and so the case can be discarded. If we assume parallel classes have $f(\Pi) = \{15, 10, 10, 10\}$ then only $(34) X_1(34), X_2(13), X_2(23), X_2(34), X_2(12)$,

$X_2(24)$, can possibly correspond to homomorphic images of a difference set in G . If we assume parallel classes have $f(H) = \{14, 12, 11, 8\}$ then only $X_1(34)$, $(13)X_1(34)$, $(23)X_1(34)$, $(12)X_1(34)$, $(24)X_1(34)$, and their transposes, can possibly correspond to homomorphic images of a difference set in G .

We will do one example. Suppose that

$$\omega_j(\Delta) = 9J + (34) \cdot X_1 = 9J + \begin{pmatrix} -4 & 1 & 1 & 1 & 1 \\ 1 & 3 & 0 & -1 & -3 \\ 1 & 0 & -1 & -3 & 3 \\ 1 & -3 & 3 & 0 & -1 \\ 1 & -1 & -3 & 3 & 0 \end{pmatrix}.$$

Then $\hat{f}(L)$ is congruent to 3 (modulo 5) for all lines L of slope 1 (such as the diagonal). This forces us into case iii of Lemma 1 and we may assume that the image of Δ in G/G' is $8G' + 11G'c + 12G'c^2 + 14G'c^3$. For example, let L be the "diagonal" of the matrix: L corresponds to the identity in F and the line $y = x$ in $AG(2, 5)$. $\hat{f}(L) = (9-4) + (9+3) + (9-1) + (9+0) + (9+0) = 43$ and so $f(L) = \{43 - 45 + 12\}/5 = 2$. In a similar fashion, we can work out that

$$\begin{aligned} \Delta = & \{2 + 4x + 1x^2 + 3x^3 + 2x^4\} + \{1 + 2x + 3x^2 + 3x^3 + 5x^4\} \beta \\ & + \{0 + 2x + 3x^2 + 2x^3 + 1x^4\} \beta^2 + \{2 + 2x + 3x^2 + 2x^3 + 2x^4\} \beta^3. \end{aligned}$$

Translating Δ to $\alpha \Delta \beta^3$ gives an element we will call Δ_9 in \mathbf{ZF} :

$$\begin{aligned} \Delta_9 = & \{5 + 1x + 2x^2 + 3x^3 + 3x^4\} + \{1 + 0x + 2x^2 + 3x^3 + 2x^4\} \beta \\ & + \{2 + 2x + 2x^2 + 3x^3 + 2x^4\} \beta^2 + \{2 + 2x + 4x^2 + 1x^3 + 3x^4\} \beta^3. \end{aligned}$$

Similar computations for other values of $\omega_j(\Delta)$ give us a complete list of 12 different possible images of Δ in F .

Let σ be the inner automorphism of F corresponding to conjugation by β , that is, $\sigma(g) = \beta g \beta^{-1}$. Define the following members of \mathbf{ZF} :

$$J = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4;$$

$$A = 5 + 2\alpha + 3\alpha^2 + 3\alpha^3 + 2\alpha^4$$

and so

$$\sigma(A) = 5 + 3\alpha + 2\alpha^2 + 2\alpha^3 + 3\alpha^4;$$

$$B = 1 + 3\alpha + 4\alpha^2 + 4\alpha^3 + 3\alpha^4$$

and so

$$\sigma(B) = 1 + 4\alpha + 3\alpha^2 + 3\alpha^3 + 4\alpha^4;$$

$$C = 3 + 4\alpha + 2\alpha^2 + 2\alpha^3 + 4\alpha^4$$

and so

$$\sigma(C) = 3 + 2\alpha + 4\alpha^2 + 4\alpha^3 + 2\alpha^4;$$

$$A' = 5J - A = 3\alpha + 2\alpha^2 + 2\alpha^3 + 3\alpha^4,$$

$$B' = 5J - B, \quad \text{and} \quad C' = 5J - C.$$

Note that $A' + J = \sigma(B)$, $B' + J = \sigma(A)$, and $C' + J = \sigma(C)$ and that all of these elements are fixed by the map $x \rightarrow x^{-1}$.

