J Algebr Comb (2008) 27: 187–203
DOI 10.1007/s10801-007-0084-1

Tightening Turyn's bound for Hadamard difference sets

Omar A. AbuGhneim · Ken W. Smith

Received: 13 June 2005 / Accepted: 8 June 2007 / Published online: 6 July 2007

Abstract This work examines the existence of $(4q^2, 2q^2 - q, q^2 - q)$ difference sets, for $q = p^f$, where p is a prime and f is a positive integer. Suppose that G is a group of order $4q^2$ which has a normal subgroup K of order q such that $G/K \cong C_q \times C_2 \times C_2$, where C_q, C_2 are the cyclic groups of order q and 2 respectively. Under the assumption that p is greater than or equal to 5, this work shows that G does not admit $(4q^2, 2q^2 - q, q^2 - q)$ difference sets.

Keywords Hadamard difference sets · Intersection numbers · Characters

1 Introduction

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

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

One can think of D as an element in the group ring $\mathbb{Z}[G]$. In this case, we write

$$D = \sum_{g \in D} g.$$

O.A. AbuGhneim (✉)
Department of Mathematics, Faculty of Science, Jordan University, Amman 11942, Jordan
e-mail: o.abughneim@ju.edu.jo

K.W. Smith
Department of Mathematics, Central Michigan University, Mount Pleasant, MI 48859, USA
e-mail: Ken.W.Smith@cmich.edu

D is a difference set if D satisfies the equation

$$DD^{(-1)} = (k-\lambda)1_G + \lambda G,$$

and so we use D to represent both a subset of the group G and an element of the group ring $\mathbb{Z}[G]$. Here $D^{(-1)}$ denotes the sum of the inverses of the elements of D and 1_G denotes the identity element of G. For more details on difference sets the reader may consult [2, 8, 10].

Difference sets with parameters $(4N^2, 2N^2-N, N^2-N)$ are known as Menon-Hadamard difference sets. More details on these difference sets can be found in [4] and [6].

This paper investigates Menon-Hadamard difference sets with parameters $(4q^2, 2q^2-q, q^2-q)$, where $q=p^f$, p prime. Turyn provided a nonexistence result for the abelian case. In his work, he showed that abelian groups of order $4p^{2f}$ and exponent greater than $4p^{f+1}$ or $2p^{f+1}$ do not admit $(4q^2, 2q^2-q, q^2-q)$ difference sets for $p>3$; see [14].

The existence of abelian $(4p^2, 2p^2-p, p^2-p)$ difference sets for $p>3$ was ruled out by McFarland; see [12].

After that, $(4p^2, 2p^2-p, p^2-p)$ nonabelian difference sets were studied by Iiams; see [6]. In his work, Iiams showed that any group of order $4p^2$ which has $\mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_2$ as a factor group, does not have $(4p^2, 2p^2-p, p^2-p)$ difference sets for $p>3$.

In a recent work, Wan generalized the work of Iiams by showing that any group of order $4p^4$ which has $\mathbb{Z}_{p^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ as a factor group, does not have $(4p^4, 2p^4-p^2, p^4-p^2)$ difference sets for $p>3$; see [15].

This paper tightens Turyn's exponent bound and generalizes Iiams's and Wan's results, through the following theorem.

Theorem 1 *Suppose that G is a group of order $4q^2$, where $q=p^f$, p is a prime greater than or equal to 5. Furthermore, assume that $K \trianglelefteq G$ with $G/K \cong C_q \times C_2 \times C_2 = G'$, where C_q, C_2 are the cyclic groups of order q and 2 respectively. Then G does not admit a $(4q^2, 2q^2-q, q^2-q)$ difference set.*

For the cases where $p=2$ and $p=3$, $f=1$, we have the parameters $(16, 6, 2)$ and $(36, 15, 6)$. Kibler gave the answer for the existence of difference sets in all groups of order 16 and 36 and constructed these difference sets when they exist; see [9]. Smith constructed a $(100, 45, 20)$ difference set in the nonabelian group $\langle a, b, c : a^5 = b^5 = c^4 = [a,b] = cac^{-1}a^{-2} = cbc^{-1}b^{-2} = 1\rangle$; see [13].

In studying difference sets, a very useful technique is to look at the image of the difference set in a factor group of G. To see this, let U be a normal subgroup of G with $G' = G/U$. The contraction of D with respect to U is the multiset $D' = D/U = \{dU : d \in D\}$, which satisfies the equation $D'D'^{(-1)} = (k-\lambda) + \lambda|U|G'$ in the group ring $\mathbb{Z}[G']$. Here $D' = \sum_{g' \in G'} |t_{g'}|_U g'$ in $\mathbb{Z}[G']$, where $|t_{g'}|_U = |g'U \cap D|$ is the number of elements of D in the coset $g'U$. The number $|t_{g'}|_U$ is called the intersection number of g' relative to U. The idea of contraction gives more information, indeed restrictions, on the equations which determine the difference sets in the factor group.

2 Character theory and algebraic number theory

We use character theory and algebraic number theory to gain information about the contractions of a difference set D. For information on character theory see [3] and [11]. More information on algebraic number theory can be found in [7] and [16].

A character of an abelian group is a homomorphism from the group to the multiplicative group of the complex roots of unity. Extending this homomorphism to the entire group ring yields a map from the group ring to the complex numbers. We will denote characters by the Greek letter χ. The all-one character (that is $\chi(g)=1$, $\forall g\in G$) is called the principal character whereas the rest are called nonprincipal characters.

Lemma 1 *Let G be a group of order v which has U as a normal subgroup of order q such that $G'=G/U$ is abelian. Take an element $D'\in\mathbb{Z}[G']$. Then D' satisfies the equation $D'D'^{(-1)}=(k-\lambda)+\lambda|U|G'$ if and only if for all character χ of G' we have*

$$|\chi(D')|=\begin{cases} k & \text{if } \chi \text{ is the principal character,}\\ \sqrt{k-\lambda} & \text{otherwise.}\end{cases}$$

In our case, G is a group of order $4q^2$ which has a normal subgroup K of order q with $G'=G/K\cong C_q\times C_2\times C_2$. If D is a $(4q^2,2q^2-q,q^2-q)$ difference set in G, then the contraction of D with respect to K is the multiset $A=D/K=\{dK:d\in D\}$. In the group ring notation $A=\sum_{g'\in G'}|g'|_K g'$, where $|g'|_K=|g'K\cap D|$ are the intersection numbers. The multiset A satisfies the equation $AA^{(-1)}=q^2+(q^2-q)|K|G'$. Hence Lemma 1 gives

$$|\chi(A)|=\begin{cases} 2q^2-q & \text{if } \chi \text{ is the principal character of } G',\\ q & \text{if } \chi \text{ is any other character of } G'.\end{cases}$$

Eventually we will show that such an A does not exist. From now on, G' will be $G/K\cong C_q\times C_2\times C_2$ and A an element of $\mathbb{Z}[G']$ which satisfies $AA^{(-1)}=q^2+(q^2-q)|K|G'$.

