New Hadamard Matrices of Order $4p^2$
obtained from Jacobi Sums of Order 16 *

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore
matlkh@nus.edu.sg

Siu Lun Ma
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore
matmasl@nus.edu.sg

Bernhard Schmidt
School of Physical & Mathematical Sciences
Nanyang Technological University
No. 1 Nanyang Walk, Blk 5, Level 3
Singapore 637616
Republic of Singapore
bernhard@ntu.edu.sg

May 12, 2005

Abstract

Let $p \equiv 7 \mod 16$ be a prime. Then there are integers $a, b, c, d$ with $a \equiv 15 \mod 16,$
$b \equiv 0 \mod 4,$ $p^2 = a^2 + 2(b^2 + c^2 + d^2),$ and $2ab = c^2 - 2cd - d^2.$ We show that there is a
regular Hadamard matrix of order $4p^2$ provided that $p = a \pm 2b$ or $p = a + \delta_1 b + 4\delta_2 c + 4\delta_1 \delta_2 d$
with $\delta_i = \pm 1.$

*This research was done during a visit of the first two authors at the University of Augsburg
1 Introduction

A Hadamard matrix of order $v$ is a $v \times v$ matrix $H$ with entries $\pm 1$ such $HH^t = vI$ where $I$ is the identity matrix. A Hadamard matrix is called regular if all of its rows contain the same number of entries 1. It is conjectured that a Hadamard matrix of order $v > 2$ exists if $v$ is divisible by 4.

While the construction of Hadamard matrices of order $4t$ for arbitrary $t$ seems out of reach at the present time, there may be some hope to construct Hadamard matrices of order $4q^2$ for all prime powers $q$. For $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 8$ this already has been accomplished by the marvelous work of Mingyuan Xia and Gang Liu [7, 8]. The constructions of Xia and Liu are based on cyclotomy, namely, the use of 4th, 8th and $(q + 1)$th cyclotomic classes in $\mathbb{F}_{q^2}$. However, it seems that the difficulty of implementing the approach using cyclotomy increases with the exact power of 2 dividing $q + 1$, cf. our Lemma 4 in Section 3. In fact, up to our knowledge, no general constructions for Hadamard matrices of order $4q^2$ with $q \equiv 7 \pmod 8$ have been known.

In the present paper, we obtain two putative infinite families of Hadamard matrices of order $4q^2$ with $q \equiv 7 \pmod 8$ prime. We believe that, for any large enough $n$, our constructions yield at least $\frac{5}{8}n^2$ primes $q < n$, $q \equiv 7 \pmod 16$ such that a regular Hadamard matrices of order $4q^2$ exists. Our approach is based on 16th and $(q + 1)$th cyclotomic classes. The necessary computations are much more involved than those in [7, 8] and we need to use Jacobi sums as well as a computer. For each value of $q$ for which our construction works, we obtain a “certificate” in terms of a quadruple of integers $a, b, c, d$. Once this quadruple is known, the verification of the construction only involves checking simple conditions on $a, b, c, d$ which can be done by hand if $q$ is not exceedingly large.

The integers $a, b, c, d$ are coefficients of the Jacobi sum

$$J := \sum_{x \in \mathbb{F}_{q^2}} \chi(x)\rho(x)$$

of order 16 (the order of a Jacobi sum is the least common multiple of the orders of the involved characters). Here $\chi$ is a multiplicative character of order 16 and $\rho$ is the quadratic character of $\mathbb{F}_{q^2}$. In Section 4 we will characterize $a, b, c, d$ by the simple congruences and equations mentioned in the abstract.

2 Preliminaries

Let $G$ be an additively written abelian group of order $v$. We write $\oplus$ respectively $\ominus$ for the addition respectively subtraction in $G$ in order to distinguish them from the group ring addition and subtraction. A $t - (v, k, \lambda)$ difference family in $G$ is a family $(D_1, ..., D_t)$ of $k$-subsets of $G$ such that for each $g \in G \setminus \{0\}$ the set

$$\{(x, y, i) : g = x \oplus y, \ x, y \in D_i, \ i \in \{1, ..., t\}\}$$

has cardinality $\lambda$.

We will always identify a subset $A$ of $G$ with the element $\sum_{g \in A} g$ of the integral group ring $\mathbb{Z}[G]$. For $B = \sum_{g \in G} b_g g \in \mathbb{Z}[G]$ we write $B^{(-1)} = \sum_{g \in G} b_g (\ominus g)$ and $|B| = \sum_{g \in G} b_g$. 


In the group ring language, a family \((D_1, ..., D_t)\) of \(k\)-subsets of \(G\) is a \(t - (v, k, \lambda)\) difference family in \(G\) if and only if
\[
\sum_{i=1}^{t} D_i D_i^{-1} = (tk - \lambda) + \lambda G. \tag{1}
\]

The following result is well known [4, 9]. For the convenience of the reader, we provide a proof.

**Proposition 1** If there is a \(4-(v^2, \frac{1}{2}v(v-1), v(v-2))\) difference family \((D_1, D_2, D_3, D_4)\) in an abelian group \(G\) then there is a regular Hadamard matrix of order \(4v^2\).

**Proof** In view of (1) we have \(\sum_{i=1}^{4} D_i D_i^{-1} = v^2 + v(v-2)G\). Let \(h_1 = 2D_1 - G\). Then each \(h_i\) has coefficients \(-1, 1\) only and we have \(\sum_{i=1}^{4} h_i h_i^{-1} = 4v^2\). Write \(h_i = \sum_{g \in G} a_{i,g} g, i = 1, ..., 4\).

We define \(v^2 \times v^2\)-matrices \(H_i\) indexed by the elements of \(G\) such that \((H_i)_{g,h} = a_{i,h \oplus g}\). Then \(\sum_{i=1}^{4} h_i h_i^{-1} = 4v^2\) implies
\[
\sum_{i=1}^{4} H_i H_i^t = 4v^2 I \tag{2}
\]
where \(I\) is the identity matrix of order \(v^2\). For \(g \in G\) let \(e(g)\) be the vector indexed with the elements of \(g\) such that \(e(g)_h = 1\) if \(g = h\) and \(e(g)_h = 0\) otherwise. Let \(R\) be the \(v^2 \times v^2\) matrix indexed by the elements of \(G\) whose \(g\)-column is \(e(\oplus g)\), \(g \in G\). Note that \(R\) is symmetric and idempotent. We have \((H_i R)_{g,h} = \sum_{k \in G} a_{i,k \oplus g} e(h)_k = a_{i,h \oplus g}\). Hence, for each \(i\), the matrix \(H_i R\) is symmetric, i.e.
\[
H_i R = R H_i^t. \tag{3}
\]

Furthermore, a straightforward computation shows
\[
H_i H_j = H_j H_i \tag{4}
\]
for all \(i, j\). Using (2), (3), (4), it can be checked that
\[
\begin{pmatrix}
-H_1 & H_2 R & H_3 R & H_4 R \\
H_2 R & H_1 & H_1^t R & -H_1^t R \\
H_3 R & -H_1^t R & H_1 & H_1^t R \\
H_4 R & H_3 R & -H_1^t R & H_1 \\
\end{pmatrix}
\]
is a Hadamard matrix of order \(4v^2\). The regularity follows from the fact that each \(H_i\) has exactly \(\frac{1}{2}v(v-1)\) entries 1. □

The following result will be useful. See [3, Section 2.3, Thm. 2] for a proof.

