

A new family of Hadamard matrices of order $4(2q^2 + 1)$

Ka Hin Leung, Koji Momihara, and Qing Xiang

ABSTRACT. Let q be a prime power of the form $q = 12c^2 + 4c + 3$ with c an arbitrary integer. In this paper we construct a difference family with parameters $(2q^2; q^2, q^2, q^2, q^2 - 1; 2q^2 - 2)$ in $\mathbb{Z}_2 \times (\mathbb{F}_{q^2}, +)$. As a consequence, by applying the Wallis-Whiteman array, we obtain Hadamard matrices of order $4(2q^2 + 1)$ for the aforementioned q 's.

1. Introduction

A *Hadamard matrix* of order v is a $v \times v$ matrix H with entries ± 1 such that $HH^\top = vI$, where I is the identity matrix. It can be easily shown that if H is a Hadamard matrix of order v , then $v = 1, 2$, or $4t$ for some positive integer t . A long-standing conjecture in combinatorics states that a Hadamard matrix of order v exists for every $v \equiv 0 \pmod{4}$. Despite the work of many researchers, the conjecture is far from being resolved. Currently it is still not known whether the set of orders of Hadamard matrices has positive density. For some sparse infinite subsequences of $\{4t : t = 1, 2, 3, \dots\}$, it is often possible to construct Hadamard matrices of order v for every v belonging to the subsequences. The most famous examples are the Paley constructions which produce Hadamard matrices of order $q + 1$ if q is a prime power congruent to 3 modulo 4, and Hadamard matrices of order $2(q + 1)$ if q is a prime power congruent to 1 modulo 4. As further examples, we mention that for prime powers $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{8}$, Xia and Liu [12, 14] construct Hadamard matrices of order $4q^2$; for $q \equiv 7 \pmod{8}$, the first author, Ma and Schmidt [4] construct two possibly infinite families of Hadamard matrices of order $4q^2$. All these constructions are based on cyclotomy of finite fields. The Paley constructions use the nonzero squares of \mathbb{F}_q . The constructions by Xia and Liu [12, 14], and by Leung, Ma, and Schmidt [4] use the 4^{th} , 8^{th} and $(q + 1)^{\text{th}}$ cyclotomic classes of \mathbb{F}_{q^2} . The main idea behind the constructions of Xia/Liu and Leung/Ma/Schmidt is to use cyclotomic classes of finite fields to construct a difference family with appropriate parameters in an abelian group G .

2010 *Mathematics Subject Classification.* 05B20, 05B10.

Koji Momihara was supported by JSPS under Grant-in-Aid for Young Scientists (B) 17K14236 and Scientific Research (B) 15H03636.

Qing Xiang was supported by an NSF grant DMS-1600850.

Throughout this paper, we will use the following notation. Let $(G, +)$ be an additively written finite abelian group and let $G^* := G \setminus \{0_G\}$. For any subset D in G , we define $D^{(-1)} := \{-x : x \in D\}$, $\overline{D} := G^* \setminus D$, and $D^c := G \setminus D$. Furthermore, we will identify D with the group ring element $\sum_{x \in D} x \in \mathbb{Z}[G]$ when there is no confusion.

Let B_i , $i = 1, 2, \dots, \ell$, be k_i -subsets of G . The set $\mathcal{B} = \{B_i : i = 1, 2, \dots, \ell\}$ is called a *difference family with parameters* $(v; k_1, k_2, \dots, k_\ell; \lambda)$ in G if the list of differences “ $x - y, x, y \in B_i, x \neq y, i = 1, 2, \dots, \ell$ ” represents every nonzero element of G exactly λ times; or equivalently

$$\sum_{i=1}^{\ell} B_i B_i^{(-1)} = \lambda G + \left(\sum_{i=1}^{\ell} k_i - \lambda \right) \cdot 0_G.$$

Each subset B_i is called a *block* of \mathcal{B} . We now define two special classes of difference families. A difference family in G with four blocks is said to be of *type H* if $\sum_{i=1}^4 k_i - |G| = \lambda$; and of *type H_4^** if $\sum_{i=1}^4 k_i - (|G| + 1) = \lambda$.

It is well known that if there is a difference family of type H in G , then we obtain a Hadamard matrix of order $4|G|$ by plugging the group invariant $(-1, 1)$ matrices obtained from its blocks into the Goethals-Seidel array [1]. In the literature, difference families of type H have been extensively studied [4, 12, 13, 14, 15, 16, 17].

On the other hand, from a difference family of type H_4^* in a finite abelian group G , we obtain a Hadamard matrix of order $4(|G| + 1)$ by plugging the the group invariant $(-1, 1)$ matrices obtained from its blocks into the Wallis-Whiteman array [10, Theorem 4.17]. Indeed difference families of type H_4^* are particularly interesting as the orders of the Hadamard matrices obtained from the difference families are no longer of the form $4|G|$, but of the form $4(|G| + 1)$. Very recently, the first and second authors [5] gave two new constructions of difference families of type H_4^* with parameters $(2n; n, n, n, n - 1; 2n - 2)$. Difference families with these parameters were initially considered by Whiteman [11], who obtained one infinite family. Soon afterwards, Spence [8] came up with two new families whose constructions are based on relative difference sets. On the other hand, the existence of difference families with parameters $(2n; n, n, n, n - 1; 2n - 2)$ in dihedral groups was also studied in [2, 3, 7]. Let us summarize all known constructions of difference families of type H_4^* with parameters $(2n; n, n, n, n - 1; 2n - 2)$.

THEOREM 1.1. *There exists a difference family of type H_4^* with parameters $(2n; n, n, n, n - 1; 2n - 2)$ if n satisfies any of the following conditions:*

- (1) [11, 7] $n = q$ and $2q - 1$ are both prime powers.
- (2) [8] $q = 2n + 1$ is a prime power for which there exists a nonnegative integer s such that $(q - 2^{s+1} - 1)/2^{s+1}$ is an odd prime power.
- (3) [8] $n = q$ is a prime power such that $q \equiv 1 \pmod{4}$, and $q - 2$ is also a prime power.

