JOURNAL OF COMBINATORIAL THEORY, Series A 72, 256–276 (1995)

# On Difference Sets in Groups of Order $4p^2$

JOEL E. IIAMS*

*Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523*

*Communicated by the Managing Editors*

Received January 19, 1993

If $p$ is a prime greater than or equal to 5, and $G$ is a group of order $4p^2$ containing a (Menon type) difference set, then either $G$ has an irreducible complex representation of degree 4, or $G \cong \langle x, y, z \mid x^p = y^p = z^4 = 1,\ xy = yx,\ xz = zx,\ zyz^{-1} = y^{-1} \rangle$ and $p \equiv 1 \pmod 4$. The proof involves representation theory, algebraic number theory, and a generalization of Fourier's inversion formula. The six remaining isomorphism classes are considered in part II. 

## I. INTRODUCTION

Let $G$ be a group of order $v$ written multiplicatively. A $(v, k, \lambda)$-*difference set* in $G$ is a subset $D$ of cardinality $k$ so that the multiset $M = \{d_1 d_2^{-1} \mid d_1, d_2 \in D,\ d_1 \neq d_2\}$ replicates each non-identity element of $G$ exactly $\lambda$ times. The integer $n := k - \lambda$ is the *order* of $D$. Counting two ways we have $\lambda(v-1) = k(k-1)$. Equivalently, $k^2 = \lambda v + n$.

Note that any group has four types of trivial difference sets. Namely, the empty set, $G$ itself, any singleton subset of $G$, or its complement. In general, difference sets come in set complementary pairs. Indeed if $D$ is a $(v, k, \lambda)$-difference set in $G$, then $D' = G - D$ is a $(v, v-k, v-2k+\lambda)$-difference set in $G$. Thus to simplify classification and eliminate the trivial types from consideration we take $1 < k < v/2$.

Speifically we are interested in $(4N^2, 2N^2 - N, N^2 - N)$-difference sets. These are known as Menon-type difference sets or Hadamard sets. Observe that Schutzenberger's theorem [4, I, Section 1] and, hence, the Bruck–Ryser–Chowla theorem, are automatically satisfied. Moreover, since every divisor of $n$ is also a divisor of $v$, multiplier theorems like those of Hall do not apply. In contrast group representation theoretic methods are effective in the study of this type of difference set. The main result of this paper is the following.

* Supported in part by a grant from the National Security Agency OCREAE Program, Grant No. MDA904-91-H-0048.



0097-3165/95 $12.00

THEOREM 1.1. *If $N = p \geqslant 5$ is prime and $G$ is a group of order $4p^2$ containing a Menon-type difference set, then one of the following holds*:

(i) *$G$ has an irreducible complex representation of degree 4. In particular, $G$ is isomorphic to one of $G_4, G_{13}, G_{14}, G_{15}$, or $G_{16}$ (see Section 4).*

(ii) *$F \cong G_{11}$ and $p \equiv 1 \pmod 4$.*

These isomorphism classes will be dealt with in part II of this paper. When $N = 2$ or 3, classification was provided by computer search in the paper by Kibler [3]. Turyn [14] and, later, Mann and McFarland [9] showed that if an abelian group of order $4p^2$ has a Menon-type difference set, then $p = 2$ or 3 or $G$ is of type $(4, p, p)$ and $p \equiv 1 \pmod 4$. In a subsequent paper [10] McFarland showed that $p = 2$ or $p = 3$.

Apparently some results in the nonabelian case were known to Lander [4, IV, Problem 3]. Dillon has a method for dealing with some nonabelian cases [4, IV, Problem 17]. Lastly, there is a paper by Liebler [6] that deals with the case $G \cong G_{12}$. Recent results include a successful computer search to find a $(100, 45, 20)$-difference set [13].

The proofs in this paper involved using group representation theory and algebraic number theory to determine the possible homomorphic images of a putative difference set under a given complex representation. These images can be used to calculate the distribution of the difference set among cosets of the kernel of the representation. In some cases this determines that a difference set cannot exist. In other cases it is necessary to take all irreducible complex representations of $G$ into account simultaneously. This is done via the inversion formula [6, Theorem 2.2].

The next section contains relevant background material for representation theory. In Section III we prove vital facts from algebraic number theory. In Section IV we present a list of the isomorphism classes of groups of order $4p^2$, $p$ an odd prime. In Section V we present preliminary results. We study dihedral homomorphic images in Section 6. We finish the proof of Theorem 1.1 in the last section.

For background material on symmetric designs, the reader is directed to Lander [4]. Results from algebraic number theory can be found in the monograph by Weyl [15] or the text by Ireland and Rosen [2]. For information on the representations of finite groups see [1 or 12].

## II. REPRESENTATION THEORY

Denote the ring of integers by $\mathscr{Z}$, the complex field by $\mathscr{C}$, the field of rational numbers by $\mathscr{Q}$, and let $G$ be a finite group written multiplicatively. Let $R$ be a commutative integral domain. For our purposes $R$ is a subring

of $\mathscr{C}$ which contains the integers (see below). The *group ring* for $G$ over $R$, $RG$, consists of all formal linear combinations of group elements with coefficients in $R$. For an element $A \in RG$ one writes

$$A = \sum_{g \in G} a_g g, \qquad a_g \in R.$$

Particularly, subsets of $G$ are represented in $RG$ with coefficients 0 or 1. For an element $A$ of the group ring denote $\sum_{g \in G} a_g g^t$ by $A^{(t)}$. If $D$ is a $(v, k, \lambda)$-difference set in $G$, we get the difference set equation

$$DD^{(-1)} = \left(\sum_{g \in D} g\right)\left(\sum_{g \in D} g^{-1}\right) = \sum_{g_1 \in D} \sum_{g_2 \in D} g_1 g_2^{-1}$$
$$= (k - \lambda) 1_G + \lambda G = n 1_G + \lambda G. \tag{2.1}$$

An *R-representation* of $G$ is a group homomorphism from $G$ into $GL_d(R)$. The integer $d$ is the *degree* of the representation. The $R$-module generated by the image of $G$ in $GL_d(R)$ is the *representation module*. Conversely, any $RG$-module determines a representation [1, p. 47]. Any complex representation for $G$ can be written as a direct sum of irreducible representations. We may also assume that any complex representation is unitary [1, I.10, Exercise 5]. Consequently $\varphi(g^{-1}) = \varphi(g)^{-1} = \overline{\varphi(g)}^{t}$, for $g \in G$, where the overbar is for the complex conjugate and super t is for the transpose.

Since $G$ is finite, the Krull–Schmidt theorem implies that $\mathscr{Q}G$ is an internal direct sum of indecomposable submodules which are $\mathscr{Q}G$-bimodules. This decomposition arises from the decomposition of 1 as the sum of central primitive idempotents [12, p. 19]. For each central primitive idempotent $e_i$ there is an irreducible representation $\varphi_i$ with $\varphi_i(g) = ge_i$ for $g \in G$. Set $\chi_i := \mathrm{tr}(\varphi_i)$. $\chi_i$ is the *character* associated with $e_i$.

A field $K$ is a *splitting field* for $G$ provided that $KG$ splits into an internal direct sum of irreducible submodules and is the smallest such field for which this occurs.

Let $m$ be the exponent of $G$ and $\xi$ be a primitive complex $m$th root of unity. A theorem of Brauer [12, Theorem 3.4.11] states that $K := \mathscr{Q}[\xi]$ is a splitting field for $G$. In this case there exists a formula for the central primitive idempotents in $KG$ [12, Theorem 3.2.22]:

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g.$$

Since $K$ is Galois over $\mathscr{Q}$ we can find the central primitive idempotents in $\mathscr{Q}G$ by summing over the orbits on the $e_i$'s under the action of the Galois group of $K$ over $\mathscr{Q}$.

Set $R = \mathbb{Z}[\xi]$, so that the quotient field, $K$, of $R$ splits $G$. Since $K$ is a splitting field for $G$ the number of terms in the decomposition of 1 in terms of central primitive idempotents is the number of conjugacy classes in $G$ [12, Theorem 3.1.23]. A *character table* for $G$ is a matrix whose columns are labeled by distinct conjugacy classes in $G$ and whose rows are labeled by all the distinct inequivalent irreducible representations over a splitting field for $G$. An essential fact is that this matrix is invertible [1, p. 220].