**Result 2** An algebraic integer all of whose conjugates have absolute value 1 is a root of unity.

Note that Result 2 implies that any cyclotomic integer of absolute value 1 must be a root of unity since the Galois group of a cyclotomic field is abelian.
3 General Results

Throughout the rest of this paper, we use the following notation. Let \( q \equiv 3 \mod 4 \) be a prime power and let \( g \) be a generator of \( \mathbb{F}_{q^2} \). We denote the additive group of \( \mathbb{F}_{q^2} \) by \( G \). As before, we use \( \oplus \) and \( \ominus \) for the addition respectively subtraction in \( G \). The multiplication of \( \mathbb{F}_{q^2} \) is denoted by \( * \) to distinguish it from the group ring multiplication. Let \( \epsilon \) be a divisor of \( q^2 - 1 \) and \( f = (q^2 - 1)/\epsilon \). We set

\[
C_{\epsilon,k} = \{ g^t \epsilon^k : t = 0, \ldots, f - 1 \}, \quad k = 0, \ldots, \epsilon - 1,
\]

\[
L_j = C_{q+1,j}, \quad j = 0, \ldots, q,
\]

\[
S_j = L_j \cup \{0\}, \quad j = 0, \ldots, q,
\]

\[
H_i = C_{2(q+1),i}, \quad i = 0, \ldots, 2q + 1.
\]

The sets \( C_{\epsilon,k} \) are called \( \epsilon \)th cyclotomic classes. Xiang [10] calls the \( L_j \)'s lines and the \( H_i \)'s half-lines. The indices \( k, j, i \) are taken modulo \( \epsilon, q + 1, 2(q + 1) \) respectively. Note \( L_j^{(-1)} = L_j \) for all \( j \) and \( H_i + H_i^{(-1)} = L_i \) for all \( i \). Furthermore, we have \( S_i S_j = G \) for \( i \neq j \) and \( S_j^2 = q S_j \) for all \( j \).

**Lemma 3** Let \( A \subset \{0, \ldots, 2q + 1\}, B \subset \{0, \ldots, q\} \) with \(|A| + 2|B| = q\) such that \( a \not\equiv b \mod q + 1 \) for all \( a \in A, b \in B \). Let

\[
H = \sum_{i \in A} H_i \quad \text{and} \quad L = \sum_{j \in B} L_j.
\]

Then

\[
(H + L)(H + L)^{(-1)} = HH^{(-1)} - |B|(H + H^{(-1)}) + \gamma + \delta G
\]

for some \( \gamma, \delta \in \mathbb{Z}^+ \).

**Proof** Write \(|A| = \alpha\) and \(|B| = \beta\). Let \( i \) and \( j \) be distinct elements of \( A \cup B \), not both in \( A \). Then \( S_i \) and \( S_j \) are distinct lines since \( i \not\equiv j \mod q + 1 \) by assumption. Hence \( S_i S_j = G \). Using this fact, we get

\[
(H + L)(H + L)^{(-1)} = \left( \sum_{i \in A} H_i + \sum_{j \in B} L_j \right) \left( \sum_{i \in A} H_i^{(-1)} + \sum_{j \in B} L_j \right)
\]

\[
= \left( \sum_{i \in A} H_i \right) \left( \sum_{i \in A} H_i^{(-1)} \right) + \left( \sum_{i \in A} [H_i^{(-1)}] \right) \sum_{j \in B} L_j + \left( \sum_{j \in B} L_j \right)^2
\]

\[
= \left( \sum_{i \in A} H_i \right) \left( \sum_{i \in A} H_i^{(-1)} \right) + \left( -\alpha + \sum_{i \in A} S_i \right) \left( -\beta + \sum_{j \in B} S_j \right) + \left( -\beta + \sum_{j \in B} S_j \right)^2
\]

\[
= \left( \sum_{i \in A} H_i \right) \left( \sum_{i \in A} H_i^{(-1)} \right) - \beta \sum_{i \in A} S_i + R
\]
where

\[ R = \alpha \beta - \alpha \sum_{j \in B} S_j + \sum_{i \in A, j \in B} \alpha \beta G + \beta^2 - 2 \beta \sum_{j \in B} S_j + q \sum_{j \in B} S_j + \beta(\beta - 1)G \]

\[ = \alpha \beta - \alpha \sum_{j \in B} S_j + \alpha \beta G + \beta^2 - 2 \beta \sum_{j \in B} S_j + q \sum_{j \in B} S_j + \beta(\beta - 1)G \]

\[ = (\alpha \beta + \beta^2) + (\alpha \beta + \beta(\beta - 1))G + (-\alpha - 2 \beta + q) \sum_{j \in B} S_j \]

\[ = (\alpha \beta + \beta^2) + (\alpha \beta + \beta(\beta - 1))G. \]

This proves the assertion. □

**Lemma 4** Let \( e \) be the exact power of 2 dividing \( q + 1 \) and let \( t > 1 \) be a divisor of \( e \). Let \( \alpha < e \) be an odd number and set \( \beta = \frac{1}{2e}[qe - \alpha(q + 1)] \). Let \( A \subset \{0, ..., 2e - 1\} \) and \( B_0, ..., B_{t-1} \subset \{0, ..., q\} \) with \( |A| = \alpha, |B_0| = \cdots = |B_{t-1}| = \beta \) such that \( b \not\equiv a \mod e \) for all \( a \in A \) and \( b \in \cup_{i=0}^{t-1} B_i \). Set

\[ H = \sum_{i \in A} C_{2e,i}, \]

\[ M_r = \sum_{j \in B_r} L_j, \quad r = 0, ..., t - 1, \]

\[ D_r = g^\frac{r}{t} \ast (H + M_r), \quad r = 0, ..., t - 1. \]

Then \( |D_r| = q(q - 1)/2 \) for \( r = 0, ..., t - 1 \) and

\[ \sum_{r=0}^{t-1} D_r D_r^{(-1)} = \gamma + R \]

with \( \gamma \in \mathbb{Z}^+ \) where \( R \) is a linear combination of \((\xi \frac{T}{t})\)th cyclotomic classes.