- (4) [5] $n = 9^{t_0} q_1^{4t_1} q_2^{4t_2} \cdots q_s^{4t_s}$, where p_i , $i = 1, 2, \dots, s$, are prime powers and t_i , $i = 0, 1, \dots, s$, are nonnegative integer.
- (5) [5] $n = q^2$ with q a prime power such that $q \equiv 1 \pmod{4}$.

In particular, there exists a Hadamard matrix of order $4(2n + 1)$ if n satisfies any of the above conditions.

In this paper, we obtain a new series of difference families of type H_4^* with parameters $(2q^2; q^2, q^2, q^2, q^2 - 1; 2q^2 - 2)$ where q is a prime power congruent to 3 modulo 8 satisfying some extra condition. The construction uses 8th cyclotomic classes of \mathbb{F}_{q^2} and ‘‘half lines’’ in $\text{AG}(2, q)$. In [4, 12, 14], the main idea is to construct difference families of type H in the group $(\mathbb{F}_{q^2}, +)$. Our approach here is analogous to that of [5]; the main difference here is the usage of Paley type partial difference sets. The following are our main results.

THEOREM 1.2. *Let q be a prime power of the form $q = 12c^2 + 4c + 3$ with c an arbitrary integer, and let $n = q^2$. Then there exists a difference family with parameters $(2n; n, n, n, n, n - 1; 2n - 2)$ in $\mathbb{Z}_2 \times (\mathbb{F}_{q^2}, +)$.*

By plugging the group invariant $(1, -1)$ matrices obtained from the blocks of the difference family in Theorem 1.2 into the Wallis-Whiteman array, we immediately obtain the following:

THEOREM 1.3. *Let q be a prime power of the form $q = 12c^2 + 4c + 3$ with c an arbitrary integer, and let $n = q^2$. Then there exists a Hadamard matrix of order $4(2n + 1)$.*

We remark that there are 386 prime powers of the form $q = 12c^2 + 4c + 3 < 10^7$ while there are 166181 prime powers $q < 10^7$ such that $q \equiv 3 \pmod{8}$. The first 58 prime powers of the form $q = 12c^2 + 4c + 3 < 10^5$ are listed below:

$$(1.1) \quad \begin{aligned} &3, 11, 19, 43, 59, 179, 211, 283, 563, 619, 739, 1163, 1499, 1979, 2083, 2411, 3011, \\ &3539, 4259, 4723, 7603, 8011, 8219, 10211, 11411, 12163, 14011, 14563, 14843, \\ &17483, 20011, 23059, 25579, 26699, 28619, 29803, 30203, 33923, 36083, 36523, \\ &41539, 49411, 54139, 55219, 55763, 59083, 60779, 63659, 65419, 69011, 70843, \\ &75211, 80363, 81019, 82339, 83003, 88411, 93283. \end{aligned}$$

2. The construction

We first fix our notation. Let q be a prime power such that $q \equiv 3 \pmod{4}$. Let ω be a primitive element of \mathbb{F}_{q^2} and let $0_{\mathbb{F}_{q^2}}$ denote the zero of \mathbb{F}_{q^2} . For any fixed positive integer N dividing $q^2 - 1$, define $C_i^{(N, q^2)} = \omega^i \langle \omega^N \rangle$, $i = 0, 1, \dots, N - 1$, called the N^{th} cyclotomic

classes of \mathbb{F}_{q^2} . Furthermore, define

$$\begin{aligned} H_i &= C_i^{(2(q+1), q^2)}, \quad i = 0, 1, \dots, 2q+1, \\ L_i &= C_i^{(q+1, q^2)}, \quad i = 0, 1, \dots, q, \\ S_i &= C_i^{(q+1, q^2)} \cup \{0\}, \quad i = 0, 1, \dots, q, \\ D_i &= C_i^{(4, q^2)} \cup C_{i+1}^{(4, q^2)}, \quad i = 0, 1, \dots, 3. \end{aligned}$$

Note that each S_i is a line through the origin of $\text{AG}(2, q)$; for this reason the H_i 's are called half lines [18]. In the group ring $\mathbb{Z}[(\mathbb{F}_{q^2}, +)]$, we have

$$(2.1) \quad S_i S_j = \mathbb{F}_{q^2} \text{ for } i \neq j \text{ and } S_i^2 = qS_i \text{ for all } i.$$

LEMMA 2.1. *For $i = 0, 1, 2, 3$, D_i is a Paley type partial difference set in $(\mathbb{F}_{q^2}, +)$. In particular,*

$$D_i D_i^{(-1)} = \frac{q^2 - 5}{4} D_i + \frac{q^2 - 1}{4} \overline{D}_i + \frac{q^2 - 1}{2} \cdot 0_{\mathbb{F}_{q^2}}.$$

For a proof of Lemma 2.1, we refer the reader to [6, p. 216]. The strongly regular Cayley graph, $\text{Cay}(\mathbb{F}_{q^2}, D_0)$, is often called a Peisert graph.

Our objective is to construct difference families with parameters $(2q^2; q^2, q^2 - 1, q^2, q^2; 2q^2 - 2)$ in $\mathbb{Z}_2 \times \mathbb{F}_{q^2}$. So we need to find four blocks B_0, B_1, B_2, B_3 with $|B_i| = q^2$, $i = 0, 2, 3$, and $|B_1| = q^2 - 1$, in $\mathbb{Z}_2 \times \mathbb{F}_{q^2}$ such that

$$\sum_{i=0}^3 B_i B_i^{(-1)} = (2q^2 - 2)(\mathbb{Z}_2 \times \mathbb{F}_{q^2}) + (2q^2 + 1) \cdot (0, 0_{\mathbb{F}_{q^2}}).$$

To construct the first two blocks, we make use of the Paley type partial difference sets D_0 and D_2 defined above. Note that $D_2 = \omega^2 D_0$ and $D_2 = \overline{D}_0$. In $\mathbb{Z}_2 \times \mathbb{F}_{q^2}$, we set

$$\begin{aligned} B_0 &= (\{0\} \times D_0) \cup (\{1\} \times (\mathbb{F}_{q^2} \setminus D_0)), \\ B_1 &= (\{0\} \times D_2) \cup (\{1\} \times D_2). \end{aligned}$$

Then $|B_0| = q^2$ and $|B_1| = q^2 - 1$.