THEOREM 3. *Let $\Delta = \sum d_g g$ be a member of \mathbf{ZF} and suppose the integers d_g are nonnegative, no larger than 5, and add up to 45. If $\Delta\Delta^{(-1)} = 25I + 100F$ then Δ is, up to equivalence, one of the following:*

$$\begin{aligned} \Delta_1 &= B + \sigma(C')\beta + A'\beta^2 + C'\beta^3, & \Delta_2 &= C + A'\beta + C'\beta^2 + \sigma(A')\beta^3, \\ \Delta_3 &= A + \sigma(C')\beta + B'\beta^2 + C'\beta^3, & \Delta_4 &= C + B'\beta + C'\beta^2 + \sigma(B')\beta^3, \\ \Delta_5 &= B + C'\beta + A'\beta^2 + \sigma(C')\beta^3, & \Delta_6 &= C + \sigma(A')\beta + C'\beta^2 + A'\beta^3, \\ \Delta_7 &= A + C'\beta + B'\beta^2 + \sigma(C')\beta^3, & \Delta_8 &= C + \sigma(B')\beta + C'\beta^2 + B'\beta^3, \\ \Delta_9 &= \{5 + 1\alpha + 2\alpha^2 + 3\alpha^3 + 3\alpha^4\} + \{1 + 0\alpha + 2\alpha^2 + 3\alpha^3 + 2\alpha^4\}\beta \\ &\quad + \{2 + 2\alpha + 2\alpha^2 + 3\alpha^3 + 2\alpha^4\}\beta^2 + \{2 + 2\alpha + 4\alpha^2 + 1\alpha^3 + 3\alpha^4\}\beta^3, \\ \Delta_{10} &= \{0 + 4\alpha + 3\alpha^2 + 2\alpha^3 + 2\alpha^4\} + \{3 + 4\alpha + 2\alpha^2 + 1\alpha^3 + 2\alpha^4\}\beta \\ &\quad + \{3 + 3\alpha + 3\alpha^2 + 2\alpha^3 + 3\alpha^4\}\beta^2 + \{2 + 2\alpha + 0\alpha^2 + 3\alpha^3 + 1\alpha^4\}\beta^3 \\ &= (5J + 5J\beta^3)(1 + \beta^2) - \Delta_9, \\ \Delta_{11} &= \Delta_9^{-1}, \quad \text{and} \quad \Delta_{12} = \Delta_{10}^{-1}. \end{aligned}$$

Remarks. These are the only solutions with non-negative entries. There are other solutions to Eq. (4), such as

$$\begin{aligned} &\{2 + 3\alpha + 3\alpha^2 + 3\alpha^3 + 3\alpha^4\} + \{4 + 2\alpha + 2\alpha^2 + 2\alpha^3 + 2\alpha^4\}\beta \\ &\quad + \{-1 + 3\alpha + 3\alpha^2 + 3\alpha^3 + 3\alpha^4\}\beta^2 + \{0 + 2\alpha + 2\alpha^2 + 2\alpha^3 + 2\alpha^4\}\beta^3, \end{aligned}$$

but the occurrence of a negative number prohibits this from being the image of a difference set.

The 12 elements in the theorem are mutually inequivalent.

If Δ_l , $l \leq 8$, are homomorphic images of a difference set then the difference set falls into case i of Lemma 1. If $\omega_l(\Delta) = \Delta_9$ or Δ_{10} then the difference set falls into case iii of Lemma 1. The last two are from case ii.