**Proof** Note that \( H \) is a union of half-lines since \( C_{2e,i} = \sum_{j=0}^{q-1} H_{2ej+i} \). Let \( r \in \{0, ..., t-1\} \) be arbitrary. If \( H_k \) is a half-line in \( H \) and \( L_j \) is a line in \( M_r \), then \( j \not\equiv k \mod q + 1 \). Hence \( H \) and \( M_r \) are disjoint and we get \( |H + M_r| = \alpha(q^2 - 1)/2e + \beta(q - 1) = q(q - 1)/2 \) and \( |D_r| = q(q - 1)/2, r = 0, ..., t - 1 \). Using Lemma 3 we get

\[ \sum_{r=0}^{t-1} D_r D_r^{(-1)} = \sum_{r=0}^{t-1} \left( g^\frac{r}{t} \ast (H + M_r)(H + M_r)^{(-1)} \right) \]

\[ = \gamma_1 + \delta_1 G + \left( \sum_{r=0}^{t-1} g^\frac{r}{t} \right) \ast (HH^{(-1)} - \beta(H + H^{(-1)})) \]

for some \( \gamma_1, \delta_1 \in \mathbb{Z}^+ \). Note \( C_{2e,i} + C_{2e,-i} = C_{e,i} \) for all \( i \). Since \( H \) is a union of \((2e)\)th cyclotomic classes, this implies that \( HH^{(-1)} - \beta(H + H^{(-1)}) \) is a linear combination of \( e \)th cyclotomic classes. We conclude that \( \left( \sum_{r=0}^{t-1} g^\frac{r}{t} \right) \ast (HH^{(-1)} - \beta(H + H^{(-1)})) \) is a linear combination of \((\xi \frac{T}{t})\)th cyclotomic classes. □

The following is a generalization of [10, Thm. 2.3].
Corollary 5 Let \( q \equiv 3 \mod 4 \) be a prime power and let \( e \) be the exact power of 2 dividing \( q + 1 \). Choose \( t = e \) and define \( D_0, ..., D_{t-1} \) as in Lemma 4. Then \((D_0, ..., D_{t-1})\) is a difference family in the additive group of \( \mathbb{F}_{q^2} \) with parameters \( e, (q^2, \frac{1}{2}q(q-1), \frac{1}{2}q(q-2)) \).

Proof By Lemma 4 we have \( |D_r| = q(q-1)/2, r = 0, ..., t-1 \), and
\[
\sum_{r=0}^{t-1} D_r D_r^{(-1)} = \gamma + R
\]
with \( \gamma \in \mathbb{Z}^+ \) where \( R \) is multiple of \( G-0 \). This implies the assertion. \( \square \).

The case \( e = 4 \) of Corollary 5 is the most interesting because it yields new Hadamard matrices through Proposition 1.

Corollary 6 Let \( q \equiv 3 \mod 8 \) be a prime power, \( e = t = 4 \), and define \( H, M_0, M_1, M_2, M_3 \) as in Lemma 4 (here \( \alpha \in \{1, 3\} \)). Set
\[
D_r = g^r * (H + M_r), \quad r = 0, ..., 3.
\]
Then \((D_0, D_1, D_2, D_3)\) is a 4-(\(q^2, \frac{1}{2}q(q-1), q(q-2)\)) difference family in the additive group of \( \mathbb{F}_{q^2} \).

Remark 7 The case \( \alpha = 1 \) of Corollary 6 coincides with [10, Cor. 2.4] while the case \( \alpha = 3 \) is new.

The following Corollary addresses the case \( e = 8 \) and \( t = 4 \) of Lemma 4 which is the main subject of this paper.

Corollary 8 Let \( q \equiv 7 \mod 16 \) be a prime power, \( e = 8 \), \( t = 4 \) and define \( H, M_0, M_1, M_2, M_3 \) as in Lemma 4. Set
\[
D_r = g^{2r} * (H + M_r), \quad r = 0, ..., 3.
\]
Then \((D_0, D_1, D_2, D_3)\) is a 4-(\(q^2, \frac{1}{2}q(q-1), q(q-2)\)) difference family in \( G \) if and only if
\[
\rho(HH^{(-1)} - \beta(H + H^{(-1)})) = 0 \tag{5}
\]
where \( \rho \) is the quadratic character of \( \mathbb{F}_{q^2} \).

Proof By the proof of Lemma 4 we have \( \sum_{r=0}^{3} D_r D_r^{(-1)} = \gamma_1 + \delta G + T \) where
\[
T := (g^0 + g^\frac{3}{2} + g^\frac{5}{2} + g^3) * (HH^{(-1)} - \beta(H + H^{(-1)}))
\]
and the coefficients of \( T \) are constant on the set of squares of \( \mathbb{F}_{q^2} \) and constant on the set of nonsquares of \( \mathbb{F}_{q^2} \). Hence \( \rho(HH^{(-1)} - \beta(H + H^{(-1)})) = 0 \) if and only if \( T \) has constant coefficients on \( G \setminus \{0\} \). \( \square \)
4 Number theoretic preparations

Let \( q \equiv 7 \mod 16 \) be a prime power and let \( \rho \) be the quadratic character of \( \mathbb{F}_{q^2} \). From now on, we write \( C_i \) instead of \( C_{16,i} \). The following numbers play a crucial role in our construction.

\[
J_i = \sum_{x \in C_i} \rho(1 \otimes x), \quad i = 0, \ldots, 15.
\]

(6)

We take the indices \( i \) of \( J_i \) modulo 16. The \( J_i \)'s are multiples of Jacobsthal sums, cf. [2, 6.1.1]. Let \( g \) be a fixed generator of \( \mathbb{F}_{q^2} \) and let \( \chi \) be the multiplicative character of \( \mathbb{F}_{q^2} \) with \( \chi(g) = \exp(2\pi i/16) \).

Lemma 9 We have

\[
\begin{align*}
J_0 + J_8 &= (3q - 1)/4, \\
J_i + J_{i+8} &= 0 \quad \text{for } i = 1, 3, 5, 7, \text{ and} \\
J_i + J_{i+8} &= -(q + 1)/4 \quad \text{for } i = 2, 4, 6.
\end{align*}
\]

Proof Let \( S \) respectively \( N \) be the set of nonzero squares respectively nonsquares in \( \mathbb{F}_{q^2} \). Then \( S = \sum_{j=0}^{(q-1)/2} L_{2j} \) and \( N = \sum_{j=0}^{(q-1)/2} L_{2j+1} \). Furthermore, \( C_{8,i} = \sum_{k=0}^{(q-7)/8} L_{8k+i} \). Let \( i \in \{1, \ldots, 7\}, j \in \{0, \ldots, (q-1)/2\}, k \in \{0, \ldots, (q-7)/8\} \). By viewing \( L_{2j} \) and \( 1 \otimes L_{8k+i} \) as lines without 0 and 1 respectively in \( \mathbb{F}_{q^2} \), we see that

\[
\begin{align*}
|L_{2j} \cap (1 \otimes L_{8k+i})| &= \begin{cases} 
0 & \text{if } j = 0 \text{ or } 2j = 8k + i \\
1 & \text{in all other cases,}
\end{cases} \\
|L_{2j+1} \cap (1 \otimes L_{8k+i})| &= \begin{cases} 
0 & \text{if } 2j + 1 = 8k + i \\
1 & \text{in all other cases.}
\end{cases}
\end{align*}
\]