PROPOSITION 2.2. *With B_0, B_1 defined as above, we have*

$$(2.2) \quad \sum_{i=0,1} B_i B_i^{(-1)} = \{0\} \times \left((q^2 - 2)\mathbb{F}_{q^2}^* + (2q^2 - 1) \cdot 0_{\mathbb{F}_{q^2}} \right) + \{1\} \times \left(2D_0 - 2D_2 + (q^2 - 1)\mathbb{F}_{q^2} \right).$$

PROOF. It is clear that

$$(2.3) \quad \begin{aligned} \sum_{i=0,1} B_i B_i^{(-1)} &= \{0\} \times \left(2 \sum_{i=0,2} D_i D_i^{(-1)} + (q^2 - 2|D_0|)\mathbb{F}_{q^2} \right) \\ &\quad + \{1\} \times \left(-2D_0 D_0^{(-1)} + 2D_2 D_2^{(-1)} + 2|D_0|\mathbb{F}_{q^2} \right). \end{aligned}$$

By Lemma 2.1, we have

$$(2.4) \quad \begin{aligned} \sum_{i=0,2} D_i D_i^{(-1)} &= \frac{q^2 - 5}{4}(D_0 + D_2) + \frac{q^2 - 1}{4}(\overline{D}_0 + \overline{D}_2) + (q^2 - 1) \cdot 0_{\mathbb{F}_{q^2}} \\ &= \frac{q^2 - 3}{2}\mathbb{F}_{q^2}^* + (q^2 - 1) \cdot 0_{\mathbb{F}_{q^2}}, \end{aligned}$$

and

$$(2.5) \quad \begin{aligned} -D_0 D_0^{(-1)} + D_2 D_2^{(-1)} &= -\left(\frac{q^2 - 5}{4}D_0 + \frac{q^2 - 1}{4}D_2\right) + \left(\frac{q^2 - 5}{4}D_2 + \frac{q^2 - 1}{4}D_0\right) \\ &= D_0 - D_2. \end{aligned}$$

It is now straight forward to obtain (2.2) from (2.3), (2.4) and (2.5). \square

To construct the remaining blocks of the desired difference family, we need difference families of type H in \mathbb{F}_{q^2} that satisfy certain conditions.

PROPOSITION 2.3. *Suppose $\mathcal{E} = \{E_i : i = 0, 1, 2, 3\}$ is a difference family of type H in \mathbb{F}_{q^2} such that $|E_0| = |E_1| = |E_2| = |E_3| = (q^2 - q)/2$ and*

$$(2.6) \quad E_0 E_1^{(-1)} + E_1 E_0^{(-1)} + E_2 E_3^{(-1)} + E_3 E_2^{(-1)} = (q - 1)^2 \mathbb{F}_{q^2} + 2D_0 - 2D_2.$$

Let B_0, B_1 be defined as above and set

$$B_2 = (\{0\} \times E_0) \cup (\{1\} \times (\mathbb{F}_{q^2} \setminus E_1)),$$

$$B_3 = (\{0\} \times E_2) \cup (\{1\} \times (\mathbb{F}_{q^2} \setminus E_3)).$$

Then $\{B_0, B_1, B_2, B_3\}$ is a difference family with parameters $(2q^2; q^2, q^2 - 1, q^2, q^2; 2q^2 - 2)$ in $\mathbb{Z}_2 \times \mathbb{F}_{q^2}$.

PROOF. First of all, we have $|B_2| = q^2 + |E_0| - |E_1| = q^2$ and $|B_3| = q^2 + |E_2| - |E_3| = q^2$. In view of (2.2), it suffices to show that

$$\sum_{i=2,3} B_i B_i^{(-1)} = \{0\} \times (2q^2 \cdot 0_{\mathbb{F}_{q^2}} + q^2 \mathbb{F}_{q^2}^*) + \{1\} \times ((q^2 - 1)\mathbb{F}_{q^2} - 2D_0 + 2D_2).$$

It is clear that

$$(2.7) \quad \begin{aligned} \sum_{i=2,3} B_i B_i^{(-1)} &= \{0\} \times \left(\sum_{i=0}^3 E_i E_i^{(-1)} + 2(q^2 - |E_1| - |E_3|)\mathbb{F}_{q^2} \right) \\ &\quad + \{1\} \times (-E_0 E_1^{(-1)} - E_1 E_0^{(-1)} - E_2 E_3^{(-1)} - E_3 E_2^{(-1)} + 2(|E_0| + |E_2|)\mathbb{F}_{q^2}). \end{aligned}$$

Since $\{E_i : i = 0, 1, 2, 3\}$ is a difference family of type H and $|E_1| + |E_3| = q^2 - q$, we have

$$(2.8) \quad \sum_{i=0}^3 E_i E_i^{(-1)} + 2(q^2 - |E_1| - |E_3|)\mathbb{F}_{q^2} = 2q^2 \cdot 0_{\mathbb{F}_{q^2}} + q^2 \mathbb{F}_{q^2}^*.$$

On the other hand, by the assumption (2.6) and $|E_0| + |E_2| = q^2 - q$, we have

$$(2.9) \quad -E_0 E_1^{(-1)} - E_1 E_0^{(-1)} - E_2 E_3^{(-1)} - E_3 E_2^{(-1)} + 2(|E_0| + |E_2|)\mathbb{F}_{q^2} = (q^2 - 1)\mathbb{F}_{q^2} - 2D_0 + 2D_2.$$

The proposition now follows from (2.7), (2.8), and (2.9). \square

To construct difference families of type H in \mathbb{F}_{q^2} satisfying the conditions in Proposition 2.3, it is then natural to consider those constructed in [4].

