New Restrictions on Possible Orders of Circulant Hadamard Matrices

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore

Bernhard Schmidt
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
Nanyang Technological University
Singapore 637371
Republic of Singapore

Abstract

We obtain several new number theoretic results which improve the field descent method. We use these results to rule out many of the known open cases of the circulant Hadamard matrix conjecture. In particular, the only known open case of the Barker sequence conjecture is settled.

1 Introduction

A **circulant Hadamard matrix of order v** is a square matrix of the form

$$H = \begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_v & a_1 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

with $a_i \in \{-1, 1\}$ for all i and $HH^T = vI$. No circulant Hadamard matrix of order larger than 4 has ever been found. This led Ryser [12, p. 134] to the following.

Conjecture 1.1 *No circulant Hadamard matrix of order larger than* 4 *exists.*

Conjecture 1.1 is roughly half a century old, but still unresolved - despite claims of the contrary which appear in the form of preprints or even published papers on a regular basis. We will settle a number of open cases of Conjecture 1.1 in this paper.

The following is a classical result [17].

Result 1.2 (Turyn) *If an Hadamard matrix of order v exists, then $v = 4u^2$ for some odd integer u which is not a prime power.*

A sequence $a_1, ..., a_v$, $a_i = \pm 1$, is called a **Barker sequence of length v** if

$$\left| \sum_{i=1}^{v-j} a_i a_{i+j} \right| \leq 1 \text{ for } j = 1, ..., v-1.$$

The following is well known, see [2, Chapter VI, §14].

Result 1.3 *If a Barker sequence of length $l > 13$ exists, then there is a circulant Hadamard matrix of order l.*

So, naturally there is also the following.

Conjecture 1.4 *There are no Barker sequences of length exceeding* 13.

Storer and Turyn [16] proved that there is no Barker sequence of odd length exceeding 13, but the case of even length is still open despite powerful partial results [5, 6, 13, 14, 17].

Curiously, there is only one known open case of Conjecture 1.4: $l = 4u^2$ with $u = 217520382953549$, see [8]. This case will be ruled out by our results on circulant Hadamard matrices.

The most powerful known results on Conjectures 1.1 and 1.4 were obtained by the so-called "field descent method", see [6, 13, 14]. It is this method we will improve upon in the present paper. To make full use of our improvements, we will combine them with results of Turyn [17], McFarland [10], and Chan [4].

2 Preliminaries

To state and prove our results on Conjecture 1.1, we will use the language of groups rings and difference sets. We first fix some notation. Let G be a finite group. 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 $B^{(-1)} := \sum_{g\in G} b_g g^{-1}$ and $|B| := \sum_{g\in G} b_g$. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ by linearity. For convenience, we write $\zeta_m = e^{2\pi i/m}$ for any integer m.

A **(v, k, λ, n)-difference set** in a finite group G of order v is a k-subset D of G such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The positive integer $n = k - \lambda$ is called the **order** of the difference set. For an introduction to difference sets, see [2, Chapter VI].

In the group ring language, difference sets can be characterized as follows [2, Chapter VI, Lemma 3.2].

Lemma 2.1 *Let D be a k-subset of a group G of order v. Then D is a (v, k, λ, n) difference set in G if and only if in the group ring $\mathbb{Z}[G]$ the following equation holds:*

$$DD^{(-1)} = n1_G + \lambda G.$$

In this paper, we mainly deal with **Hadamard difference sets**, i.e., difference sets with parameters $(v, k, \lambda, n) = (4u^2, 2u^2 - u, u^2 - u, u^2)$ where u is a positive integer. The following is well known, see [2, Chapter VI, §14].

Result 2.2 *If a circulant Hadamard matrix of order $4u^2$ exists, then there is an Hadamard difference set in the cyclic group of order $4u^2$.*

Next, we state a result concerning Hadamard difference sets, which essentially is a consequence of [10, Thm. 3.1].

Result 2.3 (McFarland) *Let G be an abelian group of order $4u^2w^2$ where u and w are odd and coprime, and assume the existence of an Hadamard difference set D in G. Let H be the subgroup of G of order $4u^2$. If*

$$\chi(D) \equiv 0 \pmod{w}$$

for all characters χ of G of order dividing $4u^2$, then there is an Hadamard difference set in H.

For convenience, we recall the following definition.