The *trivial* representation of $G$ is the map which takes each element of $G$ to 1. Since $\mathbb{C}G$ is a $G$-module it determines a representation called the *regular representation.* If $\varphi$ is an irreducible representation for $G$, then $\varphi$ occurs as a direct summand of the regular representation. As a result $\sum_{g \in G} \varphi(g) = 0$ when $\varphi$ is a representation for $G$ which does not contain the trivial representation [12, 3, Example 1.6].

Hence when a unitary representation $\varphi$ not containing the trivial representation is applied to Eq. (2.1) we get

$$\varphi(DD^{(-1)}) = \varphi(D)\,\varphi(D^{(-1)}) = \varphi(D)\,\overline{\varphi(D)}^{\mathrm{t}} = nI_d. \tag{2.2}$$

Regard (2.2) as a matrix equation in the ring of $d \times d$ matrices with entries in $R$ (not $K$!) generated by $\varphi(G)$. We wish to characterize all solutions to (2.2) which can arise from elements $A_i$ of $RG$. Liebler calls these solutions $\varphi_i$-*aliases* for $D$, since $\varphi_i(A) = \varphi_i(A_i)$. We are thus led to the general inversion formula which we state without proof.

THEOREM 2.1 [6, Theorem 2.2]. *Let $K$ be a field of characteristic 0 and let $\{e_i\}$ be the central primitive idempotents for $KG$. For $A \in KG$, we have*

$$A = \sum \varphi_i(A_i)\, e_i, \qquad \textit{where } A_i \textit{ is any } \varphi_i\textit{-alias for } A.$$

In order to find a difference set in $G$ we wish to find an element of $\mathbb{Z}G$ with coefficients either 0 or 1 which simultaneously satisfies each of the irreducible representations for $G$. From the discussion above, we can do this via the inversion formula for $\mathbb{Q}G$.

A *translate* of a difference set $D$ in a group $G$ is a set $Dg$ for some $g \in G$, where $Dg = \{dg \mid d \in D\}$. Any translate of a difference set is again a difference set with the same parameters, since the multiset of differences arising from the translate is identical to the multiset from the difference set.

## III. ALGEBRAIC NUMBER THEORY

In this section $\eta$ denotes a primitive complex $p$th root of unity, $p$ an odd prime. An *algebraic integer* is an element of an algebraic number field

which satisfies a monic polynomial with integer coefficients. The first theorem is commonly referenced in the literature (e.g., [10, p. 15 or 8, p. 83]). For the reader's convenience we provide a proof.

THEOREM 3.1 (Kronecker). *If $\alpha$ is an algebraic integer each of whose algebraic conjugates have modulus one, then $\alpha$ is a root of unity.*

*Proof.* If $\alpha$ is an algebraic integer, then $\alpha$ satisfies a polynomial

$$A(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0$$

with rational integral coefficients. Let $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be the algebraic conjugates of $\alpha$. Then

$$A(X) = \prod_{i=0}^{n-1} (X - \alpha_i).$$

Let $\kappa$ be an algebraic number field which contains all the conjugates of $\alpha$. We have that $m := [\kappa : \mathcal{Q}]$ divides $n!$; i.e., $\kappa$ is finite over $\mathcal{Q}$. Moreover, the ring of integers in $\kappa$ form a discrete lattice [15, IV, 6]. So there are finitely many integers $\beta$ in $\kappa$ having length one. Thus $\alpha$ is in a finite subgroup of $\kappa^*$, the multiplicative group of $\kappa$. Any finite subgroup of the multiplicative group of a field is cyclic [5, V, 4.9]. Thus $\alpha^j = 1$, for some $j$. ∎

LEMMA 3.2. *Let $\xi$ be a primitive $p^n$th root of unity, and let $n$ be a positive integer.*

(a) [10, p. 17]. *Let $a_0, \ldots, a_{p-1} \in \mathcal{Q}$. Then $\sum_{i=0}^{p-1} a_i \eta^i = 0$ if and only if $a_0 = \cdots = a_{p-1}$.*

(b) *Let $a_0, \ldots, a_{p^n-1} \in \mathcal{Q}$. Then $\sum_{l=0}^{p^n-1} a_l \xi^l = 0$ if and only if $a_i = a_j$ when $i \equiv j \pmod{p^{n-1}}$.*

*Proof.* The minimal polynomial for $\xi$ over $\mathcal{Q}$ is

$$\begin{aligned} v(X) &= X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + X^{p^{n-1}} + 1 \\ &= \mu(X^{p^{n-1}}) \qquad [5, \text{p. } 316]. \end{aligned}$$

Set $A(X) = a_0 + a_1 X + \cdots + a_{p^n} X^{p^n} \in \mathcal{Q}[X]$. Then $A(\xi) = 0$ if and only if $v(X)$ divides $A(X)$. Write $A(X) = v(X)\, h(X)$. By long division

$$h(X) = a_{p^n} X^{p^{n-1}} + a_{p^n-1} X^{p^{n-1}-1} + \cdots + a_{p^n-p^{n-1}+2} X + a_{p^n-p^{n-1}+1}.$$

Hence the result. ∎

Lemma 3.2.b will prove useful when groups of order $4p^2$ with cyclic Sylow $p$-subgroups are studied. Although it is elementary, the author could find no reference to it in the literature.

LEMMA 3.3. *Let $\xi$ be a primitive $p^n$th complex root of unity. If $\alpha$ is an algebraic integer in $\mathscr{Z}[\xi]$ all of whose conjugates have length $p$, then $\alpha = \pm p\xi^k$, for some $k$.*

*Proof.* Let $\sigma$ generate $\mathrm{Aut}_{\mathscr{Z}} \mathscr{Z}[\xi]$ by $\xi^\sigma = \xi^g$, where $g$ is a primitive root modulo $p^n$. The prime factorization of the ideal generated by $p$ in $\mathscr{Z}[\xi]$ is $(p) = (1-\xi)^{p^{n-1}(p-1)}$. $\sigma$ fixes $(1-\xi)$, so $\sigma$ fixes $(p)$. By hypothesis $\alpha\bar{\alpha} = p^2$. Moreover,

$$(\alpha\bar{\alpha})^{\sigma^j} = (\alpha)^{\sigma^j}\overline{(\alpha)}^{\sigma^j} = p^2, \qquad j = 0, \ldots, p^{n-1}(p-1).$$

By the uniserial factorization of $(p)$ in $\mathscr{Z}[\xi]$ we have that $\alpha = up$ for some unit $u$ in $\mathscr{Z}[\xi]$. But then every algebraic conjugate of the algebraic integer $u$ has length one. Hence, by the theorem of Kronecker, $u$ is a root of unity in $\mathscr{Z}[\xi]$. ∎

The previous lemma is particularly useful when applied to Eq. (2.2). When $D$ is a $(v, k, \lambda)$-difference set in a group $G$, $D$ must simultaneously satisfy each of $G$'s irreducible representations. In particular it must satisfy (2.2) for all conjugates of a given representation.

LEMMA 3.4 [10, Lemma 5]. *If $\alpha$ is an algebraic integer in $\mathscr{Z}[i\eta]$ of length $p$, then*

(a) *if $p \equiv 3 \pmod 4$ then $\alpha = (i\eta)^e p$, for some $e \in \mathscr{Z}$.*

(b) *if $p \equiv 1 \pmod 4$ then $\alpha$ is one of the following:*

(i) $(i\eta)^e p$,

(ii) $(i\eta)^e (a \pm 2ib)^2$,

(iii) $(i\eta)^e (a \pm 2ib) \sum_{l=1}^{p-1} [l/p]\, \eta^l = (i\eta)^e (a \pm 2ib)\sqrt{p}$,

(iv) $(i\eta)^e (a \pm 2ib) \sum_{l=0}^{p-2} i^{cl}\eta^{g^l}$ *for* $c = 1$ *and* $3$,

*where $e \in \mathscr{Z}$, $g$ is a primitive root modulo $p$, $[l/p]$ is the Legendre symbol, and $a$ and $b$ are the unique positive integers so that $p = a^2 + 4b^2$.*