LEMMA 2.4. ([4, Lemma 4 and Corollary 5]) *Let $q \equiv 3 \pmod{4}$ be a prime power and let e be the exact power of 2 dividing $q + 1$. Let $\alpha < e$ be an odd number and set $\beta = \frac{qe - \alpha(q+1)}{2e}$. Let $\mathbf{A} \subseteq \{0, 1, \dots, 2e - 1\}$ and $\mathbf{B}_0, \dots, \mathbf{B}_{e-1} \subseteq \{0, 1, \dots, q\}$ with $|\mathbf{A}| = \alpha$, $|\mathbf{B}_0| = \dots = |\mathbf{B}_{e-1}| = \beta$ such that $b \not\equiv a \pmod{e}$ for all $a \in \mathbf{A}$ and $b \in \bigcup_{r=0}^{e-1} \mathbf{B}_r$. Set*

$$\begin{aligned} H &= \bigcup_{i \in \mathbf{A}} C_i^{(2e, q^2)} \\ M_i &= \bigcup_{j \in \mathbf{B}_i} L_j, \quad i = 0, 1, \dots, e - 1 \\ \mathbf{D}_i &= \omega^i(H \cup M_i), \quad i = 0, 1, \dots, e - 1. \end{aligned}$$

Then $|\mathbf{D}_i| = \frac{q(q-1)}{2}$ for $i = 0, 1, \dots, e - 1$, and $\{\mathbf{D}_i : i = 0, 1, \dots, e - 1\}$ forms a difference family in $(\mathbb{F}_{q^2}, +)$ with $\lambda = \frac{eq(q-2)}{4}$.

We now assume that q is a prime power and $q = 8m + 3$ for some positive integer m . In view of Lemma 2.4, we need a set $\mathbf{A} \subseteq \{0, 1, \dots, 7\}$ with $|\mathbf{A}| = 3$, and four subsets \mathbf{B}_i , $i = 0, 1, 2, 3$, of $\{0, \dots, q\}$, each of size m , satisfying certain conditions.

First, we require $I \cap \{x + 4 \pmod{8} : x \in I\} = \emptyset$. Since $|I| = 3$, the condition $I \cap \{x + 4 \pmod{8} : x \in I\} = \emptyset$ simply means that I contains exactly one odd or exactly one even element, say, $y \in I$. (Note that such an I clearly exists, for example, take $I = \{0, 1, 3\}$; and in this case $y = 0$.) Next, we define two m -subsets of $\{0, 1, \dots, q\}$:

$$\begin{aligned} J_1 &= \{y + 2 + 4i \pmod{q+1} : i \in \{0, 1, \dots, m-1\}\} \text{ and} \\ J_2 &= \{y + 4i \pmod{q+1} : i \in \{0, 1, \dots, m-1\}\}. \end{aligned}$$

Now, using the notation in Lemma 2.4, we set $e = 4$, $\alpha = 3$ and $\beta = m$. Let $\mathbf{A} = I$, $\mathbf{B}_0 = \mathbf{B}_1 = J_1$,

$$\mathbf{B}_2 = \mathbf{B}_3 = \{y - 2 + 4i \pmod{q+1} : i \in \{0, 1, \dots, m-1\}\}.$$

It is then straight forward to check that the conditions in Lemma 2.4 are all satisfied. Therefore we obtain a difference family $\{\mathbf{D}_i : i = 0, 1, 2, 3\}$. However, for our purpose, we need to set $E_0 = \mathbf{D}_0$, $E_1 = \mathbf{D}_2$, $E_2 = \mathbf{D}_1$ and $E_3 = \mathbf{D}_3$. In terms of I, J_1, J_2 , we have the following:

$$(2.10) \quad \begin{aligned} E_0 &= \left(\bigcup_{i \in I} C_i^{(8, q^2)} \right) \cup \left(\bigcup_{i \in J_1} L_i \right), \quad E_1 = \left(\bigcup_{i \in I} C_{i+2}^{(8, q^2)} \right) \cup \left(\bigcup_{i \in J_2} L_i \right), \\ E_2 &= \left(\bigcup_{i \in I} C_{i+1}^{(8, q^2)} \right) \cup \left(\bigcup_{i \in J_1} L_{i+1} \right), \quad E_3 = \left(\bigcup_{i \in I} C_{i+3}^{(8, q^2)} \right) \cup \left(\bigcup_{i \in J_2} L_{i+1} \right). \end{aligned}$$

By Lemma 2.4, $\{E_i, i = 0, 1, 2, 3\}$ is a difference family of type H in $(\mathbb{F}_{q^2}, +)$. Furthermore, $|E_i| = \frac{q^2 - q}{2}$ for $i = 0, 1, 2, 3$. It therefore remains to show the following:

THEOREM 2.5. *The E_i 's defined in (2.10) satisfy the equation (2.6). In particular, there is a difference family with parameters $(2q^2; q^2, q^2, q^2, q^2 - 1; 2q^2 - 2)$ in $\mathbb{Z}_2 \times (\mathbb{F}_{q^2}, +)$.*

3. Proof of Theorem 2.5

To prove Theorem 2.5, we need to compute $E_0E_1^{(-1)} + E_0E_1^{(-1)} + E_2E_3^{(-1)} + E_3E_2^{(-1)}$. As in the case of Lemma 4 in [4], it will make the computations easier if we write each E_i in a different form (i.e., as a union of H_i 's and L_j 's). Recall that $q = 8m + 3$ is a prime power. We define

$$I_1 = \{x + 8i \pmod{2(q+1)} : x \in I, i \in \{0, 1, \dots, 2m\}\} \text{ and } I_2 = I_1 + 2.$$

Here we use the notation $K + 1 = \{x + 1 : x \in K\}$. Note that $|I_1| = |I_2| = 3(q+1)/4$. Recall that

$$J_1 = \{y + 2 + 4i \pmod{q+1} : i \in \{0, 1, \dots, m-1\}\} \text{ and } J_2 = J_1 - 2.$$

We write

$$\begin{aligned} E_0 &= \sum_{i \in I_1} H_i + \sum_{i \in J_1} L_i \text{ and } E_1 = \sum_{i \in I_2} H_i + \sum_{i \in J_2} L_i, \\ E_2 &= \sum_{i \in I_1+1} H_i + \sum_{i \in J_1+1} L_i \text{ and } E_3 = \sum_{i \in I_2+1} H_i + \sum_{i \in J_2+1} L_i. \end{aligned}$$

Observe that the following conditions are satisfied:

- (1) Since $I \cap \{x + 4 \pmod{8} : x \in I\} = \emptyset$, we have $I_i \cap \{h + (q+1) \pmod{2(q+1)} : h \in I_i\} = \emptyset$ for $i = 1, 2$,
- (2) $a \not\equiv b \pmod{q+1}$ for all $a \in I_i, b \in J_i, i = 1, 2$,
- (3) $|I_1| + 2|J_1| = |I_2| + 2|J_2| = q$,
- (4) $J_1 \subseteq I'_2 \cup J_2$ and $J_2 \subseteq I'_1 \cup J_1$, where $I'_j = \{i \pmod{q+1} : i \in I_j\}$ for $j = 1, 2$.