Let \( i \) be even, \( 2 \leq i \leq 14 \). We get

\[
J_i + J_{i+8} = \sum_{x \in C_i} \rho(1 \otimes x)
\]

\[
= \sum_{k=0}^{(q-7)/8} \sum_{x \in L_{8k+i}} \rho(1 \otimes x)
\]

\[
= \sum_{k=0}^{(q-7)/8} \sum_{j=0}^{(q-7)/8 (q-1)/2} (|S \cap (1 \otimes L_{8k+i})| - |N \cap (1 \otimes L_{8k+i})|)
\]

\[
= \sum_{k=0}^{(q-7)/8} \sum_{j=0}^{(q-7)/8 (q-1)/2} (|L_{2j} \cap (1 \otimes L_{8k+i})| - |L_{2j+1} \cap (1 \otimes L_{8k+i})|)
\]

\[
= \sum_{k=0}^{(q-7)/8} \left( \frac{q - 3}{2} - \frac{q + 1}{2} \right) = -\frac{q + 1}{4}.
\]

A similar computation shows \( J_i + J_{i+8} = 0 \) if \( i \) odd. Since \( \sum_{i=0}^{15} J_i = -1 \), we get \( J_0 + J_8 = -1 + 3(q + 1)/4 = (3q - 1)/4 \). □
We write $\zeta = \exp(2\pi i/16)$. Let $\rho$ be the quadratic character of $\mathbb{F}_{q^2}$ and let $\chi$ be the multiplicative character of $\mathbb{F}_{q^2}$ with $\chi(g) = \zeta$. Note that $\chi$ depends on the choice of the generator $g$ of $\mathbb{F}_{q^2}$. Therefore, we write $\chi = \chi_g$ when it is necessary to indicate this dependency. We can derive the values $J_i$ from the coefficients of the following Jacobi sum.

$$J = \sum_{x \in \mathbb{F}_{q^2}} \chi(x)\rho(1 \vartriangle x).$$

Note that $J$ also depends on the choice of $g$.

**Lemma 10** Write $J = \sum_{i=0}^{3} t_i \zeta^i$ with $t_i \in \mathbb{Z}$. Then

$$t_i = J_i - J_{i+8}, \quad i = 0, ..., 7. \tag{7}$$

*In particular, $t_0 \equiv 3 \mod 4$, $t_1 \not\equiv 0$ and $t_2 \equiv 0 \mod 4$.*

**Proof** Using $\zeta^8 = -1$ we get

$$J = \sum_{x \in \mathbb{F}_{q^2}} \chi(x)\rho(1 \vartriangle x) = \sum_{i=0}^{15} \sum_{x \in C_i} \zeta^i \rho(1 \vartriangle x) = \sum_{i=0}^{7} \zeta^i (J_i - J_{i+8}).$$

This implies (7) since $\{1, \zeta, ..., \zeta^7\}$ is an integral basis of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$.

By Lemma 9, $t_0 = 2J_0 - (3q - 1)/4$, $t_1 = 2J_1$ and $t_2 = 2J_2 + (q + 1)/4$. As $q \equiv 7 \mod 16$, the remaining assertions follow if we can show that $J_0$ is even and that $J_1$, $J_2$ are both odd. Recall that $C_i = \{g^{16i+t} : t = 0, ..., ([q^2 - 1]/16) - 1\}$ and $J_i = \sum_{x \in C_i} \rho(1 \vartriangle x)$. As $1 \in C_0$ and $1 \not\in C_i$ for $i = 1, 2$, we get $J_0 \equiv \frac{q^2 - 1}{16} - 1 \mod 2$ and $J_i \equiv \frac{q^2 - 1}{16} \equiv 1 \mod 2$ for $i = 1, 2$. Since $(q^2 - 1)/16$ is odd, $J_0$ is even and $J_1, J_2$ are odd. □

For $j \in \{1, 3, 5, ..., 15\}$ we define $\sigma_j \in \text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ by $\zeta^{\sigma_j} = \zeta^j$. Since $-1$ is a square in $\mathbb{F}_{q^2}$, it follows from [2, Thms. 2.1.4, 2.1.6] that $J^{\sigma_j} = J$. Since $\{1, \zeta, ..., \zeta^7\}$ is an integral basis of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$, this implies that there are integers $a, b, c, d$ such that

$$J = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5). \tag{8}$$

By Lemma 9, $a = t_0$ and $b = t_2$, so we obtain

$$a \equiv 3 \mod 4 \quad \text{and} \quad b \equiv 0 \mod 4. \tag{9}$$

Furthermore, by [2, Thm. 2.1.3] we have $|J|^2 = q^2$. This implies

$$q^2 = a^2 + 2(b^2 + c^2 + d^2), \tag{10}$$

$$2ab = c^2 - 2cd - d^2. \tag{11}$$

In order to gain more insights in the numbers $a, b, c, d$, we need to know how $q$ splits in $\mathbb{Q}(\zeta)$. Let $P_1$ be a prime ideal of $\mathbb{Q}(\zeta)$ above $q$. As $q \equiv 7 \mod 16$, $P_1^{q^{2r}} = P_1$ and $(q) = P_1P_2P_3P_4$ where $P_j = P_1^{q^{2j}}$, see [2, Section 11.1].
Lemma 11 Let $a, b, c, d$ be integers and $J' = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5)$. Suppose $b \equiv 0 \mod 4$, $|J'|^2 = q^2$ and $(J') \neq (q)$. Then

(i) $(J') = P^2(P^{\sigma_1})^2$ where $P$ is a prime ideal that contains $J'$ in $\mathbb{Q}(\zeta)$.

(ii) there exist integers $w, r, s, t$ such that $G = w + r(\zeta^2 - \zeta^6) + s(\zeta + \zeta^7) + t(\zeta^3 + \zeta^5)$, and $J' = \pm G^2(G^{\sigma_2})^2$.

Proof By assumption, $J' \mathcal{J}^r = q^2$. Hence we obtain

$$(J') = P_1^\alpha P_9^\beta P_3^\gamma P_1^\delta $$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}^+$ and $\alpha + \beta = \gamma + \delta = 2$. Since $(J') \neq (q)$, there exists $j$ such that

$$(J^{\sigma_j}) = P_1^2 P_3^2 \quad \text{or} \quad (J^{\sigma_j}) = P_1 P_3^2.$$

First we assume $(J^{\sigma_j}) = P_1 P_3 P_3^2$. Let $K$ be the subfield of $\mathbb{Q}(\zeta)$ fixed by $\sigma_7$ and $O_K$ be the ring of algebraic integers in $K$. Since $K$ has class number 1, the ideal $P_1 \cap K$ is generated by an element $G$. Define $G_2 := G^{\sigma_1}$. Note that $P_3 \cap K$ and $P_9 \cap K$ are generated by $G_3$ and $G_9$ respectively. Since $J^{\sigma_1}$ and $G_1 G_9 G_3^2$ generate the same ideal in $O_K$, we have $J^{\sigma_1} = \eta G_1 G_9 G_3^2$ for some unit $\eta$ in $O_K$. Moreover, as $P_1 \cap K$ has norm $q$, we have $G_1 G_3 G_9 G_11 = q$. Since $|J^{\sigma_1}|^2 = q^2$, we then have

$q^2 = \eta \bar{\eta}(G_1 G_9 G_3^2)^2 = \eta \bar{\eta}(G_1 G_9 G_3^2)(G_9 G_1 G_11^2) = \eta \bar{\eta} q^2$.