*Proof.* Let $\Pi$ denote the ideal generated by $1-\eta$ in $\mathscr{R} := \mathscr{Z}[i\eta]$. The ring $\mathscr{R}/\Pi$ is isomorphic to the finite ring $\mathscr{Z}_p[i]$. An element $x = c + \mathrm{id}$ of $\mathscr{R}$ generates a non-trivial ideal containing $\Pi$ if modulo $\Pi$, $x \neq 0$ and $x$ is not a unit. The norm map from the Gaussian integers induces a map $N$ from $\mathscr{R}/\Pi$ to the integers modulo $p$. Hence, if $x$ is not a unit,

$$N(x) = c^2 + d^2 \equiv 0 \pmod p.$$

Hence, when $p \equiv 3 \pmod 4$ $\Pi$ is prime. While when $p \equiv 1 \pmod 4$, $\Pi$ has prime factorization

$$\Pi = (1-\eta, a+2ib)(1-\eta, a-2ib).$$

Let $\sigma$ generate $\mathrm{Aut}_{\mathscr{Z}} \mathscr{Z}[\eta]$ and extend $\sigma$ to an automorphism of $\mathscr{R}$ by fixing $i$. From the preceding paragraph we see that $\sigma$ fixes all prime ideal factors of $(p)$ in $\mathscr{R}$ since in $\mathscr{Z}[\eta]$, $(p)$ factors as $(p) = (1-\eta)^{p-1}$. If $\alpha$ is an algebraic integer of length $p$ in $\mathscr{R}$ then $\alpha\bar{\alpha} = p^2$. Hence the ideal generated by $\alpha$ contains the ideal generated by $p$ and so it is invariant under $\sigma$. Thus $\alpha^\sigma = u\alpha$ for some unit $u \in \mathscr{R}$.

Now for $j = 0, \ldots, p-1$,

$$p^2 = (p^2)^{\sigma^j} = \alpha\bar{\alpha} = \alpha^{\sigma^j}\bar{\alpha}^{\sigma^j}.$$

Thus each algebraic conjugate of the algebraic integer $u = \alpha^\sigma/\alpha$ has length one. Thus by the theorem of Kronecker $u = (i\eta)^e$ for some $e \in \mathscr{Z}$.

If necessary, shift $\alpha$ by $\eta^{e(1-g)^{-1}}$ so that

$$\begin{aligned}(\alpha')^\sigma &= (\eta^{e(1-g)^{-1}}\alpha)^\sigma = (\eta^{e(1-g)^{-1}})^\sigma \alpha^\sigma \\ &= \eta^{e(1-g)^{-1}g}(i\eta)^e\alpha = \eta^{(eg+e-eg)/1-g} i^e\alpha \\ &= i^e\eta^{e(1-g)^{-1}}\alpha = i^e\alpha'.\end{aligned}$$

Since $\{\eta^{g^j} : j = 0, \ldots, p-2\}$ forms an integral basis for $\mathscr{Q}[i\eta]$ over $\mathscr{Q}[i]$ we can write $\alpha$ uniquely as

$$\alpha = \sum_{j=0}^{p-2} c_j \eta^j \qquad \text{with the } c_j\text{'s in } \mathscr{Z}[i].$$

Then the equation $\alpha^\sigma = i^e\alpha$ implies that $c_j = i^e c_{j+1}$ for $j = 0, \ldots, p-3$ and $c_{p-2} = i^e c_0$. So $c_j = i^{-ej}c_0$ for $j = 1, \ldots, p-2$. Set $c := c_0$; then

$$\alpha = c\sum_{j=0}^{p-2} i^{-ej}\eta^{g^j}. \tag{3.1}$$

If $e = 0$ in Eq. (3.1), then $\alpha = -c$ is an algebraic integer in $\mathscr{Z}[i]$ of length $p$. Thus when $p \equiv 3 \pmod 4$, $\alpha = p$ or an associate. While when $p \equiv 1 \pmod 4$, $\alpha$ is either of type (i) or of type (ii).

If $e = 2$, then the sum in (3.1) is a quadratic Gauss sum which is $\sqrt{p}$ when $p \equiv 1 \pmod 4$ and $i\sqrt{p}$ when $p \equiv 3 \pmod 4$ [2, Chap. 6, Theorem 1]. Thus $c$ is an algebraic integer in $\mathscr{Z}[i]$ of length $\sqrt{p}$. When $p \equiv 3 \pmod 4$ this is impossible. When $p \equiv 1 \pmod 4$, $c$ is $a \pm 2ib$ or an associate. This is type (iii) for part (b).

Finally, if $e=1$ or 3, the sum in (3.1) is a quartic Gauss sum of length $\sqrt{p}$ [2, Proposition 8.2.2]. So $c$ is again an algebraic integer of length $\sqrt{p}$ in $\mathscr{Z}[i]$. This is type (iv) for part (b). ∎

## IV. Groups of order $4p^2$, $p$ an Odd Prime

In this section $p$ is an odd prime, $C_a$ denotes the cyclic group of order $a$ and $D_a$ is the dihedral group of order $a$. When $p \equiv 1 \pmod 4$, $-1$ is a quadratic residue modulo $p$ and also modulo $p^2$. Let $f$ be an integer so that $f^2 \equiv -1 \pmod{p^2}$.

Let $G$ be a group of order $4p^2$ written multiplicatively. Let $H$ be a Sylow $p$-subgroup and $K$ a Sylow 2-subgroup. If $H$ is not normal in $G$, then $p=3$ and this case is thereby covered by Kibler [3]. So we may assume that $H$ is normal in $G$. If $z \in K$, then $zHz^{-1}=H$. That is, conjugation of $H$ by $z$ induces an automorphism of $H$. Since $H \cap K = \varnothing$ and $G = HK$, $G = H \rtimes K$ (semi-direct product) [5, I, Exercise 40]. Thus groups of order $4p^2$ can be classified by considering homomorphic images of $K$ in Aut $H$ up to equivalence by conjugation.

When $H$ is cyclic, Aut $H \cong C_p \times C_{p-1}$ is too. Thus a list of the isomorphism classes in this case is

$$G_1 \cong \langle x, z \mid x^{p^2} = z^4 = 1, \text{abelian} \rangle \cong C_{4p^2}.$$

$$G_2 \cong \langle x, z, w \mid x^{p^2} = z^2 = w^2 = 1, \text{abelian} \rangle \cong C_{2p^2} \times C_2.$$

$$G_3 \cong \langle x, z \mid x^{p^2} = z^4 = 1, zxz^{-1} = x^{-1} \rangle.$$

$$G_4 \cong \langle x, z \mid x^{p^2} = z^4 = 1, zxz^{-1} = x^f \rangle \ (p \equiv 1 \pmod 4).$$

$$G_5 \cong \langle x, z, w \mid x^{p^2} = z^2 = w^2 = 1, wx = xw, wz = zw, zxz = x^{-1} \rangle \cong D_{4p^2}.$$

When $H$ is elementary abelian, view it as a two-dimensional vector space over $GF(p)$. Then automorphisms of $H$ can be identified with $2 \times 2$ matrices over $GF(p)$ in canonical form. The image of an element of $K$ in Aut $H$ has order 1, 2, or 4. Hence the list of isomorphism classes in this case is

$$G_6 \cong \langle x, y, z \mid x^p = y^p = z^4 = 1, \text{abelian} \rangle \cong C_{4p} \times C_p.$$

$$G_7 \cong \langle x, y, z, w \mid x^p = y^p = z^2 = w^2 = 1, \text{abelian} \rangle \cong C_{2p} \times C_{2p}.$$

$$G_8 \cong \langle x, y, z, w \mid x^p = y^p = z^2 = w^2 = 1, xy = yx, xz = zx, xw = wx, yz = zy, wyw = y^{-1}, zw = wz \rangle.$$

$$G_9 \cong \langle x, y, z, w \mid x^p = y^p = z^2 = w^2 = 1, xy, xz = zx, wxw = x^{-1}, yz = zy, wyw = y^{-1}, wz = zw \rangle.$$

$G_{10} \cong \langle x, y, z, w \mid x^p = y^p = z^2 = w^2 = 1,\ xy = yx,\ zxz = x^{-1},\ xw = wx,\ yz = zy,\ wyw = y^{-1},\ wz = zw \rangle \cong D_{2p} \times D_{2p}$.