LEMMA 3.1. *In the group ring $\mathbb{Z}[(\mathbb{F}_{q^2}, +)]$, $E_0E_1^{(-1)} + E_1E_0^{(-1)} =$*

$$(3.1) \quad \sum_{i \in I_1} \sum_{j \in I_2} H_i H_j^{(-1)} + \sum_{i \in I_2} \sum_{j \in I_1} H_i H_j^{(-1)} + \lambda_1 \cdot 0_{\mathbb{F}_{q^2}} + \lambda_2 \mathbb{F}_{q^2} - |J_2| \sum_{i \in I'_1} S_i - |J_1| \sum_{i \in I'_2} S_i,$$

where $\lambda_1 = |I_1||J_2| + |I_2||J_1| + 2|J_1||J_2|$ and $\lambda_2 = |I'_1||J_2| + |I'_2||J_1| + 2|J_1||J_2| - |I'_1 \cap J_2| - |I'_2 \cap J_1| - 2|J_1 \cap J_2|$.

PROOF. Note that $L_i^{(-1)} = L_i$. We first expand the expression $E_0E_1^{(-1)} + E_0E_1^{(-1)}$ and obtain the following:

$$\begin{aligned} E_0E_1^{(-1)} + E_1E_0^{(-1)} &= \sum_{i \in I_1} \sum_{j \in I_2} H_i H_j^{(-1)} + \sum_{i \in I_2} \sum_{j \in I_1} H_i H_j^{(-1)} + Y \text{ where} \\ Y &= \sum_{i \in I_1} (H_i + H_i^{(-1)}) \sum_{i \in J_2} L_i + \sum_{i \in I_2} (H_i + H_i^{(-1)}) \sum_{i \in J_1} L_i + 2 \sum_{i \in J_1} L_i \sum_{i \in J_2} L_i. \end{aligned}$$

Note that $S_i = L_i + 0_{\mathbb{F}_{q^2}}$. So, we may replace each L_i by $S_i - 0_{\mathbb{F}_{q^2}}$ in the above sum and we get

$$\begin{aligned} Y &= -|J_2| \sum_{i \in I_1} (H_i + H_i^{(-1)}) - |J_1| \sum_{i \in I_2} (H_i + H_i^{(-1)}) \\ &\quad + \sum_{i \in I_1} \sum_{j \in J_2} S_j (H_i + H_i^{(-1)}) + \sum_{i \in I_2} \sum_{j \in J_1} S_j (H_i + H_i^{(-1)}) \\ &\quad + 2 \sum_{i \in J_1} \sum_{j \in J_2} S_i S_j - 2|J_1| \sum_{j \in J_2} S_i - 2|J_2| \sum_{j \in J_1} S_i + 2|J_1||J_2| \cdot 0_{\mathbb{F}_{q^2}}. \end{aligned}$$

Observe that $H_i + H_{q+1+i} = S_i - 0_{\mathbb{F}_{q^2}}$ for $i = 0, 1, \dots, q$ and (3) holds. Also note that

$$\begin{aligned} \sum_{i \in I_1} \sum_{j \in J_2} S_j (H_i + H_i^{(-1)}) &= \sum_{i \in I'_1} \sum_{j \in J_2} S_j S_i - |J_2| \sum_{i \in I'_1} S_i \text{ and} \\ \sum_{i \in I_2} \sum_{j \in J_1} S_j (H_i + H_i^{(-1)}) &= \sum_{i \in I'_2} \sum_{j \in J_1} S_j S_i - |J_1| \sum_{i \in I'_2} S_i. \end{aligned}$$

We then have

$$\begin{aligned} Y &= \lambda_1 \cdot 0_{\mathbb{F}_{q^2}} - |J_2| \sum_{i \in I'_1} S_i - |J_1| \sum_{i \in I'_2} S_i - q \sum_{i \in J_2} S_i - q \sum_{i \in J_1} S_i \\ (3.2) \quad &\quad + \sum_{i \in I'_1} \sum_{j \in J_2} S_j S_i + \sum_{i \in I'_2} \sum_{j \in J_1} S_i S_j + 2 \sum_{i \in J_1} \sum_{j \in J_2} S_i S_j. \end{aligned}$$

On the other hand, $S_i S_j = \mathbb{F}_{q^2}$ whenever $i \neq j$. Therefore, by the conditions (2) and (4), for distinct u, v in $\{1, 2\}$,

$$(3.3) \quad \sum_{i \in I'_u} \sum_{j \in J_v} S_j S_i = q \sum_{i \in (I'_u \cap J_v)} S_i + (|I'_u| \cdot |J_v| - |I'_u \cap J_v|) \mathbb{F}_{q^2} \text{ and}$$

$$(3.4) \quad \sum_{i \in J_1} \sum_{j \in J_2} S_i S_j = q \sum_{i \in (J_1 \cap J_2)} S_i + (|J_1| \cdot |J_2| - |J_1 \cap J_2|) \mathbb{F}_{q^2}.$$

(3.1) now follows easily from (3.2), (3.3) and (3.4). \square

Now, replace I_i with $I_i + 1$, and J_i with $J_i + 1$ in the argument above and observe that condition (2), (3) and (4) still hold. We immediately get the following:

LEMMA 3.2. *In the group ring $\mathbb{Z}[(\mathbb{F}_{q^2}, +)]$, $E_2 E_3^{(-1)} + E_3 E_2^{(-1)} =$*

$$(3.5) \quad \sum_{i \in I_1+1} \sum_{j \in I_2+1} H_i H_j^{(-1)} + \sum_{i \in I_2+1} \sum_{j \in I_1+1} H_i H_j^{(-1)} + \lambda_1 \cdot 0_{\mathbb{F}_{q^2}} + \lambda_2 \mathbb{F}_{q^2} - |J_2| \sum_{i \in I'_1} S_i - |J_1| \sum_{i \in I'_2} S_i,$$

where $\lambda_1 = |I_1||J_2| + |I_2||J_1| + 2|J_1||J_2|$ and $\lambda_2 = |I'_1||J_2| + |I'_2||J_1| + 2|J_1||J_2| - |I'_1 \cap J_2| - |I'_2 \cap J_1| - 2|J_1 \cap J_2|$.

