The Anti-Field-Descent Method

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

The essential fact behind the so-called field-descent method is that certain cyclotomic integers necessarily are contained in relatively small fields and thus must have relatively small complex modulus. In this paper, we develop a method which reveals a complementary phenomenon: certain cyclotomic integers cannot be contained in relatively small fields and thus must have relatively large complex modulus.

This method, in particular, yields progress towards the circulant Hadamard matrix conjecture. In fact, we show that such matrices give rise to certain "twisted cyclotomic integers" which often have small complex modulus, but are not contained in small fields. Hence our "anti-field-descent" method provides new necessary conditions for the existence of circulant Hadamard matrices. The application of the new conditions to previously open cases of Barker sequences shows that there is no Barker sequence of length ℓ with $13 < \ell \le 4 \cdot 10^{33}$. Furthermore, 229,682 of the 237,807 known open cases of the Barker sequence conjecture are ruled out.

[*] Ka Hin Leung's research is supported by grant No. R-146-000-209-112, Ministry of Education, Singapore.

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 [11, p. 134] to the following.

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

The following is a classical result [15].

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

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

Storer and Turyn [14] proved that there is no Barker sequence of odd length exceeding 13. Furthermore, the following is well known, see [1, Chapter VI, §14].

Result 1.3. *The existence of a Barker sequence of length $\ell > 13$ implies the existence of a circulant Hadamard matrix of order ℓ.*

Thus there is also the following.

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

While Conjecture 1.4 has been settled in [14] for odd lengths, the case of even length is still open despite powerful partial results [6, 8, 12, 13, 15].

It turns out that the results of this paper are particularly useful for the study of Conjecture 1.4. In particular, we will show that there is no Barker sequence of length ℓ with $13 < \ell \leq 4 \cdot 10^{33}$. Moreover, we will settle all 19 open cases with $\ell \leq 10^{50}$ identified in [3] (note, however, that the list of open cases with $\ell \leq 10^{50}$ given in [3] is possibly incomplete; please refer to [3] for more details). Furthermore, in total, 237,807 open cases of Barker sequences of length $\ell \leq 10^{100}$ were identified in [3] (again, this list is possibly incomplete). We will rule out 229,682 of these 237,807 cases.

As the results of our paper are highly technical, we give an informal overview of the main ideas now. We assume that the reader is familiar with basic algebraic number theory, as treated in [2], for instance.

Write $\zeta_m = \exp(2\pi i/m)$. The elements of $\mathbb{Z}[\zeta_m]$ are called **cyclotomic integers**. Suppose there is a circulant Hadamard matrix of order $4u^2$, where $u > 1$ is an integer. It is well known that this implies the existence of a "flat" $X \in \mathbb{Z}[\zeta_{4u^2}]$ with $|X|^2 = u^2$ (by "flat" we mean that X can be written as $X = \sum a_i \zeta_m^i$ with small a_i's). Let p be the largest prime divisor of u. Let σ be the unique automorphism of $\mathbb{Q}(\zeta_{4u^2})$ of order p. The "field descent method" [8] shows that the ideal $X\mathbb{Z}[\zeta_{4u^2}]$ usually is *not* be invariant under σ if X is flat. However, in many cases, most prime ideals of $\mathbb{Z}[\zeta_{4u^2}]$ above u are invariant under σ. This can be used to show that $X^\sigma \overline{X}$ often is divisible by a relatively large integer, say w. Then $Y = X^\sigma \overline{X}/w$ is a cyclotomic integer. We call Y a "twisted cyclotomic integer". The properties of these twisted cyclotomic integers are the key to all our results. Note $|Y| = u^2/w$, which is relatively small if w is large.

We will show that the ideal $Y\mathbb{Z}[\zeta_{4u^2}]$ is not invariant under σ if the same is true for the ideal $X\mathbb{Z}[\zeta_{4u^2}]$. This means that Y is contained in $\mathbb{Q}(\zeta_{4u^2})$, but $Y\eta$ is not contained in the subfield $\mathbb{Q}(\zeta_{4u^2/p})$ for any root of unity η. The details of constructing such cyclotomic integers Y with relatively small complex modulus which live in relatively large fields will be worked out in Section 3. There are several ways of optimizing the construction of Y, which substantially strengthen and complicate the results. For instance, sometimes p has to be replaced by a smaller prime divisor of u or we have to use homomorphisms to start with an X which may not be that flat, but is contained in a proper subfield of $\mathbb{Q}(\zeta_{4u^2})$.