$G_{11} \cong \langle x, y, z \mid x^p = z^4 = 1,\ xy = yx,\ xz = zx,\ zyz^{-1} = y^{-1} \rangle$.

$G_{12} \cong \langle x, y, z \mid x^p = y^p = z^4 = 1,\ xy = yx,\ zxz^{-1} = x^{-1},\ zyz^{-1} = y^{-1} \rangle$.

$G_{13} \cong \langle x, y, z \mid x^p = y^p = z^4 = 1,\ xy = yx,\ zxz^{-1} = y^{-1},\ zyz^{-1} = x \rangle$.

When $p \equiv 1 \pmod 4$ the last group is also presented by

$G'_{13} \cong \langle x, y, z \mid x^p = y^p = z^4 = 1,\ zxz^{-1} = x^f,\ zyz^{-1} = y^{-f} \rangle$,

and there are, in addition,

$G_{14} \cong \langle x, y, z \mid x^p = y^p = z^4 = 1,\ xy = yx,\ zxz^{-1} = x,\ zyz^{-1} = y^f \rangle$.

$G_{15} \cong \langle x, y, z \mid x^p = y^p = z^4 = 1,\ xy = yz,\ zxz^{-1} = x^{-1},\ zyz^{-1} = y^f \rangle$.

$G_{16} \cong \langle x, y, z \mid {}^p = y^p = z^4 = 1,\ xy = yx,\ zxz^{-1} = x^f,\ zyz^{-1} = y^f \rangle$.

Now note that each isomorphism class, where $K$ is elementary abelian has as homomorphic image either $D_{4p}$ or $C_{2p} \times C_2$. Also note that, save for $G_4$, each isomorphism class where $H$ is cyclic has as homomorphic image either $D_{2p^2}$ or $C_{p^2}$. In the next section we repeatedly use the elementary fact that the composition of onto group homomorphisms is again an onto group homomorphism.

## V. Preliminary Results

Throughout this section, $G$ is a multiplicative group of order $4p^2$ and $D$ is a putative $(4p^2, 2p^2 - p, p^2 - p)$-difference set in $G$, where $p$ is an odd prime. This section contains a sequence of lemmas with hypotheses of the following form.

Hypothesis. *Suppose $G$ has a normal subgroup $K$ so that $G/K$ is isomorphic to some explicit group with conjugacy class representatives $Kg_1, \ldots, Kg_m$. Then $G/K$ has a character table of the form $C$ (an $m \times m$ matrix). Let $\mathbf{v}$ be the $m$-tuple of integers having $i$th entry $\sum |g^k|_K$, where the summation runs over the $G/K$-conjugacy class of $g$ and $|g|_K := |Kg \cap D|$.*

The results of Section 3 give only finitely many possibilities for $\mathbf{b} = C\mathbf{v}$, and each such linear system has a unique solution by Theorem 2.1. In this manner we argue that $\mathbf{v}$ has one of finitely many explicit forms. In each case we can label the first row of the character table by the trivial representation. The linear equation arising from this row is always $\sum |g|_K = k = p^2 - p$.

We find that little is gained by generalizing later results. Therefore the statements of results throughout are not presented in full generality. The first three lemmas are due to Menon [11].

LEMMA 5.1. *Suppose* $C_2 \cong G/K = \langle Kz \rangle$, $z \in G$. *Then* $G/K$ *has as character table* $C = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$ *and in some order,* $|1|_K$ *and* $|z|_K$ *are* $p^2$ *and* $p^2 - p$.

*Proof.* Define a linear representation $\chi$ for $G$ by $\chi(z) = -1$, $\ker \chi = K$. We have that $\chi(D) = |1|_K - |z|_K$. Equation (2.2) yields

$$(|1|_K - |z|_K)^2 = p^2.$$

Thus $|1|_K - |z|_K = \pm p$. We also have that $|1|_K + |z|_K = |K \cap D| + |Kz \cap D| = |D| = k = 2p^2 - p$. Thus $C\mathbf{v} = \binom{k}{\pm p}$. The indicated $\mathbf{v}$ are the unique solutions to this linear system by Theorem 2.1.

LEMMA 5.2. *Suppose* $C_2 \times C_2 \cong G/K = \langle Kz \rangle \times \langle Kw \rangle$, $w$, $z \in G$. *Then in some order* $|1|_K$, $|z|_K$, $|w|_K$, *and* $|wz|_K$ *are*

$$\frac{p(p+1)}{2}, \frac{p(p-1)}{2}, \frac{p(p-1)}{2}, \frac{p(p-1)}{2}.$$

*Proof.* $G/K$ has character table

$$C = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}.$$

with column labels $1, z, w, zw$ and row labels, say $\varphi_0, \varphi_1, \varphi_2, \varphi_3$. The vector $\mathbf{b}$ must be

$$\begin{pmatrix} k \\ \pm p \\ \pm p \\ \pm p \end{pmatrix}.$$

Since $p$ is odd, the unique solutions are those above by integrality of the $|g|_K$. ∎

At this point the sieving action of our method begins to emerge. As the size of the kernel of a homomorphism increases, the number of possible subsets of cardinality $k$ which satisfy all pertinent representations decreases.

LEMMA 5.3. *Suppose* $C_4 \cong G/K = \langle Kz \rangle$, $z \in G$. *Then in some order the intersection numbers* $|z^l|_K$, $l = 0, 1, 2, 3$, *are*

$$\frac{p(p+1)}{2}, \frac{p(p-1)}{2}, \frac{p(p-1)}{2}, \frac{p(p-1)}{2}$$

*when* $p \equiv 3 \pmod 4$. *When* $p \equiv 1 \pmod 4$ *we may also have*

$$\{\{|1|_K, |z^2|_K\}, \{|z|_K, |z^3|_K\}\}$$
$$= \{\{\tfrac{1}{2}(p^2 \pm (a^2 - 4b^2)\}, \{\tfrac{1}{2}(p^2 - p \pm 4ab)\}\},$$

*where* $a$ *and* $b$ *are unique positive integers so that* $p = a^2 + 4b^2$.

*Proof.* Define a linear representation $\chi$ for $G$ by $\chi(z) = i$, $\ker \chi = K$. We have that $\chi(D) = |1|_K + i\,|z|_K - |z^2|_K - i\,|z^3|_K$. Equation (2.2) yields $|\chi(D)|^2 = p^2$. So $\chi(D)$ is a Gaussian integer $\alpha$ of length $p$. From the proof of Lemma 3.4 $\alpha$ is an associate of $p$ when $p \equiv 3 \pmod 4$. When $p \equiv 1 \pmod 4$, $\alpha$ may also be an associate of $(a \pm 2ib)^2$. A character table $C$ for $G/K$ has columns labeled by $z^m$, $m = 0, 1, 2, 3$, and rows labeled by $\chi^l$, where $\chi^l(g) = \chi(g)^l$, $l = 0, 1, 2, 3$, and $C_{l,m} = \chi(z^l)^m$, $l, m = 0, 1, 2, 3$. The possible vectors $\mathbf{b}$ are of the form $(k, \alpha, \pm p, \bar{\alpha})^t$. The solutions to the resulting linear systems are listed above. ∎

LEMMA 5.4. *Suppose* $C_p \cong G/K = \langle Kx \rangle$. *Then there is a unique* $j \in \{0, ..., p-1\}$ *so that*

$$|x^j|_K = 2p - 1 + \varepsilon(p-1), \qquad |x^l|_K = 2p - 1 - \varepsilon$$

*for* $l \neq j$, *where* $\varepsilon = \pm 1$.