LEMMA 3.3. Let E_i , $i = 0, 1, 2, 3$, be defined as in (2.10). Recall that $q = 8m + 3$. Then, we have

$$E_0 E_1^{(-1)} + E_0 E_1^{(-1)} + E_2 E_3^{(-1)} + E_3 E_2^{(-1)} = \sum_{h=0,1} \sum_{i,j \in I} \left(C_{i+h}^{(8,q^2)} C_{j+2+h}^{(8,q^2)^{(-1)}} + C_{i+2+h}^{(8,q^2)} C_{j+h}^{(8,q^2)^{(-1)}} \right) + Z$$

where $Z = 8m(4m + 1) \cdot 0_{\mathbb{F}_{q^2}} + m(28m + 5)\mathbb{F}_{q^2}^*$.

PROOF. Applying Lemmas 3.1 and 3.2, we obtain

$$(3.6) \quad \begin{aligned} & E_0 E_1^{(-1)} + E_0 E_1^{(-1)} + E_2 E_3^{(-1)} + E_3 E_2^{(-1)} \\ &= \sum_{h=0,1} \sum_{i,j \in I} \left(C_{i+h}^{(8,q^2)} C_{j+2+h}^{(8,q^2)^{(-1)}} + C_{i+2+h}^{(8,q^2)} C_{j+h}^{(8,q^2)^{(-1)}} \right) + 2\lambda_1 0_{\mathbb{F}_{q^2}} + 2\lambda_2 \mathbb{F}_{q^2} \\ & \quad - |J_2| \sum_{i \in I'_1} (S_i + S_{i+1}) - |J_1| \sum_{i \in I'_2} (S_i + S_{i+1}). \end{aligned}$$

Since $|I'_1| = |I'_2| = 6m + 3$, we have

$$\sum_{i \in I'_1} (S_i + S_{i+1}) = 2(6m + 3) \cdot 0_{\mathbb{F}_{q^2}} + \sum_{i \in I} \left(C_i^{(4,q^2)} + C_{i+1}^{(4,q^2)} \right)$$

and

$$\sum_{i \in I'_2} (S_i + S_{i+1}) = 2(6m + 3) \cdot 0_{\mathbb{F}_{q^2}} + \sum_{i \in I} \left(C_{i+2}^{(4,q^2)} + C_{i+3}^{(4,q^2)} \right).$$

Note that $\sum_{j=0}^3 C_{i+j}^{(4,q^2)} = \mathbb{F}_{q^2}^*$, $|I| = 3$ and $|J_1| = |J_2| = m$. Hence,

$$(3.7) \quad -|J_2| \sum_{i \in I'_1} (S_i + S_{i+1}) - |J_1| \sum_{i \in I'_2} (S_i + S_{i+1}) = -12m(2m + 1) \cdot 0_{\mathbb{F}_{q^2}} - 3m\mathbb{F}_{q^2}^*.$$

Furthermore, it is clear that

$$(3.8) \quad \lambda_1 = 2m(7m + 3) \quad \text{and} \quad \lambda_2 = 2m(7m + 2).$$

Our lemma now follows from (3.6) with (3.7) and (3.8). \square

To finish our proof, we need to evaluate $C_i^{(8,q^2)} C_j^{(8,q^2)^{(-1)}}$. The coefficient c_x of $x \in \mathbb{F}_{q^2}$ in $C_i^{(8,q^2)} C_j^{(8,q^2)^{(-1)}}$ is $|(C_j^{(8,q^2)} + x) \cap C_i^{(8,q^2)}|$. If $x \in C_h^{(8,q^2)}$, it is clear that $c_x = |(C_{j-h}^{(8,q^2)} + 1) \cap C_{i-h}^{(8,q^2)}|$. The numbers $(i, j)_N = |(C_i^{(N,q^2)} + 1) \cap C_j^{(N,q^2)}|$, $i, j = 0, 1, \dots, N - 1$, are called N^{th} cyclotomic numbers. In our case, $q \equiv 3 \pmod{8}$ is a prime power. In view of [9, Lemma 30], we obtain the following:

PROPOSITION 3.4. Let $q \equiv 3 \pmod{8}$ be a prime power. Then the cyclotomic numbers $(i, j)_8$, $i, j = 0, 1, \dots, 7$, in \mathbb{F}_{q^2} are determined by Table 1 and the relations:

$$\begin{aligned} 64n_1 &= q^2 - 15 + 2q, & 64n_2 &= q^2 + 1 - 2q - 4a, & 64n_3 &= q^2 + 1 - 6q + 8a, \\ 64n_4 &= q^2 + 1 + 18q, & 64n_5 &= q^2 - 7 - 2q + 4a, & 64n_6 &= q^2 + 1 + 6q + 4a + 16b, \\ 64n_7 &= q^2 + 1 + 6q + 4a - 16b, & 64n_8 &= q^2 - 7 + 2q - 8a, \end{aligned}$$

where a, b are specified by the unique proper representation of $q^2 = a^2 + 2b^2$ with $a \equiv 1 \pmod{4}$. Note that there is no restriction on the sign of b .

TABLE 1. Cyclotomic numbers of order 8: the (i, j) -entry is $(i, j)_8$.

	0	1	2	3	4	5	6	7
0	n_1	n_2	n_3	n_2	n_4	n_2	n_3	n_2
1	n_5	n_5	n_6	n_2	n_2	n_2	n_2	n_7
2	n_8	n_2	n_8	n_7	n_3	n_2	n_3	n_6
3	n_5	n_2	n_2	n_5	n_2	n_7	n_6	n_2
4	n_1	n_5	n_8	n_5	n_1	n_5	n_8	n_5
5	n_5	n_2	n_7	n_6	n_2	n_5	n_2	n_2
6	n_8	n_7	n_3	n_2	n_3	n_6	n_8	n_2
7	n_5	n_6	n_2	n_2	n_2	n_2	n_7	n_5

THEOREM 3.5. Suppose $q^2 = a^2 + 2b^2$ is the unique proper representation with $a \equiv 1 \pmod{4}$. Theorem 2.5 holds if either of the following conditions is satisfied.