Proof of Theorem 3. We explore the four possibilities of Lemma 2:

Case 3A. Suppose that $\omega_j(\Delta) = 9J \pm (X_2) \pi_1$. Then the requirement that the integers d_g be nonnegative and no more than 5 force us to assume that $\pi_i \neq 1$ and that we are in case i of Lemma 1. Formula (6) yields four possible solutions (up to equivalence). If $\omega_j(\Delta) = 9J + (X_2) \pi_1$ then there are two possibilities, depending on which coset of G' has weight 5. These are

$$\Delta_1 = B + \sigma(C') \beta + A' \beta^2 + C' \beta^3,$$

$$\Delta_2 = C + A' \beta + C' \beta^2 + \sigma(A') \beta^3.$$

On the other hand, if $\omega_j(\Delta) = 9J - (X_2) \pi_1$, we have

$$\Delta_3 = A + \sigma(C') \beta + B' \beta^2 + C' \beta^3,$$

$$\Delta_4 = C + B' \beta + C' \beta^2 + \sigma(B') \beta^3.$$

Case 3B. Suppose that $\omega_j(\Delta) = 9J \pm \pi_k(X_1) \pi_1$ and that case i of Lemma 1 holds; that is, Δ intersects cosets of G' in 15 or 10 points. Then modular arithmetic conditions forces $\pi_k = \pi_l = (34)$ and formula (6) gives

$$\Delta_5 = B + C' \beta + A' \beta^2 + \sigma(C') \beta^3,$$

$$\Delta_6 = C + \sigma(A') \beta + C' \beta^2 + A' \beta^3,$$

under the assumption that $\omega_j(\Delta) = 9J + (34) X_1(34)$, and yields

$$\Delta_7 = A + C' \beta + B' \beta^2 + \sigma(C') \beta^3,$$

$$\Delta_8 = C + \sigma(B') \beta + C' \beta^2 + B' \beta^3,$$

if $\omega_j(\Delta) = 9J - (34) X_1(34)$.

Case 3C. On the other hand, we might assume that $\omega_j(\Delta) = 9J \pm \pi_k(X_1) \pi_1$ and that cases ii or iii in Lemma 1 occur; that is, Δ intersects cosets of G' in 14, 12, 11, and 8 points. This forces either $\pi_k = (34)$ and $\pi_l \neq (34)$ or the transpose condition ($\pi_k = (34)$ and $\pi_l \neq (34)$, as in the example) and we discover two results, up to equivalence and inversion: Δ_9 when $\omega_j(\Delta) = 9J + \pi_k(X_1) \pi_1$ and Δ_{10} when $\omega_j(\Delta) = 9J - \pi_k(X_1) \pi_1$. The inversion map $x \rightarrow x^{-1}$ adds Δ_{11} and Δ_{12} to the list.

4. PASTING IT ALL BACK TOGETHER

Now $\phi = \chi \oplus (\sum_{j=1}^6 \omega_j)$ is a sufficient representation. We have found solutions to (4) for the ω_j and now we need to find a set Δ which

simultaneously satisfies (4) for *all* the ω_j ; that is, no matter which subgroup H_j we choose, Δ looks like the image of a difference set in G/H_j .

The first eight solutions, above, require that Δ intersects cosets of G' in 15 or 10 points. The last four require that Δ intersects cosets of G' in 14, 12, 11, or 8 points. If this occurs then all six images of Δ (or $\Delta^{(-1)}$) under the natural maps into G/H_j will be equivalent to either Δ_9 or Δ_{10} . We will show that this is impossible.

