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 $p \equiv 7 \bmod 16$ be a prime. Then there are integers a, b, c, d with $a \equiv 15 \bmod 16$, $b \equiv 0 \bmod 4$, $p^2 = a^2 + 2(b^2 + c^2 + d^2)$, 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 ± 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 $q \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 8$ 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 $q \equiv 7 \bmod 8$ have been known.

In the present paper, we obtain two putative infinite families of Hadamard matrices of order $4q^2$ with $q \equiv 7 \bmod 8$ prime. We believe that, for any large enough n, our constructions yield at least $\frac{5}{8}n^{\frac{2}{5}}$ primes $q < n$, $q \equiv 7 \bmod 16$ 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 χ is a multiplicative character of order 16 and ρ 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

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

has cardinality λ.

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 $h_i = 2D_i - G$. 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 $(H_i)_{g,h} = a_{i,h\ominus g}$. 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 $e(\ominus g)$, $g \in G$. Note that R is symmetric and idempotent. We have $(H_i R)_{g,h} = \sum_{k\in G} a_{i,k\ominus g} e(h)_k = a_{i,\,\ominus g \ominus h}$. 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

$$\begin{pmatrix} -H_1 & H_2 R & H_3 R & H_4 R \\ H_2 R & H_1 & H_4^t R & -H_3^t R \\ H_3 R & -H_4^t R & H_1 & H_2^t R \\ H_4 R & H_3^t R & -H_2^t R & H_1 \end{pmatrix}$$

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. $\Box$

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 e be a divisor of q^2-1 and $f=(q^2-1)/e$. We set

$$\begin{array}{lcll} C_{e,k} & = & \{g^{et+k} : t=0,...,f-1\}, & k=0,...,e-1, \\ L_j & = & C_{q+1,j}, & j=0,...,q, \\ S_j & = & L_j \cup \{0\}, & j=0,...,q, \\ H_i & = & C_{2(q+1),i}, & i=0,...,2q+1. \end{array}$$

The sets $C_{e,k}$ are called *eth 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 e, $q+1$, $2(q+1)$ respectively. Note $L_j^{(-1)} = L_j$ for all j and $H_i + H_i^{(-1)} = L_i$ for all i. Furthermore, we have $S_iS_j = G$ for $i \neq j$ and $S_j^2 = qS_j$ for all j.

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

$$H = \sum_{i \in A} H_i \quad \textit{and} \quad L = \sum_{j \in B} L_j.$$

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 $i \not\equiv j \bmod q+1$ by assumption. Hence $S_iS_j = G$. Using this fact, we get

$$\begin{aligned} (H+L)(H+L)^{(-1)} &= \left(\sum_{i\in A} H_i + \sum_{j \in B} L_j\right)\left(\sum_{i \in A} H_i^{(-1)} + \sum_{j\in B} L_j\right) \\ &= \left(\sum_{i\in A} H_i\right)\left(\sum_{i\in A} H_i^{(-1)}\right) + \left(\sum_{i\in A}\left[H_i + H_i^{(-1)}\right]\right)\sum_{j\in B} L_j + \left(\sum_{j\in B} L_j\right)^2 \\ &= \left(\sum_{i\in A} H_i\right)\left(\sum_{i\in A} H_i^{(-1)}\right) + \left(-\alpha + \sum_{i\in A} S_i\right)\left(-\beta + \sum_{j\in B} S_j\right) + \left(-\beta + \sum_{j\in B} S_j\right)^2 \\ &= \left(\sum_{i\in A} H_i\right)\left(\sum_{i\in A} H_i^{(-1)}\right) - \beta\sum_{i\in A} S_i \quad + R \end{aligned}$$

where

$$\begin{aligned}
R &= \alpha\beta - \alpha\sum_{j\in B} S_j + \sum_{i\in A, j\in B} S_iS_j + \beta^2 - 2\beta\sum_{j\in B} S_j + q\sum_{j\in B} S_j + \beta(\beta-1)G \\
&= \alpha\beta - \alpha\sum_{j\in B} S_j + \alpha\beta G + \beta^2 - 2\beta\sum_{j\in B} S_j + q\sum_{j\in B} S_j + \beta(\beta-1)G \\
&= (\alpha\beta+\beta^2) + (\alpha\beta+\beta(\beta-1))G + (-\alpha-2\beta+q)\sum_{j\in B} S_j \\
&= (\alpha\beta+\beta^2) + (\alpha\beta+\beta(\beta-1))G.
\end{aligned}$$