Write G' in the multiplicative notation; then $G'\cong\langle x,y,z:x^q=y^2=z^2=1,[x,y]=[x,z]=[y,z]=1\rangle$. If ξ is a primitive complex p^fth root of unity then the characters for this group are

$$\chi_{abc}(x^iy^jz^k)=\xi^{ia}(-1)^{jb}(-1)^{kc},$$

where $a\in\{0,1,\dots,p^f-1\}$ and $b,c\in\{0,1\}$.

Consider the group ring $\mathbb{Q}[\xi][G']$, where $\mathbb{Q}[\xi]$ is the cyclotomic field extension of $\mathbb{Q}$. Extending the characters to the entire group ring yields a map from the group ring to the field $\mathbb{Q}[\xi]$. In this case $\chi(\sum_{g\in G'}a_g g)=\sum_{g\in G'}a_g\chi(g)$, where the coefficients a_g's are elements from $Q[\xi]$.

The group ring $\mathbb{Q}[\xi][G']$ is a vector space with underlying field $\mathbb{Q}[\xi]$. The elements of the group G' are a basis for this vector space. This basis is often called the "standard basis".

We introduce a new basis for $\mathbb{Q}[\xi][G']$. Let C be the character table for G'. The rows of C are labelled by the characters in the following order $[\chi_{000}, \chi_{100}, \dots, \chi_{(q-1)00}, \chi_{010}, \chi_{110}, \dots, \chi_{(q-1)10}, \chi_{001}, \chi_{101}, \dots, \chi_{(q-1)01}, \chi_{011}, \chi_{111}, \dots, \chi_{(q-1)11}]$. Indeed the order here is lexicographic order (reading from right to left) with respect to the indices of the characters.

The columns of C are labelled by the elements of G' in the following order $[x^0y^0z^0, x^1y^0z^0, \dots, x^{(q-1)}y^0z^0, x^0y^1z^0, x^1y^1z^0, \dots, x^{(q-1)}y^1z^0, x^0y^0z^1, x^1y^0z^1, \dots, x^{(q-1)}y^0z^1, x^0y^1z^1, x^1y^1z^1, \dots, x^{(q-1)}y^1z^1]$. This ordered set, call it β_1, is an ordered basis for $\mathbb{Q}[\xi][G']$ over $\mathbb{Q}[\xi]$. The elements of β_1 are ordered lexicographically (reading from right to left) but with respect to the super indices.

This labelling for the columns and rows determines the matrix of the character table. Denote this matrix by U.

Define a new set of elements of the vector space as follows, $\beta_2 = \{\varphi_{abc}\}$, where $a \in \{0, 1, \dots, p^f - 1\}$ and $b, c \in \{0, 1\}$ and

$$\varphi_{abc} = \frac{1}{4q}\sum_{k=0}^{1}\sum_{j=0}^{1}\sum_{i=0}^{p^f-1}\overline{\chi_{abc}(x^iy^jz^k)}x^iy^jz^k.$$

The set β_2 has $4q$ elements. Next, we show that β_2 forms a basis for the vector space $\mathbb{Q}[\xi][G']$. This basis is often called the basis of “primitive idempotents”.

We need the following lemma from character theory. The proof of this lemma can be found in [11].

Lemma 2 (Orthogonality relations of characters) *Suppose that G is an abelian group. $G^\star$ denote the group of characters of G. Then*

(1) *If χ and χ' are two characters of G, then $\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi'(g)} = \delta_{\chi\chi'}$.*
(2) *If g and g' are two elements of G, then $\frac{1}{|G|}\sum_{\chi\in G^\star}\chi(g)\overline{\chi(g')} = \delta_{gg'}$.*

Statement (1) means that the rows of the character table are orthogonal and the square norm of each one of them equal to $|G|$. Statement (2) means the same thing for the columns of the character table. Hence one can conclude that, if U is the matrix of the character table then $U\overline{U^t} = |G|I$, where the bar for the conjugation and t for transpose and I is the identity matrix. Hence U is an invertible matrix. Using the character table one can show the following result.

Lemma 3 *β_2 is also a basis for the vector space $\mathbb{Q}[\xi][G']$.*

One can think of A as an element of $\mathbb{Q}[\xi][G']$. In this case A can be written as a linear combination of elements of β_2, say $A = \sum_{\varphi\in\beta_2} d_\varphi\varphi$, where $d_\varphi \in \mathbb{Q}[\xi]$. Let $\chi_{a'b'c'}$ be a character for G'. Apply $\chi_{a'b'c'}$ to A to get

$$\begin{aligned}\chi_{a'b'c'}(A) &= \sum_{\varphi\in\beta_2} d_\varphi\chi_{a'b'c'}(\varphi)\\ &= \sum_{a,b,c}\sum_{i,j,k}\frac{1}{4q}d_{\varphi_{abc}}\overline{\chi_{abc}(x^iy^jz^k)}\chi_{a'b'c'}(x^iy^jz^k)\end{aligned}$$

$$= \sum_{a,b,c} d_{\varphi_{abc}} \delta_{aa'} \delta_{bb'} \delta_{cc'}$$

$$= d_{\varphi_{a'b'c'}}.$$

The third equality follows from Lemma 2. The next lemma will find a specific value for $\chi_{a'b'c'}(A)$.

Lemma 4 (Iiams [6]) *Let ξ be a primitive p^fth root of unity. If α is an algebraic integer in $\mathbb{Z}[\xi]$ all of whose conjugates have modulus p^f, then $\alpha = \pm p^f \xi^l$, for some integer l.*

3 Simplifying A

Since $A = \sum_{g' \in G'} |g'|_K g'$, $\chi_{abc}(A)$ is an algebraic integer. By Lemma 1, $\chi_{abc}(A)$ satisfies $|\chi_{abc}(A)| = p^f$ for any nontrivial character χ_{abc}. Hence $\chi_{abc}(A)$ is an algebraic integer in $\mathbb{Z}[\xi]$, all of whose conjugates have modulus p^f. Lemma 4 gives $\chi_{abc}(A) = \pm p^f \xi^l$, for some integer l. The proof of the following lemma can be found in [6].