Hence $|\eta| = 1$. Result 2 implies that $\eta$ is a root of unity. Since $\pm 1$ are the only roots of unity in $O_K$, we get $J^{\sigma_1} = \pm G_1 G_9 G_3^2$. Note that

$q = G_1 G_3 G_9 G_11 \equiv w^4 + 2s^4 + 2t^4 \mod 4$.

Since $q \equiv 3 \mod 4$, this implies

$$w \equiv 1 \mod 2 \quad \text{and} \quad s + t \equiv 1 \mod 2.$$ (12)

Moreover, a straightforward computation shows that the coefficient of $\zeta^2 - \zeta^6$ in $G_1 G_9 G_3^2$ is

$$b_1 := 4s^2r^2 - 4w^2st - 4r^2t^2 - 2u^2w^2 + 2s^2w^2 + 8s^2rw + 8wrt^2 - 8r^2st.$$ Hence, $b_1 \equiv 2w^2(s^2 - t^2) \equiv 2(s + t) \equiv 2 \mod 4$ because of (12). Since $J' = \pm G_1 G_9 G_3^2$, this shows that the coefficient of $\zeta^2 - \zeta^6$ in $J'$ is $\equiv 2 \mod 4$. But the coefficient of $\zeta^2 - \zeta^6$ in $J'$ is $\pm b \equiv 0 \mod 4$, a contradiction. Hence $(J^{\sigma_1}) = P_1 P_3 P_3^2$ is impossible.

This shows $(J^{\sigma_j}) = P_1^2 P_3^2$. Now we get (i) by setting $P = P_1^{\sigma_1^{-1}}$. Finally, let $G$ be a generator of $P \cap K$. By applying a similar argument as before, we see that $J' = \pm G^2(G^{\sigma_2})^2$. □

Lemma 12 Let $a, b, c, d$ be the integers with

$$J = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5).$$

Then

$$a \equiv 15 \mod 16,$$ (13)

$$b \equiv 0 \mod 4.$$ (14)
This follows from Lemmas 9 and 10.

**Proof** By Lemma 10, \( J \neq \pm q \), \( a \equiv 3 \mod 4 \) and \( b \equiv 0 \mod 4 \). So it follows from Lemma 11 that

\[
a = \pm \left( w^4 + 2 s^4 - 8r^2 t^2 - 8s^2 r^2 - 8s^2 w r - 8s t^3 + 2 t^4 - 4 s^2 w^2 + 4r^4 + 16 s t w - 4 w^2 t^2 - 4 w^2 r^2 + 8 s^3 t + 4 s^2 t^2 + 8 w r t^2 \right).
\]

Thus \( a \equiv \pm (w^4 + 2 t^4 + 2 s^4) \equiv \pm 3 \mod 4 \) by (12). Since \( a \equiv 3 \mod 4 \), we conclude \( J = G^2(G^{\sigma_j})^2 \).

Observe that

\[-8 r^2 t^2 - 8 s^2 r^2 - 8 s^2 w r + 4r^4 - 4 w^2 r^2 + 8 w r t^2 = -8 r^2 (t^2 + s^2) - 8r(t^2 - s^2) + 4r^2 (r^2 - w^2).\]

By (12) again, \(-8r^2(t^2 + s^2) - 8r(t^2 - s^2) \equiv 0 \mod 16 \). Whereas for the term \( 4r^2(r^2 - w^2) \), either \( r^2 \) is a multiple of 4 or \( r^2 - w^2 \) is a multiple of 4 as \( w \) is odd. Hence,

\[
a \equiv w^4 + 2 s^4 - 8 s t^3 + 2 t^4 - 4 s^2 w^2 - 4 w^2 t^2 + 8 s^3 t + 4 s^2 t^2
\]

\[
\equiv w^4 + 2(s^4 + t^4) - 4 w^2 (t^2 + s^2)
\]

\[
\equiv 1 + 2 - 4 \equiv 15 \mod 16.
\]

\( \square \)

Now, we consider the converse of the above lemma.

**Lemma 13** Let \( q \equiv 7 \mod 16 \) be a prime. If \( a, b, c, d \) are integers satisfying (10), (11) and

\[
a \equiv 15 \mod 16, \quad b \equiv 0 \mod 4,
\]

then there is \( j \in \{1, 3, 9, 11\} \) with

\[
J = [a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5)]^{\sigma_j}.
\]

**Proof** Let \( J' = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5) \). By Lemma 11(i), there exist \( i, i' \) such that \( (J')^{\sigma_j} = P_i^{2}(P_{i'}^{\sigma_j})^2 \) and \( (J) = P_i^2(P_{i'}^{\sigma_j})^2 \). Therefore, we may assume \( (J')^{\sigma_j} = (J) \) for some \( j \in \{1, 3, 9, 11\} \). Using a similar argument as before, we conclude that \( J'^{\sigma_j} = \pm J \). The coefficients of 1 in \( J \) and \( J' \) are both \( \equiv 3 \mod 4 \), so \( J'^{\sigma_j} = J \). \( \square \)

**Lemma 14** Let \( a, b, c, d \) be the integers with

\[
J = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5).
\]

Then the values \( J_i \) are given by \( J_{7i} = J_i \) for all \( i \) (indices taken modulo 16) and the following table.