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 $b\not\equiv a \bmod e$ for all $a\in A$ and $b\in\cup_{r=0}^{t-1}B_r$. Set*

$$\begin{aligned}
H &= \sum_{i\in A} C_{2e,i}, \\
M_r &= \sum_{j\in B_r} L_j, \qquad r=0,...,t-1, \\
D_r &= g^{\frac{re}{t}} * (H+M_r), \quad r=0,...,t-1.
\end{aligned}$$

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

$$\sum_{r=0}^{t-1} D_rD_r^{(-1)} = \gamma + R$$

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

Proof Note that H is a union of half-lines since $C_{2e,i} = \sum_{j=0}^{\frac{q+1}{e}-1} H_{2ej+i}$. 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 $j\not\equiv k \bmod e$ by assumption. In particular, $j\not\equiv k \bmod q+1$. 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

$$\begin{aligned}
\sum_{r=0}^{t-1} D_rD_r^{(-1)} &= \sum_{r=0}^{t-1}\left(g^{\frac{re}{t}} * (H+M_r)(H+M_r)^{(-1)}\right) \\
&= \gamma_1 + \delta_1 G + \left(\sum_{r=0}^{t-1} g^{\frac{re}{t}}\right) * (HH^{(-1)} - \beta(H+H^{(-1)}))
\end{aligned}$$

for some $\gamma_1,\ \delta_1\in\mathbb{Z}^+$. Note $C_{2e,i} + C_{2e,i}^{(-1)} = C_{e,i}$ 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 eth cyclotomic classes. We conclude that $\left(\sum_{r=0}^{t-1} g^{\frac{re}{t}}\right) * (HH^{(-1)} - \beta(H+H^{(-1)}))$ is a linear combination of $(\frac{e}{t})$th cyclotomic classes. □

The following is a generalization of [10, Thm. 2.3].

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

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 $q \equiv 3 \bmod 8$ 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 $q \equiv 7 \bmod 16$ 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 ρ 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

$$T := (g^0 + g^{\frac{e}{4}} + g^{\frac{2e}{4}} + g^{\frac{3e}{4}}) * (HH^{(-1)} - \beta(H + H^{(-1)}))$$

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 $q \equiv 7 \bmod 16$ be a prime power and let ρ 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.

$$J_i = \sum_{x \in C_i} \rho(1 \ominus x), \quad i = 0, ..., 15. \tag{6}$$

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 χ be the multiplicative character of $\mathbb{F}_{q^2}$ with $\chi(g) = \exp(2\pi i/16)$.

Lemma 9 *We have*

$$\begin{array}{rcll} J_0 + J_8 & = & (3q-1)/4, & \\ J_i + J_{i+8} & = & 0 & \textit{for } i = 1,3,5,7, \textit{ and} \\ J_i + J_{i+8} & = & -(q+1)/4 & \textit{for } i = 2,4,6. \end{array}$$

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 $i \in \{1, ..., 7\}$, $j \in \{0, ..., (q-1)/2\}$, $k \in \{0, ..., (q-7)/8\}$. By viewing L_{2j} and $1 \ominus L_{8k+i}$ as lines without 0 and 1 respectively in $\mathbb{F}_{q^2}$, we see that

$$\begin{array}{rcl} |L_{2j} \cap (1 \ominus L_{8k+i})| & = & \begin{cases} 0 & \text{if } j = 0 \text{ or } 2j = 8k+i \\ 1 & \text{in all other cases,} \end{cases} \\ |L_{2j+1} \cap (1 \ominus L_{8k+i})| & = & \begin{cases} 0 & \text{if } 2j+1 = 8k+i \\ 1 & \text{in all other cases.} \end{cases} \end{array}$$

Let i be even, $2 \le i \le 14$. We get

$$\begin{aligned} J_i + J_{i+8} &= \sum_{x \in C_{8,i}} \rho(1 \ominus x) \\ &= \sum_{k=0}^{(q-7)/8} \sum_{x \in L_{8k+i}} \rho(1 \ominus x) \\ &= \sum_{k=0}^{(q-7)/8} (|S \cap (1 \ominus L_{8k+i})| - |N \cap (1 \ominus L_{8k+i})|) \\ &= \sum_{k=0}^{(q-7)/8} \sum_{j=0}^{(q-1)/2} (|L_{2j} \cap (1 \ominus L_{8k+i})| - |L_{2j+1} \cap (1 \ominus L_{8k+i})|) \\ &= \sum_{k=0}^{(q-7)/8} \left(\frac{q-3}{2} - \frac{q+1}{2} \right) = -\frac{q+1}{4}. \end{aligned}$$