Lemma 5 (a) *Let $a_0, \dots, a_{p-1} \in \mathbb{Q}$ and η be a primitive pth root of unity. Then $\sum_{i=0}^{p-1} a_i \eta^i = 0$ if and only if $a_0 = \cdots = a_{p-1}$.*

(b) *Let $a_0, \dots, a_{p^f-1} \in \mathbb{Q}$ and ξ be a primitive p^fth root of unity. Then $\sum_{i=0}^{p^f-1} a_i \xi^i = 0$ if and only if $a_i = a_j$ when $i \equiv j \pmod{p^{f-1}}$.*

But as an element of $\mathbb{Z}[G']$, A has the form $A = \sum_{i,j,k} |x^i y^j z^k|_K x^i y^j z^k$ (recall that $|x^i y^j z^k|_K = |x^i y^j z^k K \cap D|$). Therefore, for $a \in \{1, 2, \dots, p^f - 1\}$, we have

$$\chi_{a00}(A) = \sum_{i=0}^{p^f-1} (|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K) \xi^{ia} = \pm p^f \xi^{l_{a00}},$$

and

$$\chi_{a10}(A) = \sum_{i=0}^{p^f-1} (|x^i|_K - |x^i y|_K + |x^i z|_K - |x^i yz|_K) \xi^{ia} = \pm p^f \xi^{l_{a10}},$$

and

$$\chi_{a01}(A) = \sum_{i=0}^{p^f-1} (|x^i|_K + |x^i y|_K - |x^i z|_K - |x^i yz|_K) \xi^{ia} = \pm p^f \xi^{l_{a01}},$$

and

$$\chi_{a11}(A) = \sum_{i=0}^{p^f-1} (|x^i|_K - |x^i y|_K - |x^i z|_K + |x^i yz|_K) \xi^{ia} = \pm p^f \xi^{l_{a11}}.$$

Here $l_{a00}, l_{a10}, l_{a01}$ and l_{a11} are all integers. The next lemma ensures that l_{a00}, l_{a10}, l_{a01} and l_{a11} are equal.

Lemma 6 *For a fixed* $a \in \{1, \ldots, p^{f-1}\}$, $l_{a00} = l_{a10} = l_{a01} = l_{a11}$.

Proof We have two cases to consider.

Case 1: If $(a, p) = 1$ then ξ^a is a primitive p^fth root of unity. Because ξ^a is a primitive p^fth root of unity, $\{\xi^{ia}\}_{i=0}^{i=p^f-1}$ will generate all powers of ξ. Hence $\xi^{l_{a00}}$ will appear in $\chi_{a00}(A)$ and one can combine $\pm p^f \xi^{l_{a00}}$ with $\chi_{a00}(A)$. Thus we can apply Lemma 5 to $\chi_{a00}(A) - \pm p^f \xi^{l_{a00}} = 0$ and in the same way we can apply it to $\chi_{a10}(A) - \pm p^f \xi^{l_{a10}}$, $\chi_{a01}(A) - \pm p^f \xi^{l_{a01}}$, and $\chi_{a11}(A) - \pm p^f \xi^{l_{a11}}$.
Applying Lemma 5 to $\chi_{a00}(A) - \pm p^f \xi^{l_{a00}}$ gives, for $i \equiv l_{a00} \pmod{p^{f-1}}$ and $i \neq l_{a00}$,

$$\begin{aligned} &|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K \\ &\quad = |x^{l_{a00}}|_K + |x^{l_{a00}} y|_K + |x^{l_{a00}} z|_K + |x^{l_{a00}} yz|_K - \pm p^f, \end{aligned} \tag{1}$$

and for $i \not\equiv l_{a00} \pmod{p^{f-1}}$, if $i \equiv i' \pmod{p^{f-1}}$, then

$$|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K = |x^{i'}|_K + |x^{i'} y|_K + |x^{i'} z|_K + |x^{i'} yz|_K. \tag{2}$$

Again, we apply Lemma 5 to $\chi_{a10}(A) - \pm p^f \xi^{l_{a10}}$. We obtain, for $j \equiv l_{a10} \pmod{p^{f-1}}$ and $j \neq l_{a10}$,

$$\begin{aligned} &|x^j|_K - |x^j y|_K + |x^j z|_K - |x^j yz|_K \\ &\quad = |x^{l_{a10}}|_K - |x^{l_{a10}} y|_K + |x^{l_{a10}} z|_K - |x^{l_{a10}} yz|_K - \pm p^f. \end{aligned} \tag{3}$$

And for $j \not\equiv l_{a10} \pmod{p^{f-1}}$, if $j \equiv j' \pmod{p^{f-1}}$, then

$$|x^j|_K - |x^j y|_K + |x^j z|_K - |x^j yz|_K = |x^{j'}|_K - |x^{j'} y|_K + |x^{j'} z|_K - |x^{j'} yz|_K. \tag{4}$$

If $l_{a00} \not\equiv l_{a10}$ then (1) and (4) give, for any i with $i \equiv l_{a00} \not\equiv l_{a10}$,

$$\begin{aligned} &|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K \\ &\quad = |x^{l_{a00}}|_K + |x^{l_{a00}} y|_K + |x^{l_{a00}} z|_K + |x^{l_{a00}} yz|_K - \pm p^f, \end{aligned} \tag{5}$$

and

$$\begin{aligned} &|x^i|_K - |x^i y|_K + |x^i z|_K - |x^i yz|_K \\ &\quad = |x^{l_{a00}}|_K - |x^{l_{a00}} y|_K + |x^{l_{a00}} z|_K - |x^{l_{a00}} yz|_K. \end{aligned} \tag{6}$$

But $|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K$ and $|x^i|_K - |x^i y|_K + |x^i z|_K - |x^i yz|_K$ have the same parity. Also $|x^{l_{a00}}|_K + |x^{l_{a00}} y|_K + |x^{l_{a00}} z|_K + |x^{l_{a00}} yz|_K$ and $|x^{l_{a00}}|_K - |x^{l_{a00}} y|_K + |x^{l_{a00}} z|_K - |x^{l_{a00}} yz|_K$ have the same parity. This is inconsistent with (5) and (6).

Therefore, $l_{a00} \equiv l_{a10} \pmod{p^{f-1}}$.

Now assume that $l_{a00} \equiv l_{a10} \pmod{p^{f-1}}$ and $l_{a00} \neq l_{a10}$. Choose an integer i_0 with $i_0 \equiv l_{a00} \equiv l_{a10}$, $i_0 \neq l_{a00}$ and $i_0 \neq l_{a10}$, then apply (1) and (3) to get

$$\begin{aligned}&|x^{i_0}|_K + |x^{i_0}y|_K + |x^{i_0}z|_K + |x^{i_0}yz|_K \\ &\quad = |x^{l_{a00}}|_K + |x^{l_{a00}}y|_K + |x^{l_{a00}}z|_K + |x^{l_{a00}}yz|_K - \pm p^f\end{aligned} \tag{7}$$

and

$$\begin{aligned}&|x^{i_0}|_K - |x^{i_0}y|_K + |x^{i_0}z|_K - |x^{i_0}yz|_K \\ &\quad = |x^{l_{a10}}|_K - |x^{l_{a10}}y|_K + |x^{l_{a10}}z|_K - |x^{l_{a10}}yz|_K - \pm p^f.\end{aligned} \tag{8}$$

Since $|x^{i_0}|_K + |x^{i_0}y|_K + |x^{i_0}z|_K + |x^{i_0}yz|_K$ and $|x^{i_0}|_K - |x^{i_0}y|_K + |x^{i_0}z|_K - |x^{i_0}yz|_K$ have the same parity, (7) and (8) ensure that $|x^{l_{a00}}|_K + |x^{l_{a00}}y|_K + |x^{l_{a00}}z|_K + |x^{l_{a00}}yz|_K$ and $|x^{l_{a10}}|_K - |x^{l_{a10}}y|_K + |x^{l_{a10}}z|_K - |x^{l_{a10}}yz|_K$ have the same parity. Hence $|x^{l_{a00}}|_K + |x^{l_{a00}}y|_K + |x^{l_{a00}}z|_K + |x^{l_{a00}}yz|_K$ and $|x^{l_{a10}}|_K + |x^{l_{a10}}y|_K + |x^{l_{a10}}z|_K + |x^{l_{a10}}yz|_K$ have the same parity.