Definition 2.4 Let p be a prime, let m be a positive integer, and write $m = p^a m'$ with $(p, m') = 1$, $a \geq 0$. If there is an integer j with $p^j \equiv -1 \pmod{m'}$, then p is called *self-conjugate modulo m*. A composite integer n is called self-conjugate modulo m if every prime divisor of n has this property.

As we shall see, we need to deal with congruences of the form $X\overline{X} \equiv 0 \pmod{u}$. The first result in this direction is due to Turyn [17] and based on self-conjugacy.

Result 2.5 [17] *Assume that $A \in \mathbb{Z}[\zeta_m]$ satisfies*

$$A\overline{A} \equiv 0 \pmod{t^{2b}}$$

where b, t are positive integers, and t is self-conjugate modulo m. Then

$$A \equiv 0 \pmod{t^b}.$$

The next result concerns solving equation of the form $X\overline{X} = u^2$ in $\mathbb{Z}[\zeta_p]$ without using self-conjugacy. It is based on a method of Chan [4, Lemmas 2.3, 2.4].

Result 2.6 [14, Thm. 2.2.3] *Let $X \in \mathbb{Z}[\zeta_p]$ be a solution of $X\overline{X} = u^2$ where p is an odd prime with $(u, p) = 1$ and u is a positive integer. Write $u = \prod_{i=1}^{s} q_i^{a_i}$ where the q_i's are distinct primes. If*

$$\gcd(\mathrm{ord}_p(q_1), ..., \mathrm{ord}_p(q_s)) > \frac{2u(p-1)}{p},$$

then $X \equiv 0 \pmod{u}$.

The following two results are essential tools for the methods in the present paper. The first one is due to Kronecker. See [3, Section 2.3, Thm. 2] for a proof.

Result 2.7 [Kronecker] *An algebraic integer all of whose conjugates have absolute value 1 is a root of unity.*

Note that Result 2.7 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. A proof of the following result can be found in [14, Thm. 1.4.3], for instance.

Result 2.8 *Let p be a prime, and let m be a positive integer. Let P be a prime ideal above p in $\mathbb{Z}[\zeta_m]$, and write $m = p^a m'$ with $(m', p) = 1$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ satisfies $\sigma(\zeta_{m'}) = \zeta_{m'}^{p^j}$ for some positive integer j, then $\sigma(P) = P$.*

For later application, we record the following, which is a consequence of [13, Lem. 2.5].

Result 2.9 *Let $m > 1$ be an integer and $X \in \mathbb{Z}[\zeta_m]$ such that $X = \sum_{i=0}^{m-1} a_i \zeta_m^i$ with $0 \le a_i \le C$ for some constant C. If $X \equiv 0 \pmod{u}$ for some integer u, then*

$$u \le 2^{s-1} C$$

where s is the number of distinct prime divisors of m.

For a prime p and a positive integer t, let $\nu_p(t)$ be defined by $p^{\nu_p(t)} || \ t$, i.e. $p^{\nu_p(t)}$ is the highest power of p dividing t. By $\mathcal{D}(t)$ we denote the set of prime divisors of t. The following definition is required for the application of the field descent method [13].

Definition 2.10 *Let m, n be integers greater than 1. For $q \in \mathcal{D}(n)$ let*

$$m_q := \begin{cases} \prod_{p \in \mathcal{D}(m) \setminus \{q\}} p & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p \in \mathcal{D}(m) \setminus \{2,q\}} p & \text{otherwise.} \end{cases}$$

Set

$$\begin{aligned} b(2,m,n) &= \max_{q \in \mathcal{D}(n) \setminus \{2\}} \left\{ \nu_2(q^2-1) + \nu_2(\mathrm{ord}_{m_q}(q)) - 1 \right\} \text{ and} \\ b(r,m,n) &= \max_{q \in \mathcal{D}(n) \setminus \{r\}} \left\{ \nu_r(q^{r-1}-1) + \nu_r(\mathrm{ord}_{m_q}(q)) \right\} \end{aligned}$$

for primes $r > 2$ with the convention that $b(2,m,n) = 2$ if $\mathcal{D}(n) = \{2\}$ and $b(r,m,n) = 1$ if $\mathcal{D}(n) = \{r\}$. We define

$$F(m,n) := \gcd(m, \prod_{p \in \mathcal{D}(m)} p^{b(p,m,n)}).$$

The following result was proved in [13].