Suppose that Δ_9 or Δ_{10} is the image of a $(100, 45, 20)$ difference set in our group G . Pick two subgroups, say H_0 and H_∞ (so that $G/H_0 \cong G/H_\infty \cong F$) and then consider the coset of G' intersecting Δ in 8 elements; arrange these 25 elements in an array so that the rows correspond to cosets of H_0 and the columns correspond to cosets of H_∞ . We may do this in such a way that the "lines" of slope 1 in the matrix correspond to cosets of H_1 , etc., and we may assume after applying a translation or automorphism of \mathbf{Z}_5 , that the row and column sums are 0, 3, 1, 2, 2. (The sums along lines of slope 1 must also be in this pattern *or* a variation of the pattern after a translation by an element of \mathbf{Z}_5 or an automorphism of \mathbf{Z}_5 or a combination of these.) There are then 24 solutions to the row and column sum restrictions. In none of these cases do the cosets of H_1 (the lines of slope 1) yield an appropriate element of $\mathbf{Z}(G/H_1) \cong \mathbf{Z}F$. This rules out $\phi_j(\Delta) = \Delta_9$ or Δ_{10} for the group of order 100 that we are considering. Similarly, Δ_{11} and Δ_{12} are impossible also.

But fortunately the other eight $\mathbf{Z}F$ images are more complicated. Richard Stafford, Robert Morris, and Ted Shorter at the National Security did a computer search using the elements $\Delta_1, \Delta_2, \Delta_3, \dots, \Delta_8$, and found a number of simultaneous solutions, including

$$\begin{aligned} \Delta = & (1 + a + a^4) + (1 + a) b + (1 + a^2 + a^3 + a^4) b^2 \\ & + (1 + a + a^2 + a^3) b^3 + (1 + a^4) b^4 \\ & + \{(a^2 + a^4) + a^4 b + a^3 b^2 + (1 + a^2) b^3 + (a + a^2 + a^3 + a^4) b^4\} c \\ & + \{a^4 + (a + a^2 + a^4) b + (a + a^4) b^2 + (1 + a^2 + a^4) b^3 + a^3 b^4\} c^2 \\ & + \{(a^3 + a^4) + (1 + a^4) b + a^3 b^2 + (a + a^2 + a^3 + a^4) b^3 + ab^4\} c^3. \end{aligned}$$

This is a difference set! The six different images in $\mathbf{Z}F$ are equivalent to Δ_5 , Δ_7 , (twice) and Δ_8 , (three times) and so "Case 3B" of Theorem 3 gives a positive result.

An integer m is a weak multiplier of Δ if $\Delta^{(m)} = \Delta$. Many Hadamard difference sets have -1 as a weak multiplier; that is, $\Delta^{(-1)} = \Delta$. The existence of abelian difference sets with -1 as multiplier is apparently closely related to the existence of Hadamard difference sets (see [23]), although the situation is different in non-abelian groups (see [19]). The difference set Δ (above) has -1 as a weak multiplier.

LEMMA 4 (Menon and Dillon). *Let G_1 be a group with $(4t_1^2, 2t_1^2 - t_1, t_1^2 - t_1)$ difference set Δ_1 and G_2 a group with $(4t_2^2, 2t_2^2 - t_2, t_2^2 - t_2)$ difference set Δ_2 . Let $G_3 = G_1 \times G_2$ and define $\Delta_1^* = (G_1 - 2\Delta_1) \times \{1\}$, $\Delta_2^* = \{1\} \times (G_2 - 2\Delta_2)$. Then the element $\Delta_3 = (0.5) \{G_3 - (\Delta_1^* \Delta_2^*)\}$ is a $(4t^2, 2t^2 - t, t^2 - t)$ difference set in G_3 with $t = 2t_1 t_2$. If both Δ_1 and Δ_2 have multiplier -1 then Δ_3 does also.*

The group $\mathbf{Z}_3^{2s} \times \mathbf{Z}_4^a \times \mathbf{Z}_2^{2b}$ has a Hadamard difference set with multiplier -1 for all nonnegative values of $s, a,$ and $b, a + b > 0$ [5, 21]. We may recursively use such a group and copies of G (our particular non-abelian group of order 100) to construct difference sets with multiplier -1 in groups of orders $4t^2$, where $t = 2^q \cdot 3^r \cdot 5 \cdot 10^s, q, r, s \geq 0,$ and $r > 0 \Rightarrow q > 0$.