But using (1) gives

$$\begin{aligned}&|x^{l_{a10}}|_K + |x^{l_{a10}}y|_K + |x^{l_{a10}}z|_K + |x^{l_{a10}}yz|_K \\ &\quad = |x^{l_{a00}}|_K + |x^{l_{a00}}y|_K + |x^{l_{a00}}z|_K + |x^{l_{a00}}yz|_K - \pm p^f.\end{aligned} \tag{9}$$

So (9) ensures that $|x^{l_{a00}}|_K + |x^{l_{a00}}y|_K + |x^{l_{a00}}z|_K + |x^{l_{a00}}yz|_K$ and $|x^{l_{a10}}|_K + |x^{l_{a10}}y|_K + |x^{l_{a10}}z|_K + |x^{l_{a10}}yz|_K$ have distinct parities.

Thus, one time we show that these two numbers have the same parity and another time they do not. This is a contradiction. Therefore, $l_{a00} = l_{a10}$. In the same way one can show that $l_{a00} = l_{a10}$ and $l_{a00} = l_{a11}$.

Case 2: If $(a, p) = p$ then we write $a = p^k b$ where $(b, p) = 1$, $1 \leq k \leq n - 1$. We have ξ^{p^k} is a primitive p^{f-k}th root of unity and we name it ζ. So we have $\xi^a = \xi^{p^k b} = \zeta^b$ is a primitive p^{f-k}th root of unity. Hence

$$\begin{aligned}\chi_{a00}(A) = &\sum_{i=0}^{p^{f-k}-1} (|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K)\zeta^{ib} \\ &+ \sum_{i=p^{f-k}}^{2p^{f-k}-1} (|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K)\zeta^{ib} \\ &+ \sum_{i=2p^{f-k}}^{3p^{f-k}-1} (|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K)\zeta^{ib} \\ &+ \sum_{i=p^f-p^{f-k}}^{p^f-1} (|x^i|_K + |x^i y|_K + |x^i z|_K + |x^i yz|_K)\zeta^{ib} \\ = &\sum_{i=0}^{p^{f-k}-1} (B_{i1} + B_{i2} + B_{i3} + B_{i4})\zeta^{ib},\end{aligned}$$

where

$$B_{i1}=\sum_{t=0}^{p^k-1}|x^{i+tp^{f-k}}|_K,\qquad B_{i2}=\sum_{t=0}^{p^k-1}|x^{i+tp^{f-k}}y|_K,\qquad B_{i3}=\sum_{t=0}^{p^k-1}|x^{i+tp^{f-k}}z|_K,$$

and

$$B_{i4}=\sum_{t=0}^{p^k-1}|x^{i+tp^{f-k}}yz|_K.$$

In the same way we can write $\chi_{a10}(A)$, $\chi_{a10}(A)$, and $\chi_{a11}(A)$. Now, the rest of the proof will be similar to the proof of Case 1. □

Lemma 7 *For a fixed t, $0\le t<f$, there exists a positive integer j_t such that for all a, with $(a,p)=1$, we have $\chi_{ap^t00}(A)=\pm\xi^{ap^t j_t}$.*

Proof $\chi_{p^t00}(A)=\sum_{i=0}^{p^f-1}(|x^i|_K+|x^iy|_K+|x^iz|_K+|x^iyz|_K)\xi^{ip^t}$. But ξ^{p^t} is a p^{f-t}th primitive root of unity. Hence $\chi_{p^t00}(A)\in\mathbb{Z}[\xi^{p^t}]$. Applying Lemma 4 on $\chi_{p^t00}(A)$ gives $\chi_{p^t00}(A)=\pm p^f\xi^{p^tj_t}$ for some integer j_t. Because $(a,p)=1$, the map $\sigma:\xi^{p^t}\to\xi^{p^ta}$ is an element of the Galois group of $\mathbb{Q}[\xi^{p^t}]/\mathbb{Q}$. But σ maps $\chi_{p^t00}(A)$ to $\chi_{ap^t00}(A)$ and so $\chi_{ap^t00}(A)=\pm p^f\xi^{ap^tj_t}$. □

We have $A=\sum_{b=0}^{1}\sum_{c=0}^{1}\sum_{a=0}^{p^f-1}\chi_{abc}(A)\varphi_{abc}$. The goal is to simplify this sum. To do so, divide $\{\varphi_{a00}\}_{a=0}^{a=p^f-1}$ into $f+1$ sets. These sets are

$$\begin{aligned}
B_0&=\{\varphi_{000}\}\\
B_1&=\{\varphi_{a00}:(a,p)=1\}\\
B_2&=\left\{\varphi_{a00}:p|a\quad\text{and}\quad\left(\frac{a}{p},p\right)=1\right\}\\
&\vdots\quad\vdots\quad\vdots\\
B_i&=\left\{\varphi_{a00}:p^{i-1}|a\quad\text{and}\quad\left(\frac{a}{p^{i-1}},p\right)=1\right\}\\
&\vdots\quad\vdots\quad\vdots\\
B_f&=\left\{\varphi_{a00}:p^{f-1}|a\quad\text{and}\quad\left(\frac{a}{p^{f-1}},p\right)=1\right\}
\end{aligned}$$

Observe that $B_i=\{\varphi_{a00}:a\in C_i\}$, where

$$\begin{aligned}
C_0&=\{0\},\\
C_i&=\{sp^{i-1}:0\le s\le p^{f-(i-1)}-1\}\backslash\{sp^i:0\le s\le p^{f-i}-1\},\quad\text{for }1\le i\le f-1
\end{aligned}$$

and

$$C_f = \{sp^{f-1} : 0 \le s \le p-1\} \backslash \{0\}.$$

Define $e_{i00} = \sum_{a \in C_i} \chi_{a00}(A)\varphi_{a00}$. Because $\chi_{000}(A) = 2q^2 - q$,

$$e_{000} = \frac{2q^2 - q}{4q} \sum_{j=0}^{p^f-1} x^j (1+y)(1+z).$$

For e_{i00} where $i \neq 0$, if $a \in C_i$, then $a = p^{i-1}s$ where $(s, p) = 1$. Using Lemma 7 gives $\chi_{a00}(A) = \chi_{p^{i-1}s00}(A) = \pm p^f \xi^{p^{i-1}sj_{i-1}} = \pm p^f \xi^{aj_{i-1}}$, where j_{i-1} is an integer. Hence we get

$$\begin{aligned} e_{i00} &= \sum_{a \in C_i} \chi_{a00}(A)\varphi_{a00} \\ &= \sum_{a \in C_i} \pm p^f \xi^{aj_{i-1}} \varphi_{a00}. \end{aligned}$$