Result 2.11 *Assume $X\overline{X} = n$ for $X \in \mathbb{Z}[\zeta_m]$ where n and m are positive integers. Then*

$$X\zeta_m^j \in \mathbb{Z}[\zeta_{F(m,n)}]$$

for some j.

The next result is [14, Thm. 2.3.2].

Result 2.12 (F-bound) *Let $X \in \mathbb{Z}[\zeta_m]$ be of the form*

$$X = \sum_{i=0}^{m-1} a_i \zeta_m^i$$

with $0 \leq a_i \leq C$ for some constant C and assume that $n := X\overline{X}$ is an integer. Then

$$n \leq \frac{C^2 F(m,n)^2}{4\varphi(F(m,n))}.$$

3 Results

Theorem 3.1 *Assume the existence of a (v, k, λ, n) difference set in a cyclic group G. Let m be a positive integer such that m^2 divides n, and let w be a divisor of v such that m is self-conjugate modulo v/w. Then*

$$n \leq \frac{w^2 F(v/w, n/m^2)^2}{4\varphi(F(v/w, n/m^2))}.$$

Proof Let χ be character of G of order v/w. Then $\chi(D) \equiv 0 \pmod{m}$ by Result 2.5 since m is self-conjugate modulo v/w. Write $X = \chi(D)/m$. Then $|X|^2 = n/m^2$ and thus $X\zeta_{v/w}^j \in \mathbb{Z}[\zeta_F]$ for some integer j by Result 2.12 where $F = F(v/w, n/m^2)$. Hence $Z = \chi(D)\zeta_{v/w}^j = mX\zeta_{v/w}^j \in \mathbb{Z}[\zeta_F]$, too. Note that $Z = \sum_{i=0}^{v/w-1} a_i \zeta_{v/w}^i$ with $0 \leq a_i \leq w$ since χ has order v/w. Note that $|Z|^2 = |\chi(D)|^2 = n$. Hence the theorem follows by applying Theorem 2.12 to Z. □

Example 3.2 Let $u = 2838407 = 11 \cdot 13 \cdot 23 \cdot 863$. This is the seventh smallest value u such that the existence of a circulant Hadamard matrix of order $4u^2$ is still open, see [8]. We take $v = 4u^2$, $n = u^2$, $w = 2 \cdot 23^2$ and $m = 11$ in Theorem 3.1. Then $F(v/w, n/m^2) = 2 \cdot 11 \cdot 13^2 \cdot 863$ and get

$$(11 \cdot 13 \cdot 23 \cdot 863)^2 \leq \frac{(2 \cdot 23^2)^2 (2 \cdot 11 \cdot 13^2 \cdot 863)^2}{4 \cdot 10 \cdot 12 \cdot 13 \cdot 862},$$

a contradiction. Thus no circulant Hadamard matrix of order $4u^2$ exists for $u = 2838407$.

Remark 3.3 According to Mossinghoff [8], there are 1576 positive integers $u \leq 10^{13}$ for which the existence of a circulant Hadamard matrix of order $4u^2$ is still open. Theorem 3.1 rules out 135 of these cases. The details are provided in [15]. For each case, the triple $[u, w, m]$ is given which is needed for the application of Theorem 3.1 to rule out the existence of a circulant Hadamard matrix of order $4u^2$.

Lemma 3.4 *Let p be an odd prime and let a and u be positive integers. Suppose $X \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $|X|^2 = u^2$. Let w be a divisor of u which is self-conjugate modulo p. Let q_1,...,q_k be the prime divisors of u/w. If*

$$f := \gcd(\mathrm{ord}_p(q_1), ..., \mathrm{ord}_p(q_k)) > \frac{u^2}{w^2},$$

then $X \equiv 0 \pmod{u}$.

Proof If f is even, then u is self-conjugate modulo p which implies $X \equiv 0 \pmod{u}$ by Result 2.5. Hence we can assume that f is odd.

Since w is self-conjugate modulo p, we can write $X = wY$ for some $Y \in \mathbb{Z}[\zeta_{p^a}]$ by Lemma 2.5. If $w = u$, there is nothing to show, so we can assume $w < u$. Note $|Y|^2 = u^2/w^2$.