ACKNOWLEDGMENTS

This project was initiated during a sabbatical visit by the author to the National Security Agency. Much of the work continued during and between long phone calls with Richard Stafford (National Security Agency). In addition to acknowledging the many contributions of Stafford, the author wishes to thank Robert Morris and Ted Shorter who wrote the program which ultimately found the difference set. Robert Liebler and Joel Iiams (at Colorado State University) made a number of helpful suggestions regarding the general $4p^2$ case which the author specialized to the prime 5. The author also thanks an anonymous referee who pointed out the existence of case iii in Lemma 1 and who found a number of other subtle errors in an earlier version of this paper.

REFERENCES

1. M. AIGNER, "Combinatorial Theory," Springer-Verlag, New York, 1979.
2. K. T. ARASU, Recent results on difference sets, in "Coding Theory and Design Theory Part II," pp. 1-23, Springer-Verlag, New York, 1990.
3. M. ASCHBACHER, "Finite Group Theory," Cambridge Univ. Press, Cambridge, 1986.
4. E. BANNAI AND T. ITO, "Algebraic Combinatorics I, Association Schemes," Lecture Notes Series in Mathematics, Benjamin Cummings, Menlo Park, CA, 1984.
5. T. BETH, D. JUNGnickEL, AND H. LENZ, "Design Theory," Cambridge Univ. Press, Cambridge, 1986.
6. R. H. BRUCK, Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78** (1955), 464-581.
7. C. W. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associative Algebras," Interscience, New York, 1962.
8. J. F. DILLON, Difference sets in two-groups, in "Finite Geometric and Combinatorial Designs," *Contemporary Math.* **111** (1990), 65-72.
9. D. GORENSTEIN, "Finite Groups," Chelsea, New York, 1980.
10. M. HALL, JR., A survey of difference sets, *Proc. Amer. Math. Soc.* **7** (1956), 975-986.
11. M. HALL, JR., "Combinatorial Theory," Blaisdell, Waltham, MA, 1967.
12. J. IAMS, Ph.D. dissertation.
13. D. JUNGnickEL, Design theory, an update, *Ars Combin.* **28** (1989), 29-199.

14. D. JUNGnickel, Difference sets, in "Contemporary Design Theory: A Collection of Surveys" (Dinitz and Stinson, Eds.), pp. 241–324, Wiley, New York, 1992.
15. E. S. LANDER, "Symmetric Designs: An Algebraic Approach," London Math. Soc. Lecture Note Series, Vol. 74, Cambridge Univ. Press, Cambridge, 1983.
16. W. LEDERMANN, "Introduction to Group Characters," Cambridge Univ. Press, Cambridge, 1977.
17. R. A. LIEBER, The inversion formula, preprint.
18. R. A. LIEBER AND K. W. SMITH, On difference sets in certain 2-groups, in "Coding Theory, Design Theory, Group Theory: Proceedings of the Marshall Hall Conference" (D. Jungnickel, Ed.), Wiley, New York, 1992.
19. S. L. MA, A family of difference sets having -1 as an invariant, *European J. Combin.* **10** (1989), 207–209.
20. R. L. MCFARLAND, Difference sets in abelian groups of order $4p^2$, *Mitt. Math. Sem. Giessen* **192** (1989), 1–70.
21. R. L. MCFARLAND, Necessary conditions for hadamard difference sets, in "Design Theory," Vol. 21, IMA Volumes in Mathematics and Its Applications (D. K. Ray-Chaudhuri, Ed.), Springer-Verlag, New York, 1990.
22. R. L. MCFARLAND, Sub-difference sets of hadamard difference sets, *J. Combin. Theory Ser. A* **54** (1990), 112–122.
23. R. L. MCFARLAND AND S. L. MA, Abelian difference sets with multiplier -1 , *Arch. Math.* (1989), 610–623.
24. M. XIA, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory Ser. A* **61** (1992), 230–242.