But $\varphi_{a00} = \frac{1}{4p^f} \sum_{j=0}^{p^f-1} \overline{\chi_{a00}(x^j y^0 z^0)} x^j (1+y)(1+z)$ and $\overline{\chi_{a00}(x^j y^0 z^0)} = \xi^{-ja}$. Plug this into the equation for e_{i00} to get

$$\begin{aligned} e_{i00} &= \frac{\pm 1}{4} \sum_{a \in C_i} \sum_{j=0}^{p^f-1} \xi^{aj_{i-1}} \overline{\chi_{a00}(x^j y^0 z^0)} x^j (1+y)(1+z) \\ &= \frac{\pm 1}{4} \sum_{j=0}^{p^f-1} \sum_{a \in C_i} \xi^{aj_{i-1}} \xi^{-ja} x^j (1+y)(1+z) \\ &= \frac{\pm 1}{4} \sum_{j=0}^{p^f-1} \sum_{a \in C_i} \xi^{-a(j-j_{i-1})} x^j (1+y)(1+z). \end{aligned}$$

Change the counter of the sum using the substitution $j' = j - j_{i-1}$ to get

$$\begin{aligned} &= \frac{\pm 1}{4} \sum_{j'=-j_{i-1}}^{p^f-1-j_{i-1}} \sum_{a \in C_i} \xi^{-aj'} x^{(j'+j_{i-1})} (1+y)(1+z) \\ &= \frac{\pm x^{j_{i-1}}}{4} \sum_{j'=-j_{i-1}}^{p^f-1-j_{i-1}} \sum_{a \in C_i} \xi^{-aj'} x^{j'} (1+y)(1+z). \end{aligned}$$

Because x is a generator of the group C_{p^f}, $x^{-t} = x^{p^f-t}$ for any integer t and so $\{x^{j'}\}_{j'=-j_{i-1}}^{j'=p^f-1-j_{i-1}} = \{x^{j'}\}_{j'=0}^{j'=p^f-1}$. Since $\xi^{p^f} = 1$, $(\xi^a)^{-t} = (\xi^a)^{p^f-t}$ for any integer

t and so $\{\xi^{-aj'}\}_{j'=-j_{i-1}}^{j'=p^f-1-j_{i-1}} = \{\xi^{-aj'}\}_{j'=0}^{j'=p^f-1}$. This gives

$$e_{i00} = \frac{\pm x^{j_{i-1}}}{4} \sum_{j=0}^{p^f-1} \sum_{a\in C_i} \xi^{-aj} x^j (1+y)(1+z).$$

The next lemma shows that $e_{i00} \in \mathbb{Q}[G']$ and gives a specific value for it.

Lemma 8 *For* $0 < i \le f$,

$$e_{i00} = \frac{\pm p^{f-i} x^{j_{i-1}}}{4}(1+y)(1+z)\left[\sum_{t=0}^{p^{i-1}-1} (p-1)x^{tp^{f-i+1}} - \sum_{t=0,\, p\nmid t}^{p^i-1} x^{tp^{f-i}}\right].$$

Proof We have

$$e_{i00} = \frac{\pm x^{j_{i-1}}}{4} \sum_{j=0}^{p^f-1} \sum_{a\in C_i} \xi^{-aj} x^j (1+y)(1+z).$$

From the definition of C_i, one gets

$$\begin{aligned} e_{i00} &= \frac{\pm x^{j_{i-1}}}{4}(1+y)(1+z) \sum_{j=0}^{p^f-1} \sum_{a\in C_i} \xi^{-aj} x^j \\ &= \frac{\pm x^{j_{i-1}}}{4}(1+y)(1+z)\left[\sum_{j=0}^{p^f-1} \sum_{s=0}^{p^{f-(i-1)}-1} \xi^{-sjp^{i-1}} x^j - \sum_{j=0}^{p^f-1} \sum_{s=0}^{p^{f-i}-1} \xi^{-sjp^i} x^j\right]. \end{aligned} \tag{10}$$

The sums depend on the values of j. So we partition the set $\{j : 0 \le j \le p^f - 1\}$ into two subsets, namely T_1 and T_2 where

$$T_1 = \{j = tp^{f-(i-1)} : 0 \le t \le p^{i-1} - 1\},$$
$$T_2 = \{j : 0 \le j \le p^f - 1\} \backslash T_1.$$

For $j \in T_1$, we have $\xi^{-sjp^{i-1}} = \xi^{-stp^f} = 1$. This yields

$$\begin{aligned} &\sum_{s=0}^{p^{f-(i-1)}-1} \sum_{j\in T_1} \xi^{-sjp^{i-1}} x^j (1+y)(1+z) \\ &= \sum_{s=0}^{p^{f-(i-1)}-1} \sum_{t=0}^{p^{i-1}-1} x^{tp^{f-(i-1)}} (1+y)(1+z) \\ &= \sum_{t=0}^{p^{i-1}-1} p^{f-i+1} x^{tp^{f-i+1}} (1+y)(1+z). \end{aligned} \tag{11}$$

The last equality is true because the sum does not depend on s.

For a fixed $j \in T_2$, we want to show that

$$\sum_{s=0}^{p^{f-(i-1)}-1} \xi^{-sjp^{i-1}} x^j (1+y)(1+z) = 0. \tag{12}$$

From the definition of T_2, if j is a fixed element of T_2, then $\xi^{-jp^{i-1}} \neq 1$ and $\xi^{-jp^{i-1}}$ will be a p^{f-r}th root of unity, where r is a positive integer that depends on j and $i-1 \leq r \leq f-1$. Hence we get

$$\sum_{s=0}^{p^{f-r}-1} (\xi^{-jp^{i-1}})^s = 0.$$

But

$$\sum_{s=0}^{p^{f-(i-1)}-1} (\xi^{-jp^{i-1}})^s = \sum_{s=0}^{p^{f-r}-1} (\xi^{-jp^{i-1}})^s + \sum_{s=p^{f-r}}^{2p^{f-r}-1} (\xi^{-jp^{i-1}})^s + \cdots + \sum_{s=(p^{r-(i-1)}-1)p^{f-r}}^{p^{f-(i-1)}-1} (\xi^{-jp^{i-1}})^s.$$