A similar computation shows $J_i + J_{i+8} = 0$ if i odd. Since $\sum_{i=0}^{15} J_i = -1$, we get $J_0 + J_8 = -1 + 3(q+1)/4 = (3q-1)/4$. $\square$

We write $\zeta = \exp(2\pi i/16)$. Let ρ be the quadratic character of $\mathbb{F}_{q^2}$ and let χ be the multiplicative character of $\mathbb{F}_{q^2}$ with $\chi(g) = \zeta$. Note that χ 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.

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

Note that J also depends on the choice of g.

Lemma 10 *Write $J = \sum_{i=0}^{7} t_i\zeta^i$ with $t_i \in \mathbb{Z}$. Then*

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

In particular, $t_0 \equiv 3 \bmod 4$, $t_1 \neq 0$ and $t_2 \equiv 0 \bmod 4$.

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

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

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 $q \equiv 7 \bmod 16$, the remaining assertions follow if we can show that J_0 is even and that J_1, J_2 are both odd. Recall that $C_i = \{g^{16t+i} : t = 0, ..., [(q^2-1)/16] - 1\}$ and $J_i = \sum_{x\in C_i} \rho(1 \ominus x)$. As $1 \in C_0$ and $1 \notin C_i$ for $i = 1, 2$, we get $J_0 \equiv \frac{q^2-1}{16} - 1 \bmod 2$ and $J_i \equiv \frac{q^2-1}{16} \equiv 1 \bmod 2$ for $i = 1, 2$. Since $(q^2-1)/16$ is odd, J_0 is even and J_1, J_2 are odd. $\square$

For $j \in \{1, 3, 5, ..., 15\}$ we define $\sigma_j \in \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ 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 $J^{\sigma_7} = J$. 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

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

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 $q \equiv 7 \bmod 16$, $P_1^{\sigma_7} = P_1$ and $(q) = P_1P_3P_9P_{11}$ where $P_j = P_1^{\sigma_j}$, 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 $b \equiv 0 \bmod 4$, $|J'|^2 = q^2$ and $(J') \neq (q)$. Then*

(i) *$(J') = P^2 (P^{\sigma_3})^2$ 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 $J' = \pm G^2 (G^{\sigma_3})^2$.*

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

$$(J') = P_1^{\alpha} P_9^{\beta} P_3^{\gamma} P_{11}^{\delta}$$

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

$$(J'^{\sigma_j}) = P_1^2 P_3^2 \quad \text{or} \quad (J'^{\sigma_j}) = P_1 P_9 P_3^2.$$

First we assume $(J'^{\sigma_j}) = P_1 P_9 P_3^2$. Let K be the subfield of $\mathbb{Q}(\zeta)$ fixed by σ_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_1. Define $G_j := G_1^{\sigma_j}$. Note that $P_3 \cap K$ and $P_9 \cap K$ are generated by G_3 and G_9 respectively. Since J'^{σ_j} and $G_1 G_9 G_3^2$ generate the same ideal in O_K, we have $J'^{\sigma_j} = \eta G_1 G_9 G_3^2$ for some unit η in O_K. Moreover, as $P_1 \cap K$ has norm q, we have $G_1 G_3 G_9 G_{11} = q$. Since $|J'^{\sigma_j}|^2 = q^2$, we then have

$$q^2 = \eta\overline{\eta} |G_1 G_9 G_3^2|^2 = \eta\overline{\eta} (G_1 G_9 G_3^2)(G_9 G_1 G_{11}^2) = \eta\overline{\eta} q^2.$$

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

$$q = G_1 G_3 G_9 G_{11} \equiv w^4 + 2s^4 + 2t^4 \bmod 4.$$

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

$$w \equiv 1 \bmod 2 \quad \text{and} \quad s + t \equiv 1 \bmod 2. \tag{12}$$

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

$$b_1 := 4s^2r^2 - 4w^2st - 4r^2t^2 - 2w^2t^2 + 2s^2w^2 + 8s^2rw + 8wrt^2 - 8r^2st.$$

Hence, $b_1 \equiv 2w^2(s^2 - t^2) \equiv 2(s + t) \equiv 2 \bmod 4$ 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 $\equiv 2 \bmod 4$. But the coefficient of $\zeta^2 - \zeta^6$ in J' is $\pm b \equiv 0 \bmod 4$, a contradiction. Hence $(J'^{\sigma_j}) = P_1 P_9 P_3^2$ is impossible.