*Proof.* Define a representation $\chi$ for $G$ by $\chi(x) = \eta$, $\ker \chi = K$, where $\eta$ is a primitive complex $p$th root of unity. We have that $\chi(D) = \sum_{l=0}^{p-1} |x^l|_K \eta^l \in \mathscr{Z}[\eta]$. By Eq. (2.2), $\chi(D)$ has length $p$. By Lemma 3.3 $\chi(D) = \varepsilon p \eta^j$ for some integer $j$. Next, define $\chi^l$ as a representation for $G$ by $\chi^l(x) = \eta^l$, $\ker \chi^l = K$, $l = 0, ..., p-1$. Then $G/K$ has character table $C$ with $l, m$-entry $\chi^l(x^m)$, $l, m = 0, ..., p-1$, where rows of $C$ are labeled by the representations $\chi^l$ and columns of $C$ are labeled by powers of $x$. Meanwhile the $i$ th entry of $\mathbf{b}$ is

$$b_i = \begin{cases} k, & \text{if } i = 0 \\ \varepsilon p \eta^{ij}, & \text{otherwise} \end{cases}.$$

The result follows by Theorem 2.1. ∎

LEMMA 5.5. *Suppose* $C_p \times C_2 \cong G/K = \langle Kx \rangle \times \langle Kz \rangle$. *Let* $\varepsilon$ *and* $j$ *be as in the preceeding lemma. Then for some* $\zeta = \pm 1$ *and a suitable translate of* $D$ *we have*

$$|x^j|_K = p + (\varepsilon + \zeta)\frac{p-1}{2}, \qquad |x^l|_K = p - \frac{\varepsilon \in \zeta}{2} \quad \text{for} \quad l \neq j.$$

*Also* $|x^j z|_K = ((p-1)/2)(2 + \varepsilon - \zeta)$ *and* $|x^l z|_K = p - 1 + (\zeta - \varepsilon)/2$ *for* $l \neq j$.

*Proof.* Define a linear representation $\chi_1$ for $G$ with kernel $K$ by $\chi_1(x)=\eta$, $\chi_1(z)=-1$. Set $H:=K\cup Kz$ and $|g|_H=|Hg\cap D|$. Equation (2.2) implies that $|\chi_1(D)|=p$. By Lemma 3.3 $\chi(D)=\zeta p\eta^j$ for some integer $j$ and some $\zeta=\pm 1$. Hence,

$$0=\chi_1(D)-\zeta p\eta^j=(|x^j|_K-|x^jz|_K-\zeta p)\eta^j+\sum_{\substack{l=0\\ l\neq j}}^{p-1}(|x^l|_K-|x^lz|_K)\eta^l.$$

By Lemma 3.2, $|x^l|_K-|x^lz|_K$ and, hence, $|x^l|_K+|x^l|_H$ have the same parity for $l\neq j$. Thus $j$ is as in Lemma 5.4.

Now, $G/K$ has a character table of the form $C=C_1\otimes C_2$, where $C_1$ is from the previous the lemma and $C_2$ is from Lemma 5.1. The rows of $C$ are labeled by the representations $\chi^i\otimes\psi^l$; $l=0, 1$; $i=0, ..., p-1$, where $\chi^i\otimes\psi^l(x)=\eta^i$, and $\chi^i\otimes\psi^l(z)=(-1)^l$. ($\chi_1=\chi^1\otimes\psi^1$). The columns of $C$ are labeled by $x^iz^l$; $l=0, 1$; $i=0, ..., p-1$. Replace $D$ by $Dz$ if necessary so that, by Lemma 5.1, $\sum_{l=0}^{p-1}|x^l|=p^2$. Then the entries of the vector $\mathbf{b}$ are given by

$$b_i,\ l=\begin{cases} k, & \text{if } i=l=0\\ \varepsilon p\eta^{ij}, & \text{if } l=0;\ i=1, ..., p-1\\ p, & \text{if } l=1;\ i=0\\ \zeta p\eta^{ij}, & \text{if } l=1;\ i=1, ..., p-1.\end{cases}$$

The result follows by Theorem 2.1. ∎

LEMMA 5.6. *Suppose* $C_p\times C_2\times C_2\cong G/K=\langle Kx\rangle\times\langle Kz\rangle\times\langle Kw\rangle$, $x$, $z$, $w\in G$. *Let* $j$ *and* $\varepsilon$ *be as in Lemma* 5.4. *Then for a suitable translate of* $D$,

$$\begin{pmatrix}|x^j|_K\\ |x^jz|_K\\ |x^jw|_K\\ |x^jzw|_K\end{pmatrix}=\begin{pmatrix}\frac{p+1}{2}\\ \frac{p-1}{2}\\ \frac{p-1}{2}\\ \frac{p-1}{2}\end{pmatrix}+\frac{p-1}{4}C_2\begin{pmatrix}\varepsilon\\ \varepsilon_1\\ \varepsilon_2\\ \varepsilon_3\end{pmatrix},$$

*where* $C_2$ *is the character table in Lemma* 5.2 *and* $\varepsilon_i=\pm 1$. *Also for* $l\neq j$

$$|x^l|_K=\tfrac{1}{4}[2p+2-\varepsilon-\varepsilon_1-\varepsilon_2-\varepsilon_3].$$

*Proof.* Set $L=\langle Kx\rangle$ and $H=\langle Kz, Kw\rangle$ so that $G/K=L/K\times H/K$. Then $G/K$ has character table $C=C_1\otimes C_2$, where $C_1$ is as in Lemma 5.4 and $C_2$ is as in Lemma 5.2. With the notation of those lemmas we take

$$\chi^l\otimes\varphi_i(Kx^az^bw^c)=\eta^{al}\varphi_i(Hz^bw^c).$$

As in Lemma 5.5

$$\chi \otimes \varphi_i = \varepsilon_i p\eta^{k(i)}, \qquad \text{some } k(i), \quad \varepsilon_i = \pm 1,\ i = 1, 2, 3.$$

That is

$$\sum_{l=0}^{p-1} (|x^l|_K - |x^l w|_K - |x^l z|_K + |x^l zw|_K)\eta^l = \varepsilon_1 p\eta^{k(1)}$$

$$\sum_{l=0}^{p-1} (|x^l|_K - |x^l w|_K + |x^l z|_K - |x^l zw|_K)\eta^l = \varepsilon_2 p\eta^{k(2)}$$

$$\sum_{l=0}^{p-1} (|x^l|_K + |x^l w|_K - |x^l z|_K - |x^l zw|_K)\eta^l = \varepsilon_3 p\eta^{k(3)}.$$

By Lemma 3.2 for $l \neq k(1)$,

$$\begin{aligned} &|x^l|_K - |x^l w|_K - |x^l z|_K + |x^l zw|_K \\ &\quad = |x^{k(1)}|_K - |x^{k(1)} w|_K - |x^{k(1)} z|_K + |x^{k(1)} zw|_K - \varepsilon_1 p \end{aligned}$$

and for $l \neq k(2)$,

$$\begin{aligned} &|x^l|_K - |x^l w|_K + |x^l z|_K - |x^l zw|_K \\ &\quad = |x^{k(2)}|_K - |x^{k(2)} w|_K + |x^{k(2)} z|_K - |x^{k(2)} zw|_K - \varepsilon_2 p \end{aligned}$$

and for $l \neq k(3)$,

$$\begin{aligned} &|x^l|_K + |x^l w|_K - |x^l z|_K - |x^l zw|_K \\ &\quad = |x^{k(3)}|_K + |x^{k(3)} w|_K - |x^{k(3)} z|_K - |x^{k(3)} zw|_K - \varepsilon_3 p. \end{aligned}$$

So, for example, $|x^l|_K - |x^l w|_K - |x^l z|_K + |x^l zw|_K$ has the same parity for all $l \neq k(1)$. Thus, $|x^l|_K + |x^l w|_K + |x^l z|_K + |x^l zw|_K := |Hx^l \cap D|$ has the same parity for all $l \neq k(1)$. Hence, $k(1) = k(2) = k(3) := j$ as in Lemma 5.4.

Replace $D$ by $Dz$, $Dw$, or $Dwz$, if necessary, so that, by Lemma 5.2, $\sum_{l=0}^{p-1} |x^l|_K = p(p+1)/2$. Set $\varepsilon_0 := \varepsilon$. Then the vector $\mathbf{b}$ has entries indexed by the $\chi^l \otimes \varphi_i$'s which are given by

$$b_{l,i} = \begin{cases} k = 2p^2 - p, & \text{if } \ l = i = 0 \\ p, & \text{if } \ i \neq 0,\ l \equiv 0 \pmod{p} \\ \varepsilon_i \eta^{lj} p, & \text{otherwise.} \end{cases}$$

Theorem 2.1 now yields the result. ∎

LEMMA 5.7. *Suppose* $C_{p^2} \cong G/K = \langle Kx \rangle$, $x \in G$, *and* $|K| = 4$. *Then there is no Menon-type difference set in* $G$.