Let t be an integer with $\mathrm{ord}_{p^a}(t) = f$. Note that $t - 1 \not\equiv 0 \pmod{p}$ since $f > 1$. Define $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$ by $\sigma(\zeta_{p^a}) = \zeta_{p^a}^t$. Note that $t \equiv q_i^{\alpha_i} (\bmod p^a)$ for some $\alpha_i \in \mathbb{Z}$ for all i by the definition of f. Hence, by Result 2.8, all prime ideals above (Y) in $\mathbb{Z}[\zeta_{p^a}]$ are invariant under σ. Hence

$$\sigma(Y) = \delta\kappa Y \tag{1}$$

where $\delta = \pm 1$ and κ is some p^ath root of unity. Since $t - 1 \not\equiv 0 \pmod{p}$, there is an integer r with $r(t-1) \equiv -1 \pmod{p^a}$. Write $Z = Y\kappa^r$. Then

$$\sigma(Z) = \delta\kappa^{1+rt}Y = \delta\kappa^r Y = \delta Z.$$

Applying σ repeatedly to this equation, we get $Z = \sigma^f(Z) = \delta^f Z$. Thus $\delta = 1$ as f is odd. Hence $\sigma(Z) = Z$. Write

$$Z = \sum_{i=0}^{p^{a-1}} \zeta_{p^a}^i Z_i \tag{2}$$

with $Z_i \in \mathbb{Z}[\zeta_p]$. Since $\sigma(Z) = Z$, we have

$$\sum_{i=0}^{p^{a-1}-1} \zeta_{p^a}^i Z_i = \sum_{i=0}^{p^{a-1}-1} \zeta_{p^a}^{it} \sigma(Z_i). \tag{3}$$

Note that $\sigma(Z_i) \in \mathbb{Z}[\zeta_p]$ and that $\{1, \zeta_{p^a}, ..., \zeta_{p^a}^{p^{a-1}-1}\}$ is independent over $\mathbb{Z}[\zeta_p]$. Hence (3) shows that $Z_i \neq 0$ implies $Z_{it} \neq 0$ for all i where the indices are taken modulo p^{a-1}. Note that, by the definition of t, all orbits $\neq \{0\}$ of multiplication by t on $\mathbb{Z}/p^{a-1}\mathbb{Z}$ have length f. Hence, if there is $i > 0$ with $Z_i \neq 0$, then there are at least f indices j with $Z_j \neq 0$.

Recall that $|Z|^2 = |Y|^2 = u^2/w^2$. Again, since $\{1, \zeta_{p^a}, ..., \zeta_{p^a}^{p^{a-1}-1}\}$ is independent over $\mathbb{Z}[\zeta_p]$, this implies

$$\sum_{i=0}^{p^{a-1}-1} Z_i \overline{Z_i} = \frac{u^2}{w^2}. \tag{4}$$

Now assume $Z_i \neq 0$, and let $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_p/\mathbb{Q})$. Since $\prod_{\tau\in\Gamma} \tau(Z_i\overline{Z_i}) = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Z_i\overline{Z_i}) \geq 1$, we have

$$\sum_{\tau\in\Gamma} \tau(Z_i\overline{Z_i}) \geq p-1 \tag{5}$$

by the inequality of arithmetic and geometric means. Now let N be the number of indices i with $Z_i \neq 0$. Then

$$N(p-1) \leq \sum_{\tau\in\Gamma} \sum_{i=0}^{p^{a-1}-1} Z_i\overline{Z_i} = \frac{u^2(p-1)}{w^2}$$

by (4) and (5). Thus $N \leq u^2/w^2$. Above we have seen that $N \geq f$ if $Z_i \neq 0$ for some $i > 0$. Since $f > u^2/w^2$ by assumption, we infer $Z_i = 0$ for all $i > 0$. Hence $Z = Z_0 \in \mathbb{Z}[\zeta_p]$. Note

$$f > \frac{u^2}{w^2} \geq \frac{2u}{w} > \frac{2(p-1)u}{pw} \tag{6}$$

since $u/w \geq 2$. Because of $|Z|^2 = u^2/w^2$ and (6), Result 2.6 implies $Z \equiv 0 \pmod{u/w}$. Hence $X = wY = \kappa^{-r} wZ \equiv 0 \pmod{u}$. □

Theorem 3.5 *Let p be an odd prime, let a, m be positive integers with $(m,p) = 1$, and write $u = p^a m$. Let r be any divisor of m which is self-conjugate modulo p, and let $q_1, ..., q_s$ be the prime divisors of m/r. If*

$$f := \gcd(\mathrm{ord}_p(q_1), ..., \mathrm{ord}_p(q_k)) > \frac{u^2}{p^{2a}r^2} \text{ and } p^a > 2m, \tag{7}$$

then there is no circulant Hadamard matrix of order $4u^2$.