This shows $(J'^{\sigma_j}) = P_1^2 P_3^2$. Now we get (i) by setting $P = P_1^{\sigma_j^{-1}}$. Finally, let G be a generator of $P \cap K$. By applying a similar argument as before, we see that $J' = \pm G^2 (G^{\sigma_3})^2$. □

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

$$a \equiv 15 \bmod 16, \tag{13}$$
$$b \equiv 0 \bmod 4. \tag{14}$$

Proof By Lemma 10, $J \neq \pm q$, $a \equiv 3 \bmod 4$ and $b \equiv 0 \bmod 4$. So it follows from Lemma 11 that $J = \pm G^2 (G^{\sigma_3})^2$ for $G = w + r(\zeta^2 - \zeta^6) + s(\zeta + \zeta^7) + t(\zeta^3 + \zeta^5)$ where w, r, s, t are integers. Hence

$$\begin{aligned} a &= \pm(w^4 + 2s^4 - 8r^2t^2 - 8s^2r^2 - 8s^2wr - 8st^3 + 2t^4 - 4s^2w^2 \\ &\quad +4r^4 + 16strw - 4w^2t^2 - 4w^2r^2 + 8s^3t + 4s^2t^2 + 8wrt^2). \end{aligned}$$

Thus $a \equiv \pm(w^4 + 2t^4 + 2s^4) \equiv \pm 3 \bmod 4$ by (12). Since $a \equiv 3 \bmod 4$, we conclude $J = G^2(G^{\sigma_3})^2$. Observe that

$$-8r^2t^2 - 8s^2r^2 - 8s^2wr + 4r^4 - 4w^2r^2 + 8wrt^2 = -8r^2(t^2 + s^2) - 8r(t^2 - s^2) + 4r^2(r^2 - w^2).$$

By (12) again, $-8r^2(t^2 + s^2) - 8r(t^2 - s^2) \equiv 0 \bmod 16$. 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,

$$\begin{aligned} a &\equiv w^4 + 2s^4 - 8st^3 + 2t^4 - 4s^2w^2 - 4w^2t^2 + 8s^3t + 4s^2t^2 \\ &\equiv w^4 + 2(s^4 + t^4) - 4w^2(t^2 + s^2) \\ &\equiv 1 + 2 - 4 \equiv 15 \mod 16. \end{aligned}$$

□

Now, we consider the converse of the above lemma.

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

$$\begin{aligned} a &\equiv 15 \bmod 16, && (15) \\ b &\equiv 0 \bmod 4, && (16) \end{aligned}$$

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

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

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 $(J') = P_{i'}^2 (P_{i'}^{\sigma_3})^2$ and $(J) = P_i^2 (P_i^{\sigma_3})^2$. 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 $\equiv 3 \bmod 4$, so $J'^{\sigma_j} = J$. □

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.

i	0	1	2	3	4	6	8	9	11
J_i	$\frac{3q-1}{8} + \frac{a}{2}$	$\frac{c}{2}$	$-\frac{q+1}{8} + \frac{b}{2}$	$\frac{d}{2}$	$-\frac{q+1}{8}$	$-\frac{q+1}{8} - \frac{b}{2}$	$\frac{3q-1}{8} - \frac{a}{2}$	$-\frac{c}{2}$	$-\frac{d}{2}$

Proof This follows from Lemmas 9 and 10. □

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

$$\begin{aligned}
\rho(C_i C_j^{(-1)}) &= \sum_{r,s=0}^{f-1} \rho(g^{16r+i} \ominus g^{16s+j}) \\
&= \sum_{r=0}^{f-1} \rho(g^{16r+i}) \sum_{s=0}^{f-1} \rho(1 \ominus g^{16(s-r)+j-i}) \\
&= \sum_{r=0}^{f-1} (-1)^i \sum_{t=0}^{f-1} \rho(1 \ominus g^{16t+j-i}) \\
&= (-1)^i f J_{j-i}.
\end{aligned}$$

□

5 Construction with three 16th power cyclotomic classes

Let $q \equiv 7 \bmod 16$ be a prime. Recall that we write C_i instead of $C_{16,i}$. Set

$$H = C_0 + C_1 + C_2.$$

Furthermore, let B be any subset of $\{0, ..., q\}$ with $\beta = (5q-3)/16$ elements such that no element of B is $\equiv 0, 1$ or $2 \bmod 8$ 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*

$$\begin{aligned}
a &\equiv 15 \bmod 16, \\
b &\equiv 0 \bmod 4, \\
q^2 &= a^2 + 2(b^2 + c^2 + d^2), \\
2ab &= c^2 - 2cd - d^2
\end{aligned}$$