Each one of the sums in the right hand side is equal to zero. Hence the sum in the left hand side is zero. This shows the validity of (12). Use (11) and (12) to get

$$\begin{aligned} e_{i00} &= \frac{\pm x^{j_{i-1}}}{4} \sum_{t=0}^{p^{i-1}-1} p^{f-i+1} x^{tp^{f-i+1}} (1+y)(1+z) - \sum_{t=0}^{p^i-1} p^{f-i} x^{tp^{f-i}} (1+y)(1+z) \\ &= \frac{\pm p^{f-i} x^{j_{i-1}}}{4} (1+y)(1+z) \left[\sum_{t=0}^{p^{i-1}-1} p x^{tp^{f-i+1}} - \sum_{t=0}^{p^i-1} x^{tp^{f-i}} \right]. \end{aligned}$$

Partition the set $B = \{t : 0 \leq t \leq p^i - 1\}$ into $B_1 = \{t\colon\ t = ps \text{ and } 0 \leq s \leq p^{i-1} - 1\}$ (B_1 is the set of all elements which are divisible by p) and $B_2 = B \backslash B_1$ (B_2 is the set of all elements which are not divisible by p). Using this partition gives

$$\begin{aligned} \sum_{t=0}^{p^{i-1}-1} p\, x^{tp^{f-i+1}} - \sum_{t=0}^{p^i-1} x^{tp^{f-i}} &= \sum_{t=0}^{p^{i-1}-1} p\, x^{tp^{f-i+1}} - \sum_{s=0}^{p^{i-1}-1} x^{sp^{f-i+1}} - \sum_{t=0,\, p\nmid t}^{p^i-1} x^{tp^{f-i}} \\ &= \sum_{t=0}^{p^{i-1}-1} (p-1) x^{tp^{f-i+1}} - \sum_{t=0,\, p\nmid t}^{p^i-1} x^{tp^{f-i}}. \end{aligned}$$

Hence we get the required result

$$e_{i00}=\frac{\pm p^{f-i}x^{j_{i-1}}}{4}(1+y)(1+z)\left[\sum_{t=0}^{p^{i-1}-1}(p-1)x^{tp^{f-i+1}}-\sum_{t=0,\,p\nmid t}^{p^i-1}x^{tp^{f-i}}\right]. \qquad \square$$

For $A=\sum_{b=0}^{1}\sum_{c=0}^{1}\sum_{a=0}^{p^f-1}\chi_{abc}(A)\varphi_{abc}$, Lemma 8 simplifies these sums when $b=0$ and $c=0$. The next work simplifies these sums when $b\neq 0$ or $c\neq 0$.

We define

$$e_{i10}(A)=\sum_{a\in C_i}\chi_{a10}(A)\varphi_{a10},$$

$$e_{i01}(A)=\sum_{a\in C_i}\chi_{a01}(A)\varphi_{a01},$$

$$e_{i11}(A)=\sum_{a\in C_i}\chi_{a11}(A)\varphi_{a11}.$$

First, we simplify $e_{010}(A)$, $e_{001}(A)$ and $e_{011}(A)$. To do so, we compute the values of $\chi_{010}(A)$, $\chi_{001}(A)$ and $\chi_{011}(A)$. Use Lemma 1 to get $\chi_{010}(A)=\pm p^f$, $\chi_{001}(A)=\pm p^f$, and $\chi_{011}(A)=\pm p^f$. We can translate A by y, z, or yz if necessary to get $\chi_{010}(A)=p^f$, $\chi_{001}(A)=p^f$, and $\chi_{011}(A)=\pm p^f$. Hence replacing A by Ay, Az or Ayz, if necessary, gives

$$\chi_{010}(A)=\sum_{i=0}^{p^f-1}(|x^i|_K-|x^iy|_K+|x^iz|_K-|x^iyz|_K)=p^f$$

and

$$\chi_{001}(A)=\sum_{i=0}^{p^f-1}(|x^i|_K+|x^iy|_K-|x^iz|_K-|x^iyz|_K)=p^f$$

and

$$\chi_{011}(A)=\sum_{i=0}^{p^f-1}(|x^i|_K-|x^iy|_K-|x^iz|_K+|x^iyz|_K)=\pm p^f.$$

We show that $\chi_{011}(A)=p^f$. To this end, take $H=K\times\mathbb{Z}_{p^f}$; then $G/H\cong\mathbb{Z}_2\times\mathbb{Z}_2$. We find the intersection numbers relative to H. We have

$$\begin{aligned}\chi_{010}(A)=p^f&=\sum_{i=0}^{p^f-1}(|x^i|_K-|x^iy|_K+|x^iz|_K-|x^iyz|_K)\\&=|1|_H-|y|_H+|z|_H-|yz|_H.\end{aligned}$$

Similarly, we have

$$|1|_H + |y|_H - |z|_H - |yz|_H = p^f,$$
$$|1|_H - |y|_H - |z|_H + |yz|_H = \pm p^f.$$

Hence, the intersection numbers $|1|_H, |y|_H, |z|_H$ and $|yz|_H$ satisfy the equations

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \begin{bmatrix} |1|_H \\ |y|_H \\ |z|_H \\ |yz|_H \end{bmatrix} = \begin{bmatrix} \chi_{000}(A) \\ \chi_{010}(A) \\ \chi_{001}(A) \\ \chi_{011}(A) \end{bmatrix} = \begin{bmatrix} 2p^{2f} - p^f \\ p^f \\ p^f \\ \pm p^f \end{bmatrix}.$$

Solving the system gives integer solutions if $\chi_{011}(A) = p^f$ and fractional solutions if $\chi_{011}(A) = -p^f$. But the intersection numbers $|1|_H$, $|y|_H$, $|z|_H$, and $|yz|_H$ are integers. Therefore, $\chi_{011}(A) = p^f$.

We combine $e_{000}(A)$, $e_{010}(A)$, $e_{001}(A)$ and $e_{011}(A)$ together and name the sum e_0. So we get

$$\begin{aligned} e_0 &= e_{000}(A) + e_{010}(A) + e_{001}(A) + e_{011}(A) \\ &= \left(\frac{(p^f+1)}{2}1 + \frac{(p^f-1)}{2}y + \frac{(p^f-1)}{2}z + \frac{(p^f-1)}{2}yz\right)\left(\sum_{j=0}^{p^f-1} x^j\right). \quad (13) \end{aligned}$$