- (a) $I = \{0, 2, 3\}$ and $3q = a + 4b + 16$.
- (b) $I = \{0, 2, 7\}$ and $3q = a - 4b + 16$.

PROOF. By Lemma 3.3, it is sufficient to show the following:

$$(3.9) \quad U := \sum_{h=0,1} \sum_{i,j \in I} \left(C_{i+h}^{(8,q^2)} C_{j+2+h}^{(8,q^2)^{(-1)}} + C_{i+2+h}^{(8,q^2)} C_{j+h}^{(8,q^2)^{(-1)}} \right) = \frac{q^2 - 1}{2} \cdot 0_{\mathbb{F}_{q^2}} + \frac{9q^2 - 17}{16} \mathbb{F}_{q^2}^* + 2D_0 - 2D_2.$$

We give a proof only in the case where $3q = a + 4b + 16$. The proof for the case where $3q = a - 4b + 16$ is similar.

Define $D = \bigcup_{i \in I} C_i^{(8,q^2)}$, and let c_x denote the coefficient of $x \in \mathbb{F}_{q^2}$ in U . To show that $c_0 = \frac{q^2-1}{2}$, it is sufficient to check number of pairs $(i, j) \in I \times I$ such that $i \equiv j+2 \pmod{8}$ and $i+2 \equiv j \pmod{8}$. Clearly, the solution is $(2, 0)$ and $(0, 2)$ in each case respectively. Therefore, $c_0 = 2 \times 2 \times \frac{q^2-1}{8} = \frac{q^2-1}{2}$. To prove that (3.9) holds, it is enough to see that $c_1 = c_\omega = c_{\omega^2} + 4 = c_{\omega^3} + 4$ since $c_{\omega^i} = c_{\omega^{i+4j}}$ for all i, j . On the other hand, c_x for $x \in \mathbb{F}_{q^2}^*$ is given by

$$c_x = |D \cap (\omega^2 D + x)| + |\omega^2 D \cap (D + x)| + |\omega D \cap (\omega^3 D + x)| + |\omega^3 D \cap (\omega D + x)|.$$

Hence, the system of equations $c_1 = c_\omega = c_{\omega^2} + 4 = c_{\omega^3} + 4$ is reformulated as

$$\begin{aligned} & |D \cap (\omega^2 D + 1)| + |\omega^2 D \cap (D + 1)| + |\omega D \cap (\omega^3 D + 1)| + |\omega^3 D \cap (\omega D + 1)| \\ &= |\omega^{-1} D \cap (\omega D + 1)| + |\omega D \cap (\omega^{-1} D + 1)| + |D \cap (\omega^2 D + 1)| + |\omega^2 D \cap (D + 1)| \\ &= |\omega^{-2} D \cap (D + 1)| + |D \cap (\omega^{-2} D + 1)| + |\omega^{-1} D \cap (\omega D + 1)| + |\omega D \cap (\omega^{-1} D + 1)| + 4 \\ &= |\omega^{-3} D \cap (\omega^{-1} D + 1)| + |\omega^{-1} D \cap (\omega^{-3} D + 1)| + |\omega^{-2} D \cap (D + 1)| + |D \cap (\omega^{-2} D + 1)| + 4. \end{aligned}$$

Noting that $|\omega D \cap (\omega^3 D + 1)| + |\omega^3 D \cap (\omega D + 1)| = |\omega^{-3} D \cap (\omega^{-1} D + 1)| + |\omega^{-1} D \cap (\omega^{-3} D + 1)|$, the equations above are reduced to

$$(3.10) \quad |\omega D \cap (\omega^3 D + 1)| + |\omega^3 D \cap (\omega D + 1)| = |\omega^{-1} D \cap (\omega D + 1)| + |\omega D \cap (\omega^{-1} D + 1)|$$

and

$$(3.11) \quad |D \cap (\omega^2 D + 1)| + |\omega^2 D \cap (D + 1)| = |\omega^{-2} D \cap (D + 1)| + |D \cap (\omega^{-2} D + 1)| + 4.$$

Let

$$N_1 = |\omega D \cap (\omega^3 D + 1)| + |\omega^3 D \cap (\omega D + 1)|, \quad N_2 = |\omega^{-1} D \cap (\omega D + 1)| + |\omega D \cap (\omega^{-1} D + 1)|,$$

$$N_3 = |D \cap (\omega^2 D + 1)| + |\omega^2 D \cap (D + 1)|, \quad N_4 = |\omega^{-2} D \cap (D + 1)| + |D \cap (\omega^{-2} D + 1)|.$$

Then, (3.10) and (3.11) are rewritten as $N_1 = N_2$ and $N_3 = N_4 + 4$, respectively. From the definition of I and Table 1 of Proposition 3.4, we have

$$\begin{aligned} N_1 &= (1, 3)_8 + (1, 5)_8 + (1, 6)_8 + (3, 3)_8 + (3, 5)_8 + (3, 6)_8 + (4, 3)_8 + (4, 5)_8 + (4, 6)_8 \\ &\quad + (3, 1)_8 + (5, 1)_8 + (6, 1)_8 + (3, 3)_8 + (5, 3)_8 + (6, 3)_8 + (3, 4)_8 + (5, 4)_8 + (6, 4)_8 \\ &= 8n_2 + n_3 + 4n_5 + 2n_6 + 2n_7 + n_8, \end{aligned}$$

$$\begin{aligned} N_2 &= (7, 1)_8 + (7, 3)_8 + (7, 4)_8 + (1, 1)_8 + (1, 3)_8 + (1, 4)_8 + (2, 1)_8 + (2, 3)_8 + (2, 4)_8 \\ &\quad + (1, 7)_8 + (3, 7)_8 + (4, 7)_8 + (1, 1)_8 + (3, 1)_8 + (4, 1)_8 + (1, 2)_8 + (3, 2)_8 + (4, 2)_8, \\ &= 8n_2 + n_3 + 4n_5 + 2n_6 + 2n_7 + n_8, \end{aligned}$$