In Sections 4 and 5, we develop tools which provide necessary conditions for the existence of twisted cyclotomic integers Y. A major step is Theorem 4.5 which deals with the basic case $Y \in \mathbb{Q}(\zeta_q)$ where q is a prime power. This result is of independent interest and essentially solves the following number theoretic problem: Consider a "nontrivial" solution $X \in \mathbb{Z}[\zeta_q]$ of $|X|^2 = v^2$, which is contained in a subfield K of $\mathbb{Q}(\zeta_q)$. Find a sharp general lower bound for v in terms of the extension degree $[\mathbb{Q}(\zeta_q) : K]$.

The necessary condition for the existence of Y in Theorem 4.5 is so strong that it provides the desired contradictions in most applications we are interested in. Thus, after Theorem 4.5 has been established, it essentially suffices to concentrate on deriving necessary conditions for the existence of twisted cyclotomic integers in fields that are not of form $\mathbb{Q}(\zeta_q)$. This is the purpose of Theorem 5.4. The main tool for the proof of Theorem 5.4 is new estimates for Cassel's $\mathcal{M}$-function [4] that are obtained from Galois action on cyclotomic integers.

Finally, in Section 6, the number theoretic results of Sections 3 – 5 are applied to circulant Hadamard matrices and Barker sequences, and some computational results are presented.

2 Preliminaries

2.1 Group Rings, Characters, and Difference Sets

Let G be a finite (multiplicatively written) group of order v, let R be a ring, and let $R[G]$ denote group ring of G over R. Every $X \in R[G]$ can be written as $X = \sum_{g \in G} a_g g$ with $a_g \in R$. The a_g's are called the **coefficients** of X. We identify a subset S of G with the group ring element $\sum_{g \in S} g$. Let 1_G denote the identity element of G and let r be an integer. To simplify notation, we write r for the group ring element $s1_G$. Let s be an integer. We set $X^{(s)} = \sum_{g \in G} a_g g^s$.

We need some additional notation for the case $R = \mathbb{Z}[\zeta_m]$. Let t be an integer coprime to m. For $X = \sum_{g \in G} a_g g \in \mathbb{Z}[\zeta_m][G]$, we write $X^{(t)} = \sum a_g^\sigma g^t$ where σ is the automorphism of $\mathbb{Q}(\zeta_m)$ determined by $\zeta_m^\sigma = \zeta_m^t$.

For an abelian group G, we denote its group of complex characters by $\hat{G}$. The **trivial character** of G is the character χ_0 with $\chi_0(g) = 1$ for all $g \in G$. We always implicitly assume that characters are extended to group rings in the natural way, i.e., $\chi(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g \chi(g)$. The following is a standard result, see [1, Chapter VI, Lemma 3.5], for instance.

Result 2.1. *Let G be a finite abelian group and $X = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(X g^{-1})$$

for all $g \in G$.

To prove our results on Conjecture 1.1, we will use the language of difference sets. 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 [1, Chapter VI].

Using group rings and characters, difference sets in abelian groups can be characterized as follows [1, Chapter VI, Lemma 3.2].

Result 2.2. *Let D be a k-subset of a abelian group G of order v. Then D is a (v, k, λ, n) difference set in G if and only if*

$$DD^{(-1)} = n + \lambda G \tag{1}$$

in $\mathbb{Z}[G]$. Furthermore, (1) holds if and only if

$$|\chi(D)|^2 = n$$

for all nontrivial characters χ of G.

In this paper, we only 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 [1, Chapter VI, §14].

Result 2.3. *A circulant Hadamard matrix of order* $4u^2$ *exists if and only if there is a Hadamard difference set in the cyclic group of order* $4u^2$.