For $i \neq 0$, Lemma 6 ensures that if $\chi_{i00}(A)$, $\chi_{i10}(A)$, $\chi_{i01}(A)$ and $\chi_{i11}(A)$ are different, then they differ by a sign. Hence a similar argument, as what we have done for $e_{i00}(A)$, gives

$$e_{i10}(A) = \frac{\pm p^{f-i} x^{j_{i-1}}}{4}(1-y)(1+z)\left[\sum_{t=0}^{p^{i-1}-1} (p-1)x^{tp^{f-i+1}} - \sum_{t=0, p\nmid t}^{p^i-1} x^{tp^{f-i}}\right],$$

$$e_{i01}(A) = \frac{\pm p^{f-i} x^{j_{i-1}}}{4}(1+y)(1-z)\left[\sum_{t=0}^{p^{i-1}-1} (p-1)x^{tp^{f-i+1}} - \sum_{t=0, p\nmid t}^{p^i-1} x^{tp^{f-i}}\right],$$

$$e_{i11}(A) = \frac{\pm p^{f-i} x^{j_{i-1}}}{4}(1-y)(1-z)\left[\sum_{t=0}^{p^{i-1}-1} (p-1)x^{tp^{f-i+1}} - \sum_{t=0, p\nmid t}^{p^i-1} x^{tp^{f-i}}\right].$$

As the case when $i = 0$, one can combine $e_{i00}(A)$, $e_{i10}(A)$, $e_{i01}(A)$ and $e_{i11}(A)$ together. To do that define the vectors $\epsilon_i = \begin{bmatrix} \epsilon_{i1} \\ \epsilon_{i2} \\ \epsilon_{i3} \\ \epsilon_{i4} \end{bmatrix}$ where $\epsilon_{ij} = \pm 1$. We define this vector because the signs of $e_{i00}(A)$, $e_{i10}(A)$, $e_{i01}(A)$ and $e_{i11}(A)$ are not necessarily the same.

For $i \neq 0$, name the sum e_i, so we get

$$\begin{aligned} e_i &= e_{i00}(A) + e_{i10}(A) + e_{i01}(A) + e_{i11}(A) \\ &= \frac{p^{f-i}x^{j_{i-1}}}{4}[1 \quad y \quad z \quad zy] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \begin{bmatrix} \epsilon_{i1} \\ \epsilon_{i2} \\ \epsilon_{i3} \\ \epsilon_{i4} \end{bmatrix} \\ &\quad \times \left[\sum_{t=0}^{p^{i-1}-1} (p-1)x^{tp^{f-i+1}} - \sum_{t=0, p\nmid t}^{p^i-1} x^{tp^{f-i}} \right]. \end{aligned} \tag{14}$$

But,

$$A = \sum_{i=0}^{f} e_i, \tag{15}$$

where the e_i's are known from (13) and (14). One can get all intersection numbers of A by using (15). But these intersection numbers are integers that lie between 0 and p^f. Next, we show that these intersection numbers involve fractions or do not lie between 0 and p^f which gives a contradiction.

4 Main result

Theorem 1 *Suppose that G is a group of order $4q^2$, where $q = p^f$, p is a prime greater than or equal to 5. Furthermore, assume $K \trianglelefteq G$ with $G' = G/K \cong C_q \times C_2 \times C_2 = G'$, where C_q, C_2 are the cyclic groups of order q and 2 respectively. Then G does not have a $(4q^2, 2q^2 - q, q^2 - q)$ difference set.*

Proof There are two cases to consider.

Case 1: The number of ϵ_{1j}'s which are positive is even, where $1 \leq j \leq 4$. In this case we show that one of the intersection numbers do not lie between 0 and p^f.

Equation (14) gives, $e_1 = \frac{p^{f-1}x^{j_0}}{4}[(\epsilon_{11} + \epsilon_{12} + \epsilon_{13} + \epsilon_{14})1 + (\epsilon_{11} - \epsilon_{12} + \epsilon_{13} - \epsilon_{14})y + (\epsilon_{11} + \epsilon_{12} - \epsilon_{13} - \epsilon_{14})z + (\epsilon_{11} - \epsilon_{12} - \epsilon_{13} + \epsilon_{14})yz][(p-1) - x^{p^{f-1}} - x^{2p^{f-1}} - \cdots - x^{(p-1)p^{f-1}}]$. Since the number of positive ϵ_{1j}'s is even, the coefficient of one of the elements x^{j_0}, $x^{j_0}y$, $x^{j_0}z$ or $x^{j_0}yz$ is $\frac{p^{f-1}}{4}(\pm 4)(p-1) = \pm(p^f - p^{f-1})$. Name this element g' and denote the coefficient of g' in e_i by $|g'|_{e_i}$. Any element of G' appears in e_0 and its coefficient is either $\frac{p^f-1}{2}$ or $\frac{p^f+1}{2}$. Hence

$$|g'|_{e_0+e_1} = \pm(p^f - p^{f-1}) + \frac{(p^f \pm 1)}{2}.$$

Our goal is to find an estimate for the intersection number $|g'|_K$. So we need an estimate for $|g'|_{e_i}$ for the rest of the e_i's. From (14), the value of $|g'|_{e_i}$ is a number in the set $\{0, \pm\frac{p^{f-i}}{2}, \pm p^{f-i}, \pm\frac{(p^{f-i+1} - p^{f-i})}{2}, \pm(p^{f-i+1} - p^{f-i})\}$, for $i \neq 0, 1$.

But $(p^{f-i+1} - p^{f-i})$ is the largest coefficient in absolute value. So, if $|g'|_{e_0+e_1} = (p^f - p^{f-1}) + \frac{(p^f \pm 1)}{2}$ then we have

$$\begin{aligned}
|g'|_K &= |g'|_{e_0+e_1} + \sum_{i\neq 0,1} |g'|_{e_i} \\
&\geq (p^f - p^{f-1}) + \frac{(p^f \pm 1)}{2} - \sum_{i\neq 0,1} (p^{f-i+1} - p^{f-i}) \\
&= (p^f - p^{f-1}) + \frac{(p^f \pm 1)}{2} - \sum_{i\neq 0,1} (p-1)p^{f-i} \\
&= (p^f - p^{f-1}) + \frac{(p^f \pm 1)}{2} - \sum_{i=0}^{f-2} (p-1)p^{i} \\
&\geq p^f + \left[\left(\frac{p^f+1}{2}\right) - 2p^{f-1}\right].
\end{aligned}$$

But the function $f(x) = [(\frac{x^f+1}{2}) - 2x^{f-1}]$ is positive, for $x \geq 5$. Hence $[(\frac{p^f+1}{2}) - 2p^{f-1}] > 0$, for $p \geq 5$. This gives $|g'|_K > p^f$, for $p \geq 5$. This contradicts the fact that $|g'|_K$ between 0 and p^f.

If $|g'|_{e_0+e_1} = -(p^f - p^{f-1}) + \frac{(p^f \pm 1)}{2}$, then the same argument shows that $|g'|_K$ is negative. This completes case 1.