Proof Suppose D is a Hadamard difference set in a cyclic group G corresponding to a circulant Hadamard matrix of order $4u^2$. Let χ be a character of G of order p^{2a} or $2p^{2a}$. Then $\chi(D) \in \mathbb{Z}[\zeta_{p^{2a}}]$ and $|\chi(D)|^2 = u^2$ by (2.1).

Since $w := p^a r$ is self-conjugate modulo p by assumption, Lemma 3.4 implies $\chi(D) \equiv 0 \pmod{u}$, i.e., $\chi(D) = \pm\eta u$ for some p^{2a}th root of unity η.

Let W be the subgroup of order $2u^2$ of G, and write $D = A + Bg$ where $A, B \subset W$, and g is an element of order 4 in G. Let χ_1 be a character of G of order p^{2a} and let χ_2 be the unique character of G defined by $\chi_2(h) = \chi_1(h)$ for all $h \in W$ and $\chi_2(g) = -1$. Note that the order of χ_2 is $2p^{2a}$. By what we have shown above, $\chi_i(D) = \delta_i \eta_i u$ for some p^{2a}th roots of unity η_i and $\delta_i \in \{-1, 1\}$, $i = 1, 2$. Replacing D by Dk for some $k \in G$, if necessary, we can assume $\chi_2(D) = u$. Note that

$$\chi_1(D) = \chi_1(A) + \chi_1(B) \text{ and } \chi_2(D) = \chi_1(A) - \chi_1(B).$$

Hence $\chi_1(D) + \chi_2(D) = 2\chi_1(A)$ and thus $\delta_1\eta_1 u + u \equiv 0 \pmod{2}$. Since u is odd, this implies $\delta_1\eta_1 + 1 \equiv 0 \pmod{2}$ and thus $\eta_1 = 1$. Hence we have $\chi_2(D) = \chi_1(D)$ or $\chi_2(D) = -\chi_1(D)$. If $\chi_2(D) = \chi_1(D)$, then $2\chi_1(A)\chi_1(D) + \chi_2(D) = 2u$, and if $\chi_2(D) = -\chi_1(D)$, then $2\chi_1(B) = \chi_1(D) - \chi_2(D) = -2u$. In summary,

$$\chi_1(A) = u \text{ or } \chi_1(B) = -u.$$

Since $A, B \subset W$ the kernel of χ_1 on W has order $2u^2/p^{2a} = 2m^2$, we can write $\chi_1(A) = \sum_{i=0}^{p^{2a}-1} a_i \zeta_{p^{2a}}$ with $0 \le a_i \le 2m^2$, and $\chi_1(B)$ has a similar representation. Hence $u \le 2m^2$ by Result 2.9, i.e., $p^a \le 2m$, contradicting the assumptions. □

Example 3.6 Let $u = 217520382953549 = 13 \cdot 41 \cdot 2953 \cdot 138200401$. This corresponds to the only known open case of the Barker sequence conjecture, see [8]. Assume a circulant Hadamard matrix of order $4u^2$ exists. We take $p = 138200401$, $a = 1$, $m = 13 \cdot 41 \cdot 2953$, $r = 2953$ in Theorem 3.5. We find

$$f = \gcd(\mathrm{ord}_p(13), \mathrm{ord}_p(41)) = 959725 > 284089 = \frac{u^2}{p^{2a} r^2}$$

and $p = 138200401 > 3147898 = 2m$. Hence (7) is satisfied and we get a contradiction. Hence no circulant Hadamard matrix of order $4u^2$ exists.

Remark 3.7 Theorem 3.5 rules out 22 of the open cases of circulant Hadamard matrices of order $4u^2$ with $u \le 10^{13}$ in Mossinghoff's list [8]. The details are provided in [15]. For each case, the quadruple $[u, p, m, r]$ is given which is needed for the application of Theorem 3.10.