$$\begin{aligned} N_3 &= (0, 2)_8 + (0, 4)_8 + (0, 5)_8 + (2, 2)_8 + (2, 4)_8 + (2, 5)_8 + (3, 2)_8 + (3, 4)_8 + (3, 5)_8 \\ &\quad + (2, 0)_8 + (4, 0)_8 + (5, 0)_8 + (2, 2)_8 + (4, 2)_8 + (5, 2)_8 + (2, 3)_8 + (4, 3)_8 + (5, 3)_8, \\ &= n_1 + 4n_2 + 2n_3 + n_4 + 2n_5 + n_6 + 3n_7 + 4n_8, \end{aligned}$$

$$\begin{aligned} N_4 &= (6, 0)_8 + (6, 2)_8 + (6, 3)_8 + (0, 0)_8 + (0, 2)_8 + (0, 3)_8 + (1, 0)_8 + (1, 2)_8 + (1, 3)_8 \\ &\quad + (0, 6)_8 + (2, 6)_8 + (3, 6)_8 + (0, 0)_8 + (2, 0)_8 + (3, 0)_8 + (0, 1)_8 + (2, 1)_8 + (3, 1)_8 \\ &= 2n_1 + 6n_2 + 4n_3 + 2n_5 + 2n_6 + 2n_8. \end{aligned}$$

It is clear that $N_1 = N_2$. By the evaluations for n_1, n_2, \dots, n_8 in Proposition 3.4, we have $N_3 = (18q^2 + 28q - 8a - 32b - 46)/64$ and $N_4 = (18q^2 + 20q + 8a + 32b - 46)/64$. Hence, $N_3 = N_4 + 4$ if and only if $3q = a + 4b + 16$. This shows that (3.9) holds if $3q = a + 4b + 16$. \square

It is not difficult to see that the condition $q^2 = a^2 + 2b^2$ with $3q = a \pm 4b + 16$ and $a \equiv 1 \pmod{4}$ is equivalent to that q has the form $q = 12c^2 + 4c + 3$ with c an arbitrary integer; in this case, $a = 4c^2 + 12c + 1$ and $b = \pm(8c^2 - 2)$. Hence, by Theorem 3.5 and Proposition 2.3, Theorem 1.2 now follows.

To see whether we have constructed an infinite family of Hadamard matrices in Theorem 1.3, a natural question arises: are there infinitely many prime powers q of the form

$q = 12c^2 + 4c + 3$ with c an integer? We believe that there are infinitely many primes of the form $12c^2 + 4c + 3$ with c an integer. But this is probably very difficult to prove. On the other hand, we conjecture that there are no proper prime powers q of the form $q = 12c^2 + 4c + 3$ (c is an integer). That is, we conjecture that there are no solutions to the equation

$$12c^2 + 4c + 3 = p^\alpha, \alpha > 1,$$

where c is an integer, and p is a prime. Some evidence is given in Introduction, namely all 58 prime powers listed in (1.1) are actually primes.

References

- [1] J.-M. Goethals, J. J. Seidel, Orthogonal matrices with zero diagonal, *Canad. J. Math.* **19** (1967), 1001–1010.
- [2] H. Kimura, Hadamard matrices and dihedral groups, *Des. Codes Cryptogr.* **8** (1996), 71–77.
- [3] H. Kimura, T. Niwasaki, Some properties of Hadamard matrices coming from dihedral groups, *Graphs Combin.* **8** (2002), 319–327.
- [4] K. H. Leung, S. L. Ma, B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, *J. Combin. Theory, Ser. A* **113** (2006), 822–838.
- [5] K. H. Leung, K. Momihara, New constructions of Hadamard matrices, [arXiv:1809.05253](https://arxiv.org/abs/1809.05253).
- [6] W. Peisert, All self-complementary symmetric graphs, *J. Algebra* **240** (2001), 209–229.
- [7] K. Shinoda, M. Yamada, A family of Hadamard matrices of dihedral group type, *Discrete Appl. Math.* **102** (2000), 141–150.
- [8] E. Spence, Hadamard matrices from relative difference sets, *J. Combin. Theory, Ser. A* **19** (1975), 287–300.
- [9] T. Storer, *Cyclotomy and Difference Sets*, Markham Publishing Company, 1967.
- [10] W. D. Wallis, A. P. Street, J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics, **292**, Springer, New York, 1972.
- [11] A. L. Whiteman, Hadamard matrices of order $4(2p+1)$, *Notices Amer. Math. Soc.* **19** (1972), A-681.
- [12] M.-Y. Xia, G. Liu, An infinite class of supplementary difference sets and Williamson matrices, *J. Combin. Theory, Ser. A* **58** (1991), 310–317.
- [13] M.-Y. Xia, G. Liu, On the class \mathcal{H}_1^* , *Acta Math. Sci.* **15** (1995), 361–369.
- [14] M.-Y. Xia, G. Liu, A new family of supplementary difference sets and Hadamard matrices, *J. Statist. Plann. Inference* **51** (2003), 263–275.
- [15] M.-Y. Xia, T. B. Xia, Hadamard matrices constructed from supplementary difference sets in the class \mathcal{H}_1 , *J. Combin. Des.* **2** (1994), 325–339.
- [16] M.-Y. Xia, T. B. Xia, A family of C -partitions and T -matrices, *J. Combin. Des.* **7** (1999), 269–281.
- [17] M.-Y. Xia, T. B. Xia, J. Seberry, J. Wu, An infinite family of Goethals-Seidel arrays, *Discrete Appl. Math.* **145** (2005), 498–504.
- [18] Q. Xiang, Difference families from lines and half lines, *Europ. J. Combin.* **19** (1998), 395–400.

DEPARTMENT OF MATHEMATICS, NATIONAL UNIVERSITY OF SINGAPORE, KENT RIDGE, SINGAPORE 119260, REPUBLIC OF SINGAPORE

E-mail address: `matlkh@nus.edu.sg`

DIVISION OF NATURAL SCIENCE,, FACULTY OF ADVANCED SCIENCE AND TECHNOLOGY,, KUMAMOTO UNIVERSITY, 2-40-1 KUROKAMI, KUMAMOTO 860-8555, JAPAN

E-mail address: `momihara@educ.kumamoto-u.ac.jp`

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF DELAWARE, NEWARK DE 19716, USA

E-mail address: `qxiang@udel.edu`