Case 2: The number of positive ϵ_{1j}'s is odd, where $1 \leq j \leq 4$. In this case we show that some of the intersection numbers are fractions. To do that we examine the coefficients of the e_i's. For a fixed $i \neq 0$, if the number of positive ϵ_{ij}'s is odd, then

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \begin{bmatrix} \epsilon_{i1} \\ \epsilon_{i2} \\ \epsilon_{i3} \\ \epsilon_{i4} \end{bmatrix} = \begin{bmatrix} \pm 2 \\ \pm 2 \\ \pm 2 \\ \pm 2 \end{bmatrix}.$$

Hence, in e_i we have $p^i - p^{i-1}$ elements that have $\pm\frac{p^{f-i}}{2}$ as a coefficient (which is a fraction) and p^{i-1} elements that have $\pm\frac{p^{f-i+1}-p^{f-i}}{2}$ as a coefficient (which is an integer). Let $i' = \max\{i : 1 \leq i \leq f$ such that the number of positive ϵ_{ij}'s is odd$\}$. Note that the maximum is well-defined, because at least the number of positive ϵ_{1j}'s is odd.

For a fixed integer k with $i' < k \leq f$, the number of ϵ_{kj}'s is even. Hence we have

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \begin{bmatrix} \epsilon_{k1} \\ \epsilon_{k2} \\ \epsilon_{k3} \\ \epsilon_{k4} \end{bmatrix} = \begin{bmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \\ \delta_4 \end{bmatrix},$$

where each one of the δ_j's is either 0 or ± 4. This shows that the coefficients in e_k are integers for $i' < k \leq f$.

The coefficients in e_0 are integers and this is because these coefficients are either $\frac{p^f-1}{2}$ or $\frac{p^f+1}{2}$. For a fixed k, where $1 \leq k < i'$, if the number of ϵ_{kj}'s is odd then the coefficients of the elements of e_k are fractions. From the analysis above we get fractional coefficients in e_k when $k = i'$ and possibly when $1 \leq k < i'$. Now, we estimate the number of elements in A which have fractional coefficients.

The number of elements with fractional coefficient in $e_{i'}$ is $p^{i'} - p^{i'-1}$. But we have at most another $\sum_{k=1}^{i'-1} p^k - p^{k-1} = p^{i'-1} - 1$ elements in the e_k's that have a fractional coefficient, where $1 \leq k < i'$. Since $p^{i'-1} - 1 < p^{i'} - p^{i'-1}$ for $p \geq 5$, when we sum up the e_i's to get A, we will have at least $(p^{i'} - p^{i'-1}) - (p^{i'-1} - 1)$ intersection numbers of A with fractional coefficients. This contradicts the fact that intersection numbers are integers. So this completes the second case. Hence G does not have a $(4q^2, 2q^2 - q, q^2 - q)$ difference set. □

The following result is often called Dillon's dihedral trick.

Lemma 9 (Dillon [5]) *Suppose that G_1 is an abelian group of even order with a subgroup G_2 of index 2. Hence $G_1 = G_2 \cup \theta G_2$ where $\theta \in G_1 \setminus G_2$. Let $\widehat{G_1}$ be the generalized dihedral extension of G_1, i.e. $\widehat{G_1} = \langle G_2, Q : Q^2 = 1, QgQ = g^{-1}\ \forall g \in G_2 \rangle$. Furthermore, let G be a group which has U as a normal subgroup with $G/U \cong \widehat{G_1}$. If $\widehat{D} = X + QY \in \mathbb{Z}[\widehat{G_1}]$, where $X, Y \in \mathbb{Z}[G_2]$, satisfies $\widehat{D}\widehat{D}^{(-1)} = (k - \lambda) + \lambda|U|\widehat{G_1}$, then this forces $D = X + \theta Y \in \mathbb{Z}[G_1]$ to satisfy $DD^{(-1)} = (k - \lambda) + \lambda|U|G_1$.*

Corollary 1 *Suppose that G is a group of order $4q^2$ which have a normal subgroup U so that G/U is isomorphic to $\mathbb{D}_{4q}$ (the dihedral group of order $4q$). Then G does not admit $(4q^2, 2q^2 - q, q^2 - q)$ difference sets.*

Proof Use Theorem 1 and Lemma 9 to get the result. □

If the Sylow 2-subgroup of G' is cyclic (i.e. $G' = G/K \cong C_q \times C_4$) then the possible values of α in Lemma 4 depend on p. For instance, if $p \equiv 1 \pmod 4$ and η is a primitive pth root of unity and α is an algebraic integer in $\mathbb{Z}[i\eta]$ all of whose conjugates have modulus p, then α has four possible values. More details about these four values of α can be found in [6]. AbuGhneim, Becker, Mendes, and Smith used one of these values to construct images of a putative Menon-Hadamard difference set in $G' = G/K \cong C_p \times C_4$, see [1].

But, if $p \equiv 3 \pmod 4$ then α has one possible value similar to the one in Lemma 4. In this case we expect to get a similar result to Theorem 1.

References

1. AbuGhneim, O.A., Becker, P.E., Mendes, J.K., Smith, K.W.: On Menon-Hadamard difference sets in groups of order $4p^2$. In: Proceedings of the 36th Southeastern International Conference on Combinatorics, Graph Theory and Computing. Congresus Numerantium, vol. 172, pp. 97–121 (2005).
2. Beth, T., Jungnickel, D., Lenz, H.: Design Theory. Cambridge University Press, Cambridge (1986)
3. Curtis, C.W., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Wiley Interscience, New York (1988)

4. Davis, J.A., Jedwab, J.: A survey of Hadamard difference sets. In: Arasu, K.T. (ed.) Groups, Difference Sets and the Monster, pp. 145–156. de Gruyter, Berlin (1996)
5. Dillon, J.F.: Variatios on a scheme of McFarland for noncyclic difference sets. J. Comb. Theory Ser. A **40**, 9–21 (1985)
6. Iiams, J.E.: On difference sets in groups of order $4p^2$. J. Comb. Theory Ser. A **72**, 256–276 (1995)
7. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Springer, New York (1990)
8. Jungnickel, D.: Contemporary Design Theory, Dinitz, J.H., Stinson, D.R. (eds.). Wiley, New York (1992), pp. 241–324
9. Kibler, R.E.: A summary of noncyclic difference sets $k < 20$. J. Comb. Theory Ser. A **25**(1), 62–67 (1978)
10. Lander, E.S.: Symmetric Designs: An Algebraic Approach. Cambridge University Press, Cambridge (1983)
11. Ledermann, W.: Introduction to Group Characters. Cambridge University Press, Cambridge (1977)
12. McFarland, R.L.: Difference sets in abelian groups of order $4p^2$. Mitt. Math. Sem. Giessen **192**, 1–70 (1989)
13. Smith, K.W.: Non-abelian Hadamard difference sets. J. Comb. Theory Ser. A **70**(1), 144–156 (1995)
14. Turyn, R.J.: Characters sums and difference sets. Pac. J. Math. **15**, 319–346 (1965)
15. Wan, Z.: Difference sets in groups of order $4p^4$. Beijing Daxue Xuebao Ziran Kexue Ban **36**(3), 331–341 (2000)
16. Weyl, H.: Algebraic Theory of Numbers. Princeton University Press, Princeton (1940)