Corollary 3.8 *No Barker sequence of length L exists with $13 < L \leq 2 \cdot 10^{30}$.*

Proof If there is a Barker sequence of length L with $13 < L \leq 2 \cdot 10^{30}$, then $L = 4u^2$ with $u = 217520382953549$ by the results in [5, 6, 17] and a computer search described in [8]. But a Barker sequence of this length cannot exist by Example 3.6 since the existence of a Barker sequence of even length L implies the existence of a circulant Hadamard matrix of order L. □

Lemma 3.9 *Let $p \equiv 3 \pmod 4$ be a prime, and let u be an integer all of whose prime divisors are $\equiv 3 \pmod 4$. Let $X \in \mathbb{Z}[\zeta_{4p^a}]$ with $|X|^2 = u^2$. Then*

$$X\zeta_4^j \in \mathbb{Z}[\zeta_{p^a}]$$

for some integer j.

Proof Suppose q is a prime divisor of u such that $t := \mathrm{ord}_p(q)$ is even. Then $t \equiv 2 \pmod 4$ as $p \equiv 3 \pmod 4$. Hence $q^{t/2} \equiv -1 \pmod p$ and thus $q^{p^{a-1}t/2} \equiv -1 \pmod{p^a}$. Moreover $q^{p^{a-1}t/2} \equiv -1 \pmod 4$ since $q \equiv 3 \pmod 4$ and $p^{a-1}t/2$ is odd. We conclude $q^{p^{a-1}t/2} \equiv -1 \pmod{4p^a}$, i.e., q is self-conjugate modulo $4p^a$. Using Result 2.5, we conclude $X \equiv 0 \pmod q$. Repeating this argument, if necessary, we can write

$$X = wY \text{ with } |Y|^2 = u^2/w^2$$

where w is a positive integer dividing u, and all prime divisors of u/w are of odd order modulo p.

Now let q be a prime divisor of u/w, so $s := \mathrm{ord}_p(q)$ is odd. Then $q^{tp^{a-1}} \equiv 1 \pmod{p^a}$ and $q^{tp^{a-1}} \equiv 3 \pmod 4$ since $q \equiv 3 \pmod 4$ and tp^{a-1} is odd. Hence, by Result 2.8, the automorphism of $\mathbb{Q}(\zeta_{4p^a})$ defined by $\sigma(\zeta_{p^a}) = \zeta_{p^a}$ and $\sigma(\zeta_4) = -\zeta_4$ fixes all prime ideals of $\mathbb{Z}[\zeta_{4p^a}]$ above q. Since this holds for all prime divisors of u/w and $|Y|^2 = u^2/w^2$, we conclude that σ fixes the ideal $Y\mathbb{Z}[\zeta_{4p^a}]$. Hence $\sigma(Y) = \delta Y$ for some unit δ of $\mathbb{Z}[\zeta_{4p^a}]$ with $|\delta| = 1$. By Result 2.7, we have $\delta = \zeta_{p^a}^j i^k$ for some integers j, k, i.e.,

$$\sigma(Y) = \zeta_{p^a}^j \zeta_4^k Y. \tag{8}$$

Applying σ to (8), we get

$$Y = \sigma^2(Y) = \zeta_{p^a}^j(-\zeta_4)^k\sigma(Y) = \zeta_{p^a}^{2j}Y.$$

This implies $\zeta_{p^a}^j = 1$, i.e.,

$$\sigma(Y) = \zeta_4^k Y. \tag{9}$$

Now write $Y = A + B\zeta_4$ with $A, B \in \mathbb{Z}[\zeta_{p^a}]$. Then (9) implies

$$A - B\zeta_4 = \zeta_4^k(A + B\zeta_4). \tag{10}$$

If $k = 0$, then $B = 0$ by (10). If $k = 1$, then $A = -B$ by (10) and thus $Y = A(1 - \zeta_4)$. But then $|Y|^2 = 2|A|^2$, contradicting the assumption that u is odd. The cases $k = 2, 3$ are treated similarly. In summary, we have $A = 0$ or $B = 0$ in all cases. This concludes the proof. □

Theorem 3.10 *Let u be an integer all of whose prime divisors are congruent to 3 modulo 4 and let p be one these prime divisors. Let w be a divisor of u which is self-conjugate modulo p. Let q_1,...,q_k be the prime divisors $\neq p$ of u/w. If*

$$\gcd(\mathrm{ord}_p(q_1), ..., \mathrm{ord}_p(q_k)) > \frac{u^2}{w^2}, \tag{11}$$

then no circulant Hadamard matrix of order $4u^2$ exists.