(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

$$\begin{aligned}
\rho(HH^{(-1)}) &= \sum_{i,j=0}^{2} C_i C_j^{(-1)} \\
&= f \sum_{i,j=0}^{2} (-1)^i J_{j-i} \\
&= \frac{f}{8}(8b + 4a + q - 3).
\end{aligned}$$

Moreover, we have $\rho(H + H^{(-1)}) = 2f$ since $\rho(C_i) = (-1)^i f$. We get

$$\begin{aligned}
\rho(HH^{(-1)} - \beta(H + H^{(-1)})) &= \frac{f}{16}(16b + 8a + 2q - 6 - 2(5q-3)) \\
&= \frac{1}{2}(2b + a - q).
\end{aligned}$$

Hence, if $q = a + 2b$ then $\mathcal{D}$ 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 $s \equiv 11 \bmod 16$. Let χ_{g^s} be the multiplicative character of F_{q^2} defined by $\chi_{g^s}(g^s) = \zeta$. If we replace g by g^s then

$$\begin{aligned}
J &= \sum_{x \in F_{q^2}} \chi_{g^s}(x)\rho(x) \\
&= \sum_{x \in F_{q^2}} \chi_g(x)^3 \rho(x) \\
&= \left[\sum_{x \in F_{q^2}} \chi_g(x)\rho(x)\right]^{\sigma_3} \\
&= a - b(\zeta^2 - \zeta^6) - d(\zeta + \zeta^7) + c(\zeta^3 + \zeta^5).
\end{aligned}$$

Hence, in this case the condition for $\mathcal{D}$ being a difference family becomes $q = a - 2b$. $\square$

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 $s \equiv 11 \bmod 16$, $(q^2-1, s) = 1$.

6 Construction with five 16th power cyclotomic classes

Let $q \equiv 7 \bmod 16$ 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 $7 \bmod 8$ and let

$$L = \sum_{j \in B} L_j.$$

Set

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

Write $\mathcal{D} = (D_0, D_1, D_2, D_3)$.

Theorem 18 *Let a, b, c, d be any integers with*

$$\begin{aligned} a &\equiv 15 \bmod 16, \\ b &\equiv 0 \bmod 4, \\ q^2 &= a^2 + 2(b^2 + c^2 + d^2), \\ 2ab &= c^2 - 2cd - d^2 \end{aligned}$$

(*the existence of a, b, c, d is guaranteed by* (10), (11) *and Lemma* 12). *If*

$$q = a + \delta_1 b + \delta_2 4c + \delta_1\delta_2 4d \tag{17}$$

with $\delta_i = \pm 1$ 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

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

Let $T = \{0, 1, 2, 3, 7\}$. Using Lemmas 14 and 15 we get

$$\begin{aligned} \rho(HH^{(-1)}) &= \sum_{i,j \in T} C_i C_j^{(-1)} \\ &= f \sum_{i,j \in T} (-1)^i J_{j-i} \\ &= \frac{f}{8}(-4a + 8b + 16c + 16d + q + 5). \end{aligned}$$

Moreover, we have $\rho(H + H^{(-1)}) = -2f$. We get

$$\begin{aligned} \rho(HH^{(-1)} - \beta(H + H^{(-1)})) &= \frac{f}{16}(-8a + 16b + 32c + 32d + 2q + 10 + 2(3q - 5)) \\ &= \frac{1}{2}(-a + 2b + 4c + 4d + q). \end{aligned}$$

Hence, if $q = a - 2b - 4c - 4d$ then $\mathcal{D}$ 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 $s \equiv 3, 9$ or $11 \bmod 16$ 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 $s \equiv 3, 9$ or $11 \bmod 16$ 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 $q \equiv 7 \bmod 16$ be a prime. Then there are integers a, b, c, d with*

$$\begin{aligned} a &\equiv 15 \bmod 16, \\ b &\equiv 0 \bmod 4, \\ q^2 &= a^2 + 2(b^2 + c^2 + d^2), \\ 2ab &= c^2 - 2cd - d^2. \end{aligned}$$

If

$$q = a \pm 2b \text{ or} \tag{18}$$

$$q = a + \delta_1 b + 4\delta_2 c + 4\delta_1\delta_2 4d \text{ with } \delta_i = \pm 1, \tag{19}$$

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 $s \equiv i \bmod 16$ and $(s, q^2 - 1) = 1$.