2.2 Number Theoretic Background

Throughout this paper, we assume basic algebraic number theory as treated in [2] or [7], for instance.

See [2, Section 2.3, Thm. 2] for a proof of the following result of Kronecker.

Result 2.4. *An algebraic integer all of whose conjugates have absolute value at most* 1 *is a root of unity.*

Note that Result 2.4 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.

To exploit Galois action on cyclotomic integers, we need the following relative integral bases of cyclotomic fields which are invariant under certain automorphisms.

Lemma 2.5. *Let* p *be an odd prime and let* $a\ge 2$ *be an integer. Let* t *be an integer with* $(t,p)=1$ *and write* $f=\mathrm{ord}_p(t)$. *If* $\mathrm{ord}_{p^a}(t)=f$, *then there is* $B\subset\{1,\dots,p^{a-1}-1\}$ *with* $|B|=(p^{a-1}-1)/f$ *such that*

$$\{1\}\cup\bigcup_{b\in B}\{\zeta_{p^a}^{bt^i}: i=0,\dots,f-1\} \tag{2}$$

is an integral basis of $\mathbb{Q}(\zeta_{p^a})$ *over* $\mathbb{Q}(\zeta_p)$.

Proof. Let $I\subset\mathbb{Z}$ with $|I|=p^{a-1}=[\mathbb{Q}(\zeta_{p^a}):\mathbb{Q}(\zeta_{p^{a-1}})]$. It is well known and straightforward to prove that $\{\zeta_{p^a}^j : j\in I\}$ is an integral basis of $\mathbb{Q}(\zeta_{p^a})$ over $\mathbb{Q}(\zeta_p)$ if and only if the elements of I are pairwise incongruent modulo p^{a-1}.

For $x=1,\dots,p^{a-1}-1$, let $g(x)$ be the unique integer with $g(x)\equiv x^t \pmod{p^{a-1}}$ and $1\le g(x)\le p^{a-1}-1$. Note $\mathrm{ord}_{p^{a-1}}(t)=f$, as $\mathrm{ord}_{p^a}(t)=\mathrm{ord}_p(t)=f$ by assumption. Thus every orbit of the map g on $\{1,\dots,p^{a-1}-1\}$ has length f. Let $B\subset\{1,\dots,p^{a-1}-1\}$ be a set with $|B|=(p^{a-1}-1)/f$ which contains exactly one representative of each of these orbits. Then the set

$$\{0\}\cup\bigcup_{b\in B}\{bt^i : i=0,\dots,f-1\}$$

has cardinality p^{a-1} and its elements are pairwise incongruent modulo p^{a-1}. This implies the set defined in (2) is an integral basis of $\mathbb{Q}(\zeta_{p^a})$ over $\mathbb{Q}(\zeta_p)$. □

Remark 2.6. The assumption $a \geq 2$ in Lemma 2.5 cannot be omitted. In fact, if $a = 1$, then $\bigcup_{b\in B}\{\zeta_p^{bt^i} : i = 0, \ldots, f-1\}$ (and not $\{1\} \cup \bigcup_{b\in B}\{\zeta_{p^a}^{bt^i} : i = 0, \ldots, f-1\}$) is an integral basis of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$.

The following result is a special case of [12, Thm. 2.1.4]. As it is needed repeatedly in this paper and the proof for this special case is easier than in the general case, we include a proof here for the convenience of the reader.

If η is a complex root of unity and k is the smallest positive integer with $\eta^k = 1$, we say that k is the **order** of η.

Result 2.7. *Let v, t be positive integers with $(v,t) = 1$. Let σ be the automorphism of $\mathbb{Q}(\zeta_v)$ determined by $\zeta_v^\sigma = \zeta_v^t$. Suppose $X \in \mathbb{Z}[\zeta_v]$ and $|X|^2$ is an integer. If all prime ideals of $\mathbb{Z}[\zeta_v]$ above $X\mathbb{Z}[\zeta_v]$ are invariant under σ, then there are roots of unity $\eta, \tau \in \mathbb{Z}[\zeta_v]$ with*

$$(X\tau)^\sigma = \pm\eta(X\tau) \tag{3}$$

such that every prime divisor of the order of η divides $t-1$.