*Proof.* Note that $0 \leqslant |g|_K \leqslant 4$, since $|K| = 4$. Define $\chi$ by $\chi(x) = \xi$, where $\xi$ is a primitive $p^2$th root of unity. We have $\chi(D) = \sum_{l=0}^{p^2-1} |x^l| \xi^l$. Equation (2.2) implies that $|\chi(D)| = p$. By Lemma 3.3, $\chi(D) = \zeta p \xi^m$, $\zeta = \pm 1$ for some $m$. Apply Lemma 3.2(b) with $n = 2$ to $\chi(D) - \zeta p \xi^m$; then when $j \equiv m \pmod{p}$, but $j \neq m$,

$$|x^j|_K = |x^m|_K - \zeta p.$$

Since $0 \leqslant |g|_K \leqslant 4$, we must have that $p \leqslant 3$. Kibler [3] reports that no group of order 36 with cyclic Sylow 3-subgroup has a non-trivial difference set. ∎

## VI. Groups of Order $4p^2$ with Dihedral Homomorphic Images

In this section we study groups of order $4p^2$ with dihedral images for $p$ an odd prime. Throughout this section $D$ is a putative $(4p^2, 2p^2 - p, p^2 - p)$-difference set in $G$ and $K$ is a normal subgroup of $G$ so that $D_{2t} \cong G/K = \langle Kh \rangle \rtimes \langle Kz \rangle$, $h, z \in G$. In this case, $\langle Kh \rangle$ generates a cyclic subgroup of order $t$ dividing $2p^2$. Let $\langle Kx \rangle$ generate the $p$-part of this subgroup and let $\langle Kw \rangle$ generate the 2-part (if any). Set $H/K = \langle Kh \rangle$ and $L/K = \langle Kx \rangle$. Regard $H$ and $L$ as subgroups of $G$ and for an element $g$ of $G$ and a subgroup $S$ of $G$ write $|g|_s$ for $|Sg \cap D|$.

With the notation above, let $\psi$ be a non-trivial linear representation of $H$ with kernel containing $K$. Then $G$ affords an induced representation $\varphi = \psi^G$ of degree 2 by

$$\varphi(h) = \begin{bmatrix} \psi(h) & 0 \\ 0 & \overline{\psi(h)} \end{bmatrix}, \qquad \varphi(z) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

In addition, $\ker \varphi = \ker \psi$ [1, II, Section 12D]. Two such representations are equivalent if and only if they have the same character. Hence there are $(t-1)/2$ distinct inequivalent representations of $G/K$ of this form. These are irreducible as long as $x$ is not in the kernel of $\psi$.

When $x$ is in the kernel, $\varphi$ reduces to a linear representation of $\langle Kz \rangle \times \langle Kw \rangle$. If $\langle Kw \rangle$ is non-trivial we label the representation $\varphi_i$, $i = 1, 2, 3$, as in Lemma 5.2. If $\langle Kw \rangle$ is trivial, define $\varphi_1$ by $\varphi(h) = 1$, $\varphi(z) = -1$. In both cases denote the trivial representation by $\varphi_0$.

Finally, set $c = \sum_{l=0}^{t-1} |h|_K \psi(h)$ and $d = \sum_{l=0}^{t-1} |hz|_K \psi(h)$, where $x$ is not in the kernel of $\psi$. Then we have that

$$\varphi(D) = \begin{bmatrix} c & d \\ \bar{d} & \bar{c} \end{bmatrix}.$$

By Eq. (2.2)

$$\begin{bmatrix} c\bar{c}+d\bar{d} & 2cd \\ 2\overline{cd} & c\bar{c}+d\bar{d} \end{bmatrix} = \begin{bmatrix} p^2 & 0 \\ 0 & p^2 \end{bmatrix}. \tag{6.1}$$

Thus $2cd=0$. So one of $c$ or $d$ is 0 and the other has length $p$.

LEMMA 6.1. *Let $K \lhd G$ with $G/K \cong D_{2p}$. Then for a suitable translate of $D$ there is a unique $j \in \{0, ..., p-1\}$ so that*

(i) $|x^j|_K = p + \varepsilon(p-1)$, $|x^l|_K = p - \varepsilon$, $l \neq j$; $|x^l z|_K = p-1$, $l \in \{0, ..., p-1\}$ *or*

(ii) $|x^l|_K = p$, $l \in \{0, ..., p-1\}$; $|x^j z|_K = (1+\varepsilon)(p-1)$, $|x^l z|_K = p-1-\varepsilon$, $l \neq j$.

*Proof.* Let $\eta$ be a primitive complex $p$th root of unity and set $\psi(x)=\eta$. The degree 2 irreducible representations of $G/K$ are induced from $\psi^l(x)=\eta^l$, $l=1, ..., (p-1)/2$, and are all conjugate. In this case $\langle Kw \rangle$ is trivial, so $H=L$. Replace $D$ by $Dz$ if necessary so that $|1|_H = p^2$ by Lemma 5.1.

*Case $d=0$.* If $d=\sum_{l=0}^{p-1} |x^l z|_K \eta^l = 0$, by Lemma 3.2 and the fact that $p^2 - p = \sum_{l=0}^{p-1} |x^l z|_K = |z|_H$ we get $|x^l z|_K = p-1$, $l=0, ..., p-1$. Next, apply Lemma 3.3 to $c$. Then apply Lemma 3.2 to $c - \varepsilon\eta^k$ and use the fact that $p^2 = \sum_{l=0}^{p-1} |x^l|_K = |H \cap D|$. This is case (i) of the lemma.

*Case $c=0$.* This is similar and we omit the proof. ∎

LEMMA 6.2. *Let $K$ be a normal subgroup of $G$ with $G/K \cong D_{4p}$ and $|K|=p$. If $G$ has a Menon-type difference set then $p \leqslant 3$.*

*Proof.* Apply Lemma 5.2 to $L$ and replace $D$ by one of $Dz$, $Dw$, or $Dzw$, if necessary, so that

$$\sum_{j=0}^{p-1} |x^j|_K = |L \cap D| = \frac{p(p+1)}{2}. \tag{6.2}$$

Let $\psi = \chi \otimes \varphi_3$ be a representation of $H$ with kernel $K$, where $\chi$ is as in Lemma 5.4 and $\varphi_3$ is from Lemma 5.2. Denote by $\varphi^{(2)}$ the degree-2 representation of $G/K$, induced from $\chi$ with kernel $N := K \cup Kw$.

*Case $d=0$.* If $d=\sum_{l=0}^{p-1} (|x^l z|_K - |x^l zw|_K)\eta^l = 0$, then $|x^j z|_K - |x^j zw|_K := f$ is constant for all $j$ by Lemma 3.2. Hence $|x^j z|_K + |x^j zw|_K = |x^j z|_N$ has the same parity for all $j$. Thus case (i) of Lemma 6.1 holds. Therefore,

$$\left.\begin{aligned} |x^l z|_K - |x^l zw|_K &= f \\ |x^l z|_K + |x^l zw|_K &= p-1 \end{aligned}\right\}, \qquad l=0, ..., p-1.$$

So $|x^l z|_K = \frac{1}{2}(p-1+f)$, $l=0, ..., p-1$.