Appendix 1: Table of parameters for the three-class family

q	a	b	c	d	k	g
7	-1	4	2	2	3	1
199	127	36	102	6	6	1
727	527	-100	-250	-230	31	11
4327	799	-1764	2058	1302	10	11
4999	4607	-196	14	-1358	15	11
27239	-4513	-15876	-10206	2142	7	11
34807	22639	6084	11778	-13182	26	1
43159	-4273	-23716	-18634	-3542	3	11
55399	7967	-23716	7546	-29722	6	11
92647	26399	-33124	8918	-52598	14	11
99527	11327	44100	-26670	47250	20	1
144967	31679	56644	-45458	68782	6	1
196247	192719	1764	18438	-18522	7	1
205879	64367	-70756	96026	69958	12	11
226087	112799	56644	-125902	-11662	6	1
239831	151631	44100	82110	-92610	7	1
273719	247727	12996	81282	1026	19	1
281959	277727	-2116	-24334	-24242	24	11
390727	387199	1764	-37002	-42	33	1
390967	239	195364	-180778	-74698	10	1
431479	-56593	244036	-11362	178334	21	1
477767	-42433	-260100	114750	-180030	10	11
517927	272927	122500	-184450	218750	10	1
549719	-46513	298116	-56238	240786	11	1
606247	201247	-202500	-281250	-208350	10	11
679127	393359	142884	238518	-275562	5	1
694567	-20641	-357604	316342	114218	20	11
715639	119407	298116	389298	92274	11	1
737719	677167	30276	143202	-146334	6	1
830359	318287	256036	-474122	-61226	12	1

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 $\frac{1}{8}n^{\frac{2}{5}}$ primes q satisfying the conditions of Theorem 16.

Appendix 2: Table of parameters for the five-class family

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

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 $\frac{1}{2}n^{\frac{2}{5}}$ 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.

$\boldsymbol{q = 167}$: 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 $k = 5$).

$\boldsymbol{q = 311}$: In this case, we set

$$\begin{aligned} D_0 &= C_0 + C_1 + C_2 + C_3 + C_{10} + L, \\ D_1 &= C_0 + C_6 + C_7 + C_{10} + C_{13} + L', \\ D_2 &= g^4 * D_0, \\ D_3 &= g^4 * D_1 \end{aligned}$$

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.

$\boldsymbol{q = 439}$: Put $H = C_0 + C_1 + C_2 + C_3 + C_4 + C_6 + C_7$ in Corollary 8. Then (5) can be verified using $a = -337$, $b = 28$, $c = 166$, $d = 106$ (here $k = 23$).

$\boldsymbol{q = 1223}$: 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 $q \equiv 3 \bmod 4$, 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 $A_i \subset \{0, ..., 19\}$, $|A_i| = 9$, $i = 0, 1, 2, 3$.

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

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier: *A User's Guide to PARI-GP* (2000). Available at `http://pari.math.u-bordeaux.fr`.

[2] B.C. Berndt, R.J. Evans, K.S. Williams: *Gauss and Jacobi sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley (1998).

[3] Z.I. Borevich, I.R. Shafarevich: Number Theory. Academic Press, New York/San Francisco/London (1966).

[4] J.M. Goethals, J.J. Seidel: A skew Hadamard matrix of order 36. *J. Aust. Math. Soc.* **11** (1970), 343-344.

[5] P. van Wamelen: Jacobi sums over finite fields. *Acta Arith.* **102** (2002), 1-20.

[6] L.C. Washington: *Introduction to Cyclotomic Fields.* Graduate Texts in Math. **83**, Springer (1997).

[7] M.Y. Xia, G. Liu: An infinite class of supplementary difference sets and Williamson matrices. *J. Combin. Theory Ser. A* **58** (1991), 310-317.

[8] M.Y. Xia, G. Liu: A new family of supplementary difference sets and Hadamard matrices. *J. Stat. Plann. Inference* **51** (1996), 283-291.

[9] T. Xia, M.Y. Xia, J. Seberry: Regular Hadamard matrices, maximum excess and SBIBD. *Australas. J. Comb.* **27** (2003), 263-275.

[10] Q. Xiang: Difference families from lines and half lines. *Eur. J. Comb.* **19** (1998), 395-400.