Proof Suppose D is a Hadamard difference set in a cyclic group G corresponding to a circulant Hadamard matrix of order $4u^2$. If χ is a character of G of order dividing 4, then $\chi(D) \equiv 0 \pmod{u}$ by Result 2.5 since u is self-conjugate modulo 4.

Write $u = p^a m$ with $(p, m) = 1$. Let χ be a character of G of order $2^b p^c$ where $0 \leq b \leq 2$, $1 \leq c \leq 2a$. Then $\chi(D) \in \mathbb{Z}[\zeta_{4p^c}]$ and $|\chi(D)| = u^2$ by Result 2.1. Lemma 3.9 shows that $\chi(D)\eta \in \mathbb{Z}[\zeta_{p^c}]$. In view of (11), Lemma 3.4 implies $\chi(D) \equiv 0 \pmod{u}$.

In summary, we have shown $\chi(D) \equiv 0 \pmod{u}$ for all characters χ of G of order dividing $4p^{2a}$. Thus, by McFarland's Result 2.3, there is a Hadamard difference set in the cyclic group of order $4p^{2a}$. This contradicts Turyn's Result 1.2. □

Example 3.11 Let $u = 16401 = 3 \cdot 7 \cdot 11 \cdot 71$ which corresponds to the second smallest open case of circulant Hadamard matrices, see [8]. We take $p = 71$, $w = 7 \cdot 11 \cdot 71$ in Theorem 3.10. Then $u/w = 3$ and $\mathrm{ord}_p(3) = 35 > 9 = u^2/w^2$. Hence no circulant Hadamard matrix of order $4u^2$ exists by Theorem 3.10.

Remark 3.12 Theorem 3.10 rules out 63 cases of Mossinghoff's list [8] of open cases of the circulant Hadamard matrix conjecture. Please see [15] for the details. For each case, the triple $[u, p, r]$ is given where p and r are the numbers needed for the application of Theorem 3.10.

Acknowledgement Part of this research was done during a visit of the second author at the Unversität Augsburg who thanks Dieter Jungnickel for his kind hospitality.

References

[1] K.T. Arasu, S.L. Ma: Abelian difference sets without self-conjugacy. *Des. Codes Cryptogr.* **15** (1998), 223-230.

[2] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press 1999.

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

[4] W.K. Chan: Necessary Conditions for Menon Difference Sets. Designs, Codes and Cryptography **3** (1993), 147-154.

[5] S. Eliahou, M. Kervaire, B. Saffari: A new restriction on the length of Golay complementary sequences. *J. Comb. Theory Ser. A* **55** (1990), 49-59.

[6] K.H. Leung and B. Schmidt, The Field Descent Method. *Des. Codes Crypt.* **36** (2005), 171-188.

[7] S.L. Ma: *Polynomial addition sets.* Ph.D. thesis, University of Hong Kong, 1985.

[8] M. Mossinghoff: Wieferich pairs and Barker sequences, Des. Codes Cryptogr. **53** (2009), 149-163.

[9] R.L. McFarland: *On multipliers of abelian difference sets.* Ph.D. Dissertation, Ohio State University 1970.

[10] R.L. McFarland: Sub-difference sets of Hadamard difference sets. J. Comb. Theory A **54** (1990), 112-122.

[11] A. Pott: *Finite geometry and character theory.* Lecture Notes **1601**, Springer 1995.

[12] H.J. Ryser: *Combinatorial Mathematics.* Wiley, New York 1963.

[13] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* **12** (1999), 929-952.

[14] B. Schmidt: *Characters and cyclotomic fields in finite geometry.* Lecture Notes in Mathematics **1797**, Springer 2002.

[15] B. Schmidt: Data on Circulant Hadamard Matrices. `http://www3.ntu.edu.sg/home/Bernhard/CW/CW.html`

[16] J. Storer, R. Turyn: On binary sequences. *Proc. Amer. Math. Soc.* **12** (1961), 394-399.

[17] R.J. Turyn: Character sums and difference sets. Pacific J. Math. **15** (1965), 319-346.