Proof. As all prime ideals of $\mathbb{Z}[\zeta_v]$ above $X\mathbb{Z}[\zeta_v]$ are invariant under σ by assumption, we have $X^\sigma = \gamma X$ for some unit γ of $\mathbb{Z}[\zeta_v]$. Since $|X|^2$ is an integer, we have $|X^\sigma|^2 = |X|^2$. Thus γ is a root of unity by Result 2.4. Suppose p is a prime divisor of the order of γ which does not divide $t-1$. Write $\gamma = \zeta_{p^a}^j\gamma'$ where γ' is a root of unity whose order is not divisible by p. As $(p, t-1)$, there is an integer i with $j + i(t-1) \equiv 0 \pmod{p^a}$. Hence

$$(X\zeta_{p^a}^i)^\sigma = \gamma'\zeta_{p^a}^{j+it}X = \gamma'(X\zeta_{p^a}^i).$$

Repeating this argument, if necessary, we obtain (3). □

A proof of the following result can be found in [13, Thm. 1.4.3], for instance.

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

Definition 2.9. 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.

The following is a result of Turyn [15].

Result 2.10. *Suppose that $A \in \mathbb{Z}[\zeta_m]$ satisfies*

$$|A|^2 \equiv 0 \bmod n^2$$

for some positive integer n which is self-conjugate modulo m. Then $A \equiv 0 \bmod n$.

Note that Results 2.4 and 2.10 imply the following well-known fact: If $A \in \mathbb{Z}[\zeta_m]$ satisfies $|A|^2 = n^2$ and n is self-conjugate modulo m, then $A = \eta n$ for some root of unity η. We will need the following generalization.

Proposition 2.11. *Suppose that $A \in \mathbb{Z}[\zeta_m]$ satisfies $|A|^2 = n$, where n is an odd integer which is self-conjugate modulo m. Write $n = w^2 n'$ where $n' = \prod_{i=1}^k p_i$ is the square-free part of n and the p_i's are distinct primes ($k = 0$, i.e., $n' = 1$ is allowed). Then n' divides m and there is a root of unity η such that*

$$A = \eta w \prod_{i=1}^{k} G_{p_i}, \tag{4}$$

where

$$G_{p_i} = \sum_{x=1}^{p_i - 1} \left(\frac{x}{p}\right) \zeta_{p_i}^x$$

and $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol.

Proof. Let X, Y be any elements of $\mathbb{Z}[\zeta_m]$ satisfying $|X|^2 = |Y|^2 = n$.

Claim We have $Y = \eta X$ for some root of unity η.

Proof of the claim: As n is self-conjugate modulo m by assumption, all prime ideals of $\mathbb{Z}[\zeta_m]$ above $n\mathbb{Z}[\zeta_m]$ are invariant under complex conjugation by Result 2.8. Thus $|X|^2 = |Y|^2 = n$ implies that $X\mathbb{Z}[\zeta_m]$ and $Y\mathbb{Z}[\zeta_m]$ have the same prime ideal factorization. Hence $X = \epsilon Y$ for some unit ϵ. Note $|\epsilon| = 1$, as $|X|^2 = |Y|^2$. Hence ϵ is a root of unity by Result 2.4, and this proves the claim.

Suppose that p_i does not divide m for some i. Then the prime ideals of $\mathbb{Z}[\zeta_m]$ above $p_i\mathbb{Z}[\zeta_m]$ are unramified. Furthermore, as shown above, these prime ideals are invariant under complex conjugation. Hence each of these prime ideal occurs in the factorization of $p_i\mathbb{Z}[\zeta_m]$ to the first power and occurs in the factorization of $|A|^2\mathbb{Z}[\zeta_m] = A\bar{A}\mathbb{Z}[\zeta_m]$ to an even power. This contradicts $|A|^2 = n = w^2 \prod_{i=1}^k p_i$. Thus each p_i divides m, i.e., n' divides m.