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>9</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>( J_i )</td>
<td>( \frac{3q-1}{8} + \frac{d}{2} )</td>
<td>( \frac{c}{2} )</td>
<td>( -\frac{q+1}{8} + \frac{b}{2} )</td>
<td>( \frac{d}{2} )</td>
<td>( -\frac{q+1}{8} - \frac{b}{2} )</td>
<td>( \frac{3q-1}{8} - \frac{a}{2} )</td>
<td>( -\frac{c}{2} )</td>
<td>( -\frac{d}{2} )</td>
<td></td>
</tr>
</tbody>
</table>

**Proof** This follows from Lemmas 9 and 10. \( \square \)

The terms \( C_i C_j^{(-1)} \) will play a crucial role in the verification of our construction. We can compute the quadratic character of these terms from the values \( J_i \).
Lemma 15 Write \( f = (q^2 - 1)/16 \). We have
\[
\rho(C_i C_j^{(-1)}) = (-1)^i f J_{j-i}.
\]

Proof We compute
\[
\rho(C_i C_j^{(-1)}) = \sum_{r,s=0}^{f-1} \rho(g^{16r+i} \ominus g^{16s+j}) = \sum_{r=0}^{f-1} \rho(g^{16r+i}) \sum_{s=0}^{f-1} \rho(1 \ominus g^{16(s-r)+j-i}) = \sum_{r=0}^{f-1} (-1)^i \sum_{t=0}^{f-1} \rho(1 \ominus g^{16t+j-i}) = (-1)^i f J_{j-i}.
\]

\[
\square
\]

5 Construction with three 16th power cyclotomic classes

Let \( q \equiv 7 \mod 16 \) be a prime. Recall that we write \( C_i \) instead of \( C_{16i} \). Set
\[
H = C_0 + C_1 + C_2.
\]

Furthermore, let \( B \) be any subset of \( \{0, \ldots, q\} \) with \( \beta = (5q - 3)/16 \) elements such that no element of \( B \) is \( \equiv 0, 1 \) or 2 mod 8 and let
\[
L = \sum_{j \in B} L_j.
\]

Finally, set
\[
D_i = g^{2i}(H + L), \quad i = 0, 1, 2, 3.
\]

We write \( \mathcal{D} = (D_0, D_1, D_2, D_3) \). Note that \( \mathcal{D} \) depends on the choice of the generator \( g \) of \( \mathbb{F}_{q^2} \).

Theorem 16 Let \( a, b, c, d \) be any integers with
\[
\begin{align*}
a &\equiv 15 \mod 16, \\
b &\equiv 0 \mod 4, \\
q^2 &= a^2 + 2(b^2 + c^2 + d^2), \\
2ab &= c^2 - 2cd - d^2
\end{align*}
\]

(the existence of \( a, b, c, d \) is guaranteed by (10), (11) and Lemma 12). If \( q = a \pm 2b \) and \( g \) is chosen suitably, then \( \mathcal{D} \) is a \( 4-(q^2, \frac{1}{2}q(q-1), q(q-2)) \) difference family in the additive group of \( \mathbb{F}_{q^2} \).

Proof By Lemma 13 we can choose the generator \( g \) of \( \mathbb{F}_{q^2} \) such that
\[
J = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5).
\]
Write \( f = (q^2 - 1)/16 \). Using Lemmas 14 and 15 we get
\[
\rho(HH^{(-1)}) = \sum_{i,j=0}^2 C_i C_j^{(-1)} = f \sum_{i,j=0}^2 (-1)^i J_{j-i} = f \frac{1}{8}(8b + 4a + q - 3).
\]
Moreover, we have \( \rho(H + H^{(-1)}) = 2f \) since \( \rho(C_i) = (-1)^i f \). We get
\[
\rho(HH^{(-1)} - \beta(H + H^{(-1)})) = \frac{f}{16}(16b + 8a + 2q - 6 - 2(5q - 3)) = \frac{1}{2}(2b + a - q).
\]
Hence, if \( q = a + 2b \) then \( D \) is a \( 4(q^2, \frac{1}{2}q(q-1), q(q-2)) \) difference family by Lemma 4.

Let \( s \) be an integer coprime to \( q^2 - 1 \) with \( s \equiv 11 \mod 16 \). Let \( \chi_{g^s} \) be the multiplicative character of \( F_{q^2} \) defined by \( \chi_{g^s}(g^r) = \zeta \). If we replace \( g \) by \( g^s \) then
\[
J = \sum_{x \in F_{q^2}} \chi_{g^s}(x) \rho(x) = \sum_{x \in F_{q^2}} \chi_g(x)^3 \rho(x) = \left[ \sum_{x \in F_{q^2}} \chi_g(x) \rho(x) \right]^{\sigma_3} = a - b(\zeta^2 - \zeta^6) - d(\zeta + \zeta^7) + c(\zeta^3 + \zeta^5).
\]
Hence, in this case the condition for \( D \) being a difference family becomes \( q = a - 2b \). □

**Remark 17** As the proof of Theorem 16 shows, “if \( g \) is chosen suitably” only means that we have to replace \( g \) by \( g^s \) if necessary where \( s \) is any integer with \( s \equiv 11 \mod 16 \), \( (q^2 - 1, s) = 1 \).

### 6 Construction with five 16th power cyclotomic classes

Let \( q \equiv 7 \mod 16 \) be a prime. Set
\[
H = C_0 + C_1 + C_2 + C_3 + C_7.
\]
Furthermore, let \( B \) be any subset of \{0, ..., q\} with \( \beta = (3q-5)/16 \) elements such that no element of \( B \) is \( \equiv 0, 1, 2, 3 \) or 7 mod 8 and let
\[
L = \sum_{j \in B} L_j.
\]
Set
\[ D_i = g^{2i}(H + L), \quad i = 0, 1, 2, 3. \]
Write \( D = (D_0, D_1, D_2, D_3) \).

**Theorem 18** Let \( a, b, c, d \) be any integers with
\[
\begin{align*}
    a &\equiv 15 \mod 16, \\
b &\equiv 0 \mod 4, \\
q^2 &= a^2 + 2(b^2 + c^2 + d^2), \\
2ab &= c^2 - 2cd - d^2
\end{align*}
\]
(the existence of \( a, b, c, d \) is guaranteed by (10), (11) and Lemma 12). If
\[ q = a + \delta_1 b + \delta_2 4c + \delta_1 \delta_2 4d \quad (17) \]
with \( \delta_i = \pm 1 \) and \( g \) is chosen suitably, then \( D \) is a 4-\((q^2, 1, 2q(q - 1), q(q - 2))\) difference family in the additive group of \( \mathbb{F}_{q^2} \).

**Proof** By Lemma 13 we can choose the generator \( g \) of \( \mathbb{F}_{q^2} \) such that
\[ J = a + b(\zeta^2 - \zeta^6) + c(\zeta + \zeta^7) + d(\zeta^3 + \zeta^5). \]
Let \( T = \{0, 1, 2, 3, 7\} \). Using Lemmas 14 and 15 we get
\[
\rho(HH^{(-1)}) = \sum_{i,j \in T} C_i C_j^{(-1)} = f \sum_{i,j \in T} (-1)^i J_{j-i} = f \sum_{i,j \in T} (-4a + 8b + 16c + 16d + q + 5).
\]
Moreover, we have \( \rho(H + H^{(-1)}) = -2f \). We get
\[
\rho(HH^{(-1)} - \beta(H + H^{(-1)})) = \frac{f}{16}(-8a + 16b + 32c + 32d + 2q + 10 + 2(3q - 5)) = \frac{1}{2}(-a + 2b + 4c + 4d + q).
\]
Hence, if \( q = a - 2b - 4c - 4d \) then \( D \) is a 4-\((q^2, \frac{1}{2} q(q - 1), q(q - 2))\) difference family by Lemma 4. The theorem now follows by replacing \( g \) by \( g^s \) if necessary where \( s \equiv 3, 9 \text{ or } 11 \mod 16 \) and \( (s, q^2 - 1) = 1 \). \( \square \)

**Remark 19** As the proof of Theorem 18 shows, “if \( g \) is chosen suitably” only means that we have to replace \( g \) by \( g^s \) if necessary where \( s \) is an integer with \( s \equiv 3, 9 \text{ or } 11 \mod 16 \) and \( (s, q^2 - 1) = 1 \).
7 Main Result

Combining Proposition 1, Lemma 12, Theorems 16 and 18 we get our main result.