By the normalization in Eq. (6.2)

$$\frac{p(p-1)}{2}=\sum_{l=0}^{p-1}|x^l z|_K=\frac{p(p-1+f)}{2}.$$

Hence, $f=0$ and

$$|x^l z|_K=|x^l z w|_K=\frac{p-1}{2}, \qquad l=0, \ldots, p-1.$$

Next by Eq. (6.1) we can apply Lemma 3.3 to $c=\sum_{l=0}^{p-1}(|x^l|_K-|x^l w|_K)\eta^l$ and then apply Lemma 3.2 to $c-\zeta p\eta^j$, where $\zeta=\pm 1$. Then

$$|x^l|_K-|x^l w|_K=|x^j|_K-|x^j w|_K-\zeta p \qquad \text{for} \quad l\neq j.$$

So for $l\neq j$, $|x^l|_K+|x^l w|_K=|x^l|_N$ has the same parity. Hence $j$ is as in Lemma 6.1. Therefore for $l\neq j$

$$\left.\begin{aligned}|x^l|_K-|x^l w|_K&=|x^j|_K-|x^j w|_K-\zeta p\\ |x^l|_K+|x^l w|_K&=p-\varepsilon\end{aligned}\right\}, \qquad \varepsilon \text{ as in Lemma 6.1.}$$

Thus $|x^l|_K=\frac{1}{2}(|x^j|_K-|x^j w|_K-\zeta p+p-\varepsilon)$ for $l\neq j$. By Eq. (6.2)

$$\frac{p(p+1}{2}=\sum_{l=0}^{p-1}|x^l|_K=\frac{p-1}{2}(|x^j|_K-|x^j w|_K-\zeta p+p-\varepsilon)+|x^j|_K.$$

So $p(p+1)=(p+1)|x^j|_K-(p-1)|x^j w|_K-\zeta p(p-1)+p(p-1)-\varepsilon(p-1)$. By Lemma 6.1, $(p-1)(p+\varepsilon(p-1))=(p-1)|x^j|_K+(p-1)|x^j w|_K=(p-1)|x^j|_L$. Hence, $p(p+1)+p(p-1)+\varepsilon(p-1)^2=2p|x^j|_K-\zeta p(p-1)+p(p-1)-\varepsilon(p-1)$. So we find that

$$\begin{aligned}|x^j|_K&=\tfrac{1}{2}[p+1+(p-1)(\varepsilon+\zeta)]\\ |x^j w|_K&=\tfrac{1}{2}[p-1+(p-1)(\varepsilon-\zeta)]\\ |x^l|_K&=\tfrac{1}{2}[p+1-\varepsilon-\zeta]\\ |x^l w|_K&=\tfrac{1}{2}[p-1-\varepsilon+\zeta] \qquad \text{for} \quad l\neq l.\end{aligned}$$

Now note that we have $0\leqslant|g|_K\leqslant p$ for all $g\in G$. When $\varepsilon=\zeta=1$, $|x^j|_K=(3p-1)/2$ which implies $p\leqslant 1$. When $\varepsilon=1=-\zeta$, $|x_j w|_K=(3p-3)/2$ which implies $p\leqslant 3$. Wheb $\varepsilon=-1$ and $\zeta=1$, $|x^j w|_K=(1-p)/2$

which implies $p \leqslant 1$. Finally, $\varepsilon = \zeta = -1$ implies $|x^j|_K = (3-p)/2$ which implies $p \leqslant 3$.

*Case* $c = 0$. When $c = 0$, $d\bar{d} = p^2$. Calculations like those above yield

$$|x^l|_K = \frac{p+1}{2}, \qquad l = 0, \ldots, p-1,$$

$$|x^l w|_K = \frac{p-1}{2}, \qquad l = 0, \ldots, p-1,$$

$$|x^j z|_K = \frac{p-1}{2}(1+\varepsilon+\zeta), \qquad j \text{ as in Lemma 6.1},$$

$$|x^j zw|_K = \frac{p-1}{2}(1+\varepsilon-\zeta), \qquad j \text{ as above},$$

$$|x^l z|_K = \tfrac{1}{2}(p-1-\varepsilon-\zeta) \qquad \text{for} \quad l \neq j,$$

$$|x^l zw|_K = \tfrac{1}{2}(p-1-\varepsilon+\zeta) \qquad \text{for} \quad l \neq j.$$

When $\varepsilon = \zeta = 1$, $|x^j z|_K = (3p-3)/2$, which implies $p \leqslant 3$. When $\varepsilon = -\zeta = 1$, one finds that $|x^j zw|_K = (3p-3)/2$ which leads to $p \leqslant 3$. When $\varepsilon = -1$ and $\zeta = 1$, $|x^j zw|_K = (1-p)/2$, leading to $p \leqslant 1$. Lastly, when $\varepsilon = \zeta = -1$, $|xjkz|_K = (1-p)/2$, yielding $p \leqslant 1$.

In each case, $p \leqslant 3$. ∎

LEMMA 6.3. *If $G$ has a normal subgroup $K$ so that $G/K \cong D_{2p^2}$ and $|K| = 2$, then $G$ possesses no Menon-type difference set.*

*Proof.* Let $\psi$ be a linear representation for $H$. Set $\psi(x) = \xi$, where $\xi$ is a primitive complex $p^2$ th root of unity. Let $\varphi$ be the representation induced from $\psi$ with kernel $K$. All other faithful irreducible representations of $G/K$ of degree two are conjugate to $\varphi$.

*Case* $c = 0$. If $c = \sum_{l=0}^{p^2-1} |x^l|_K \xi^l = 0$, then $d\bar{d} = |d|^2 = p^2$ by Eq. (6.1). Hence, $|d| = p$. Hence, by Lemma 3.3, $d = \varepsilon p \xi^m$ for some $m$, $\varepsilon = \pm 1$. Apply Lemma 3.2(b) to $d - \varepsilon p \xi^m$. Then $|x^{p^2-1-i}z|_K = |x^{p^2-1-i-jp}z|_K$, when $p^2 - 1 - i$ and $m$ are not congruent modulo $p$, and $i, j \in \{0, \ldots, p-1\}$. Also, when $k \equiv m \pmod{p}$ but $k \neq m$, $|x^k z|_K = |x^m z|_K - \varepsilon p$. This is impossible, since $0 \leqslant |g|_K \leqslant 2$ for all $g \in G$.

*Case* $d = 0$. A similar contradiction is reached if $d = 0$. ∎

## VII. End of the Proof

We can now state the major results of this paper.

THEOREM 7.1. *Let $p>3$ be prime. Let $G$ be a multiplicative group of order $4p^2$ having a $(4p^2, 2p^2-p, p^2-p)$-difference set $D$. Then a Sylow 2-subgroup of $G$ is cyclic.*

*Proof.* If a Sylow 2-subgroup of $G$ is elementary abelian, then $G$ has an homomorphic image either $D_{4p}$ or $C_p \times C_2 \times C_2$.

Lemma 6.2 shows that there is no difference set if $p>3$ and $G$ has as homomorphic image $D_{4p}$.

If $G$ has $C_p \times C_2 \times C_2$ as homomorphic image, then by Lemma 5.6 there are 16 types of possibilities for the distribution of $D$ among cosets of the factor group. However, when $\zeta=\varepsilon_1=\varepsilon_2=\varepsilon_3=1$, $|x^k|_K=(3p-1)/2$ which means that $p\leqslant 1$. When exactly one of $\zeta$ and the $\varepsilon_i$ is $-1$, $|x^l|_K=p/2$ which implies that $p$ is even, i.e., $p=2$. This occurs four times. For the opposite cases when exactly one of $\zeta$ and the $\varepsilon_i$ is 1, we find $|x^l|_K=(p+2)/2$ which again only works when $p$ is even. This also occurs four times. When $\zeta=1$ and 2 of the $\varepsilon_i$'s are $-1$, one of $|x^kw|_K$, $|x^kz|_K$, or $|x^kzw|_K$, or $|x^kzw|_K$ is $(3p-3)/2$. This happens three times and we must have $p\leqslant 3$. In the opposite cases in which $\zeta=-1$ and exactly two of the $\varepsilon_i$'s are 1, one finds that one of $|x^kw|_K$, $|x^kz|_K$, or $|x^kzw|_K$ is $(1-p)/2$. In these cases, $p\leqslant 1$. The final case has $\zeta=\varepsilon_1=\varepsilon_2=\varepsilon_3=-1$. One finds that $|x^k|_K=(3-p)/2$ in this case, implying $p\leqslant 3$.

We have accounted for $1+4+4+3+3+1=16$ cases. All cases show $p\leqslant 3$. ∎

Kibler's paper shows that this bound is sharp.

THEOREM 7.2. *Let $p$ be an odd prime. Let $G$ be a multiplicative group of order $4p^2$ having a $(4p^2, 2p^2-p, p^2-p)$-difference set $D$. If a Sylow $p$-subgroup of $G$ is cyclic, then $p\equiv 1 \pmod 4$ and $G\cong G_4$.*

*Proof.* If $G$ is not isomorphic to $G_4$, then $G$ has as homomorphic image either $D_{2p^2}$ or $C_{p^2}$. Lemmas 5.7 and 6.3 show this cannot happen for an odd prime. ∎

McFarland [10] shows that a group $G\cong G_6$ has a Menon-type difference set only when $p=2$ or 3. Liebler [6] proves that for $G\cong G_{12}$, $G$ has a Menon-type difference set if and only if $p=3$. Hence, we need only prove part (ii) of Theorem 1.1.