**Theorem 20** Let \( q \equiv 7 \mod 16 \) be a prime. Then there are integers \( a, b, c, d \) with

\[
\begin{align*}
    a &\equiv 15 \mod 16, \\
    b &\equiv 0 \mod 4, \\
    q^2 &= a^2 + 2(b^2 + c^2 + d^2), \\
    2ab &= c^2 - 2cd - d^2.
\end{align*}
\]

If

\[
\begin{align*}
    q &= a \pm 2b \text{ or } \\
    q &= a + \delta_1 b + 4\delta_2 c + 4\delta_1 \delta_2 4d \text{ with } \delta_i = \pm 1,
\end{align*}
\]

then there is a regular Hadamard matrix of order \( 4q^2 \).

We call the Hadamard matrices satisfying (18) respectively (19) the **three-class family** respectively the **five-class family**. We believe that both families are infinite. In the following tables we give all primes \( q < 10^6 \) respectively \( q < 50000 \) for which Theorem 20 yields a three-class respectively a five-class Hadamard matrix of order \( 4q^2 \). We also list the corresponding values \( a, b, c, d \) and the choice of the generator \( g \) which gives the corresponding difference family according to Theorems 16 and 18. The values \( a, b, c, d \) were obtained with the help of Paul van Wamelen’s PARI-implementation [5] for the computation of Jacobi sums.

We use the following representation of \( \mathbb{F}_{q^2} \). Let \( k \) be the smallest positive integer such that \( h := x^2 + x + k \) is a primitive polynomial over \( \mathbb{F}_q \). Then \( \mathbb{F}_{q^2} \cong \mathbb{F}_q[x]/(h) \) and \( x \in \mathbb{F}_q[x]/(h) \) is a primitive element of \( \mathbb{F}_{q^2} \) (we write \( x \) instead of \( x + (h) \)). The value of \( k \) is provided in the following tables. An entry \( i \) in the \( g \)-column has the following meaning: For the generator \( g \) we take \( x^s \) where \( s \equiv i \mod 16 \) and \( (s, q^2 - 1) = 1 \).
Appendix 1: Table of parameters for the three-class family

<table>
<thead>
<tr>
<th>q</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>k</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-1</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>199</td>
<td>127</td>
<td>36</td>
<td>102</td>
<td>6</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>727</td>
<td>527</td>
<td>-100</td>
<td>-250</td>
<td>-230</td>
<td>31</td>
<td>11</td>
</tr>
<tr>
<td>4327</td>
<td>799</td>
<td>-1764</td>
<td>2058</td>
<td>1302</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>4999</td>
<td>4607</td>
<td>-196</td>
<td>14</td>
<td>-1358</td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>27239</td>
<td>-4513</td>
<td>-15876</td>
<td>-10206</td>
<td>2142</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>34807</td>
<td>22639</td>
<td>6084</td>
<td>11778</td>
<td>-13182</td>
<td>26</td>
<td>1</td>
</tr>
<tr>
<td>43159</td>
<td>-4273</td>
<td>-23716</td>
<td>-18634</td>
<td>-3542</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>55399</td>
<td>7967</td>
<td>-23716</td>
<td>7546</td>
<td>-29722</td>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>92647</td>
<td>26399</td>
<td>-33124</td>
<td>8918</td>
<td>-52598</td>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td>99527</td>
<td>11327</td>
<td>44100</td>
<td>-26670</td>
<td>47250</td>
<td>20</td>
<td>1</td>
</tr>
<tr>
<td>144967</td>
<td>31679</td>
<td>56644</td>
<td>-45458</td>
<td>68782</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>196247</td>
<td>192719</td>
<td>1764</td>
<td>18438</td>
<td>-18522</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>205879</td>
<td>64367</td>
<td>-70756</td>
<td>96026</td>
<td>69958</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td>226087</td>
<td>112799</td>
<td>56644</td>
<td>-125002</td>
<td>-11662</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>239631</td>
<td>151631</td>
<td>44100</td>
<td>82110</td>
<td>-92610</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>273719</td>
<td>247727</td>
<td>12996</td>
<td>81282</td>
<td>1026</td>
<td>19</td>
<td>1</td>
</tr>
<tr>
<td>281959</td>
<td>277727</td>
<td>-2116</td>
<td>-24334</td>
<td>-24242</td>
<td>24</td>
<td>11</td>
</tr>
<tr>
<td>390727</td>
<td>387199</td>
<td>1764</td>
<td>-37002</td>
<td>-42</td>
<td>33</td>
<td>1</td>
</tr>
<tr>
<td>390967</td>
<td>239</td>
<td>195364</td>
<td>-180778</td>
<td>-74698</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>431479</td>
<td>-56593</td>
<td>244036</td>
<td>-11362</td>
<td>178334</td>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>477767</td>
<td>-42433</td>
<td>-260100</td>
<td>114750</td>
<td>-180030</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>517927</td>
<td>272927</td>
<td>122500</td>
<td>-18450</td>
<td>218750</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>549719</td>
<td>-46513</td>
<td>298116</td>
<td>-56238</td>
<td>240786</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>606247</td>
<td>201247</td>
<td>-202500</td>
<td>-281250</td>
<td>-208350</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>679127</td>
<td>393359</td>
<td>142884</td>
<td>238518</td>
<td>-275562</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>694567</td>
<td>-20641</td>
<td>-357604</td>
<td>316342</td>
<td>114218</td>
<td>20</td>
<td>11</td>
</tr>
<tr>
<td>715639</td>
<td>119407</td>
<td>298116</td>
<td>389298</td>
<td>92274</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>737719</td>
<td>677167</td>
<td>30276</td>
<td>143202</td>
<td>-146334</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>830359</td>
<td>318287</td>
<td>256036</td>
<td>-474122</td>
<td>-61226</td>
<td>12</td>
<td>1</td>
</tr>
</tbody>
</table>

**Remark 21** There are exactly 356 primes $q < 3.9 \cdot 10^8$ satisfying the conditions of Theorem 16. Some further computational experiments suggest that for any $n > 2 \cdot 10^8$ there are at least $\frac{1}{8}n^{\frac{2}{3}}$ primes $q$ satisfying the conditions of Theorem 16.
## Appendix 2: Table of parameters for the five-class family

<table>
<thead>
<tr>
<th>q</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>k</th>
<th>g</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-1</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>23</td>
<td>-17</td>
<td>4</td>
<td>2</td>
<td>10</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>71</td>
<td>31</td>
<td>-28</td>
<td>10</td>
<td>34</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>151</td>
<td>47</td>
<td>28</td>
<td>46</td>
<td>-86</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>263</td>
<td>-97</td>
<td>-36</td>
<td>-78</td>
<td>150</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>359</td>
<td>-1</td>
<td>252</td>
<td>-6</td>
<td>30</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>599</td>
<td>463</td>
<td>-92</td>
<td>-134</td>
<td>-214</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>631</td>
<td>527</td>
<td>-68</td>
<td>-134</td>
<td>-194</td>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>919</td>
<td>-17</td>
<td>612</td>
<td>186</td>
<td>114</td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>2087</td>
<td>1759</td>
<td>124</td>
<td>478</td>
<td>-622</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>2423</td>
<td>-977</td>
<td>700</td>
<td>-190</td>
<td>1390</td>
<td>14</td>
<td>9</td>
</tr>
<tr>
<td>2503</td>
<td>-97</td>
<td>1700</td>
<td>-230</td>
<td>-430</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>4967</td>
<td>4639</td>
<td>-196</td>
<td>-782</td>
<td>-962</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6311</td>
<td>-1889</td>
<td>3100</td>
<td>-790</td>
<td>-2810</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>7879</td>
<td>-1921</td>
<td>3332</td>
<td>-3374</td>
<td>-2590</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td>8087</td>
<td>-3281</td>
<td>196</td>
<td>1918</td>
<td>-4858</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>10711</td>
<td>-3793</td>
<td>4508</td>
<td>-434</td>
<td>-5446</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>11447</td>
<td>79</td>
<td>-8036</td>
<td>-238</td>
<td>-938</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>11831</td>
<td>-5969</td>
<td>-4100</td>
<td>5230</td>
<td>-2830</td>
<td>21</td>
<td>9</td>
</tr>
<tr>
<td>12391</td>
<td>191</td>
<td>7100</td>
<td>-4810</td>
<td>-1790</td>
<td>26</td>
<td>1</td>
</tr>
<tr>
<td>13399</td>
<td>8143</td>
<td>-3708</td>
<td>2766</td>
<td>5934</td>
<td>28</td>
<td>11</td>
</tr>
<tr>
<td>14071</td>
<td>-433</td>
<td>9212</td>
<td>3094</td>
<td>2114</td>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td>19559</td>
<td>-5921</td>
<td>-9212</td>
<td>7490</td>
<td>-5726</td>
<td>23</td>
<td>9</td>
</tr>
<tr>
<td>20743</td>
<td>-10657</td>
<td>4700</td>
<td>-1390</td>
<td>11590</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>21767</td>
<td>-4801</td>
<td>10044</td>
<td>-8658</td>
<td>-7038</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>25463</td>
<td>-17</td>
<td>17444</td>
<td>4102</td>
<td>1750</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>30871</td>
<td>-2449</td>
<td>19012</td>
<td>-8050</td>
<td>-6874</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>31607</td>
<td>25199</td>
<td>-4284</td>
<td>-6978</td>
<td>-10722</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>32503</td>
<td>13423</td>
<td>5436</td>
<td>-10050</td>
<td>17538</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>32839</td>
<td>31679</td>
<td>-508</td>
<td>4574</td>
<td>4030</td>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>35527</td>
<td>-30721</td>
<td>-196</td>
<td>5138</td>
<td>-11522</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>41927</td>
<td>-16481</td>
<td>-17444</td>
<td>-17458</td>
<td>11578</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

**Remark 22** There are exactly 1401 primes $q < 3.9 \cdot 10^8$ satisfying the conditions of Theorem 18. Some further computational experiments suggest that for any $n > 2 \cdot 10^8$ there are at least $\frac{1}{2}n^{\frac{2}{3}}$ primes of $q$ satisfying the conditions of Theorem 18.
Appendix 3: Some sporadic examples

In the following, we chose $g = x$ as the generator of $\mathbb{F}_{q^2}$ where we use the representation of $\mathbb{F}_{q^2}$ described at the end of Section 7. For the following primes $q$ we obtain $4-(q^2, \frac{1}{2}q(q-1), q(q-2))$ difference families and hence regular Hadamard matrices of order $4q^2$. Note that when we use Corollary 8, we only need to specify the half-line part $H$ and verify (5) since $M_0, M_1, M_2,$ and $M_3$ can always be chosen such that the remaining condition is satisfied.

$q = 167$: Set $H = C_0 + C_1 + C_{13}$ in Corollary 8. Then (5) can be verified using $a = 31, b = 28, c = -106, d = -38$ (here $k = 5$).

$q = 311$: In this case, we set
\[
D_0 = C_0 + C_1 + C_2 + C_3 + C_{10} + L,
D_1 = C_0 + C_6 + C_7 + C_{10} + C_{13} + L',
D_2 = g^4 * D_0,
D_3 = g^4 * D_1
\]
such that $L, L'$ are unions of lines, $|D_i| = q(q-1)/2$ and each $D_i$ has coefficients 0,1 only. This construction can be verified by direct computation.

$q = 439$: Put $H = C_0 + C_1 + C_2 + C_3 + C_4 + C_5 + C_7$ in Corollary 8. Then (5) can be verified using $a = -337, b = 28, c = 166, d = 106$ (here $k = 23$).

$q = 1223$: Put $H = C_0 + C_1 + C_2 + C_6 + C_7 + C_{12} + C_{13}$ in Corollary 8. Then (5) can be verified using $a = 223, b = -700, c = -110, d = -470$ (here $k = 15$).

Appendix 4: Something negative

In [10], a $4-(q^2, \frac{1}{2}q(q-1), q(q-2))$ difference family is constructed for $q = 7$ by using $(q-1)$th and $2(q-1)$th cyclotomic classes. We tried to extend this to further prime powers $q \equiv 3 \mod 4$, but we already failed for $q = 11$. Note for $q = 11$ a brute force search already is impossible on a common PC within a reasonable amount of time. Hence we had to use a quite complicated method using character sums. We conjecture that our search shows that for $q = 11$ there is no $4-(q^2, \frac{1}{2}q(q-1), q(q-2))$ difference family $(D_0, D_1, D_2, D_3)$ in the additive group of $\mathbb{F}_{q^2}$ of the following form.

\[
D_i = \{0\} \bigcup_{j \in A_i} C_{20,j}
\]

where $A_i \subset \{0, ..., 19\}, |A_i| = 9, i = 0, 1, 2, 3$. 

17
Acknowledgement

We are grateful to Paul van Wamelen for letting us use his PARI-implementation for the computation of Jacobi sums. His program was very helpful in the discovery of our two families of Hadamard matrices. Furthermore, we thank two anonymous referees for useful suggestions concerning the exposition.

References