For the remainder $p$ is an odd prime and $G$ is a multiplicative group of order $4p^2$ with elementary abelian, normal Sylow $p$-subgroup $H$ generated

by $x$ and $y$. In addition, $z$ generates a cyclic Sylow 2-subgroup of $G$. $D$ remains as a putative $(4p^2, 2p^2-p, p^2-p)$-difference set in $G$.

Let $K$ be the kernel of a linear representation $\varphi$ for $G$ so that $C_p \times C_4 \cong G/K = \langle Kx \rangle \times \langle Kz \rangle$. For $g \in G$ set $|g|_K := |Kg \cap D|$. Let $\eta$ be a primitive $p$th root of unity. Define $\chi$ as in Lemma 5.4 and define $\psi(x) = 1$, $\psi(z) = i$. The irreducible representations of $G/K$ have the form $\chi^l \otimes \psi^m$, when $l = 0, ..., p-1$ and $m = 0, 1, 2, 3$. Thus $G/K$ has as character table $C = C_1 \otimes C_2$, where $C_1$ is as in Lemma 5.4 and $C_2$ is as in Lemma 5.3. The rows of $C$ are labeled by the $\chi^l \otimes \psi^m$'s. The columns are labeled by $Kx^l z^m$'s. The representation $\varphi$ may be taken as $\chi \otimes \psi$. All other faithful linear representations of $G/K$ are conjugate to $\varphi$.

Set $c = \sum_{l=0}^{p-1} (|x^l|_K - |x^l z^2|_K)\eta^l$ and $d = \sum_{l=0}^{p-1} (|x^l z|_K - |x^l z^3|_K)\eta^l$. We have that $\varphi(D) = c + id$. By Eq. (2.2), $\varphi(D)$ is an algebraic integer in $\mathscr{Z}[i\eta]$ of length $p$. Hence $\varphi(D)$ is one of the algebraic integers listed in Lemma 3.4.

LEMMA 7.3. *If $\varphi(D) = i^e \eta^j p$, then $p \leqslant 3$.*

*Proof.* Replace $D$ by $Dx^l$, some $l$, if necessary so that $j = 0$. Comparing real and imaginary parts, one of $c$ or $d$ is 0. The other is then $\pm p$. Set $H := K \cup Kz^2$, and $L = \langle Kx \rangle$.

*Case $d = 0$.* If $d = 0$, by Lemma 3.2, $|x^l z|_K - |x^l z^3|_K$ is constant for all $l$. Hence $|x^l z|_K + |x^l z^3|_K = |x^l z|_H$ has the same parity for all $l$ and is, therefore, constant. Thus $|x^l z|_K$ is constant for all $l$. Hence $|z|_L = \sum_{l=0}^{p-1} |x^l z|_K \equiv 0 \pmod{p}$. Hence $\psi(D) = i^e p$ and the first case of Lemma 5.3 holds.

Thus for the vector $\mathbf{b}$ whose entries are indexed by the $\chi^l \otimes \psi^m$'s we have

$$b_{l,m} = \begin{cases} k = 2p^2 - p, & \text{if } l = m = 0 \\ i^m \eta^{jl} p, & \text{otherwise.} \end{cases}$$

By Theorem 2.1 we find that

$$|x^l z|_K = |x^l z^3|_K = \frac{p-1}{2}, \qquad l = 0, ..., p-1,$$

$$|x^j|_K = \tfrac{1}{2}[p + 1 + (\varepsilon + \zeta)(p-1)], \qquad j \text{ as in Lemma 5.4,}$$

$$|x^j z^2|_K = \frac{p-1}{2}(1 - \varepsilon + \zeta), \qquad j \text{ as above,}$$

$$|x^l|_K = \tfrac{1}{2}(p + 1 - \varepsilon - \zeta), \qquad \text{for } l \neq j,$$

$$|x^l z^2|_K = \tfrac{1}{2}(p - 1 + \varepsilon - \zeta), \qquad \text{for } l \neq j,$$

where $\varepsilon, \zeta = \pm 1$. However, when $\varepsilon = \zeta = 1$, $|x^j|_K = (3p-1)/2$ which implies that $p \leqslant 1$. When $\zeta = 1 = -\varepsilon$, $|x^j z^2|_K = (3p-3)/2$ which implies $p \leqslant 3$. In case $\zeta = -1 = -\varepsilon$, $|x^j z^2|_K = (1-p)/2$ which is impossible. Lastly, when $\zeta = \varepsilon = -1$, $|x^j|_K = (3-p)/2$ which implies that $p \leqslant 3$.

*Case* $c = 0$. Similar computations in this case yield

$$|x^l|_K = \frac{p+1}{2}, \qquad l = 0, \ldots, p-1,$$

$$|x^l z^2|_K = \frac{p-1}{2}, \qquad l = 0, \ldots, p-1,$$

$$|x^j z|_K = \tfrac{1}{2}[(p-1)(1-\zeta+eps)], \qquad j \text{ as in Lemma 5.4},$$

$$|x^j z^3|_K = \tfrac{1}{2}[(p-1)(1-\varepsilon-\zeta)], \qquad j \text{ as above},$$

$$|x^l z|_K = \tfrac{1}{2}(p-1-\varepsilon+\zeta) \qquad \text{for} \quad l \neq j,$$

$$|x^l z^3|_K = \tfrac{1}{2}(p-1+\varepsilon+\zeta) \qquad \text{for} \quad l \neq j,$$

where $\varepsilon, \zeta = \pm 1$. When $\varepsilon = \zeta = 1$, $|x^j z^3|_K = (1-p)/2$, a contradiction. If $\varepsilon = -1 = -\zeta$, $|x^j z|_K = (1-p)/2$. This is again impossible. In case $\varepsilon = 1 = -\zeta$, $|x^j z|_K = (3p-3)/2$ which implies $p \leqslant 3$. Finally, when $\varepsilon = \zeta = -1$, $|x^j z^3|_K = (3p-3)/2$ which, again, implies $p \leqslant 3$. In any case we have $p \leqslant 3$. ∎

Theorem 1.1 now follows by Lemma 3.4, part a.

## Acknowledgment

The author wishes to express deep gratitude to Robert A. Liebler. This paper represents part of a dissertation written under his guidance.

## References

1. C. W. Curtis and I. Reiner, "Representation Theory of Finite Groups and Associative Algebras," Wiley Interscience, New York, 1988.
2. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," Springer-Verlag, New York, 1990.
3. R. E. Kibler, A summary of noncyclic difference sets, $k < 20$, *J. Combin. Theory Ser. A* **25** (1978), 62–67.
4. E. S. Lander, "Symmetric Designs: An Algebraic Approach," Cambridge Univ. Press, New York, 1983.
5. S. Lang, "Algebra," Addison–Wesley, New York, 1984.
6. R. A. Liebler, The inversion formula, to appear.

7. R. A. LIEBLER AND K. W. SMITH, On difference sets in certain 2-groups, *in* "Coding Theory, Design Theory, Group Theory: Proceedings of the Marchall Hall Conference," edited by D. Jungnickel, Wiley, New York, 1992.
8. H. B. MANN, "Addition Theorems," Wiley, New York, 1965.
9. H. B. MANN AND R. L. MCFARLAND, On Hadamard difference sets, *in* "A Survey of Combinatorial Theory" (J. N. Srivastava *et al.*, Eds.), pp. 333–334, American Elsevier, New York, 1973.
10. R. L. MCFARLAND, Difference sets in abelian groups of order $4p^2$, *Mitt. Math. Sem. Giessen* **192** (1989), 1–70.
11. P. K. MENON, On difference sets whose parameters satisfy a certain relation, *Proc. Amer. Math. Soc.* **13** (1962), 739–745.
12. H. NAGAO AND Y. TSUSHIMA, "Representations of Finite Groups," Academic Press, San Diego, 1991.
13. K. W. SMITH, Non-abelian Hadamard difference sets, *J. Combin. Theory Ser. A* **70** (1995), 144–156.
14. R. J. TURYN, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.
15. H. WEYL, "Algebraic Theory of Numbers," Princeton, Univ. Press, Princeton, NJ, 1940.