Let $Y = \eta w \prod_{i=1}^k G_{p_i}$. Note that $|G_{p_i}|^2 = G_{p_i}$ for all i, as G_{p_i} is a quadratic Gauss sum (see [7, Prop. 8.2.2, p. 92]). Hence $|Y|^2 = w^2 \prod_{i=1}^k p_i = n = |A|^2$ and (4) follows from the claim. □

We now recall some results of Cassels [4] which will be needed to derive necessary conditions on the existence of twisted cyclotomic integers. For $X \in \mathbb{Z}[\zeta_m]$, let

$$\mathcal{M}(X) = \frac{1}{\varphi(m)} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} (X\overline{X})^\sigma,$$

where φ denotes the Euler totient function. Note

$$\mathcal{M}(X) \geq 1 \tag{5}$$

for $X \neq 0$ by the inequality of geometric and arithmetic means, since $\prod (X\overline{X})^\sigma \geq 1$. The following was proved in [4].

Result 2.12. *Let $X \in \mathbb{Z}[\zeta_m]$. Let p be a prime divisor of m and write $m = p^a m'$ with $(p, m') = 1$.*

(a) Supppose $a > 1$ and write $X = \sum_{i=0}^{p^{a-1}-1} X_i \zeta_{p^a}^i$ with $X_i \in \mathbb{Z}[\zeta_{pm'}]$. Then

$$\mathcal{M}(X) = \sum_{i=0}^{p^{a-1}-1} \mathcal{M}(X_i).$$

(b) Suppose $a = 1$ and write $X = \sum_{i=0}^{p-1} X_i \zeta_p^i$ with $X_i \in \mathbb{Z}[\zeta_{m'}]$. Then

$$(p-1)\mathcal{M}(X) = \sum_{i<j}^{p-1} \mathcal{M}(X_i - X_j).$$

For a prime q, let $\mathbb{F}_q$ denote the field of order q. Let χ be a multiplicative character of $\mathbb{F}_q$. The Gauss sum $G(\chi)$ is defined by

$$G(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x) \zeta_q^x.$$

Note that this definition uses the convention $\chi(0) = 0$. For a proof of the following result, see [12, Thm. 2.2.2].

Result 2.13. *Let q be an odd prime and let b, w be positive integers with $(w, q) = 1$. Suppose $X \in \mathbb{Z}[\zeta_{q^b w}]$ satisfies $|X|^2 = q^c$ for some positive integer c. Then there is an integer j such that*

$$X\zeta_{q^b w}^j \in \mathbb{Z}[\zeta_w]$$

or

$$X\zeta_{q^b w}^j = G(\chi)Z,$$

where $Z \in \mathbb{Z}[\zeta_w]$ and χ is a multiplicative character of $\mathbb{F}_q$. Furthermore, $|Z|^2 = q^{c-1}$.

2.3 A Bound on the Complex Modulus of Character Sums

Suppose D is a difference set of order n in an abelian group G. Let χ be a nontrivial character of G. By Result 2.2, the character sum $\chi(D) = \sum_{d \in d} \chi(d)$ has squared complex modulus n.

The field descent method developed in [8, 12, 13] provides upper bounds on the complex modulus of character sums and thus yields necessary conditions for the existence of difference sets. The following result can be obtained by the field descent approach and, in fact, is implicitly contained in [8]. For the convenience of the reader, we include a self-contained proof just for the situation we need, which is substantially simpler than the general version in [8].

Result 2.14. *Let $G = V \times H$ be an abelian group where $(|V|, |H|) = 1$, $V = \langle g\rangle$ is cyclic of order v, and H is an abelian group of exponent h^*. Let p be an odd prime such that $v \equiv 0 \pmod{p^2}$. Let n be a positive integer coprime to $|H|$, and let D be an element of $\mathbb{Z}[G]$ with whose coefficients all lie in the interval $[0, C]$. Suppose that, for every character χ of G with $\chi(g) = \zeta_v$, we have*

$$|\chi(D)|^2 = n \tag{6}$$

and

$$\chi(D)\eta_\chi \in \mathbb{Z}[\zeta_{vh^*/p}] \tag{7}$$

for some root of unity η_χ (depending on χ). Then

$$n \le \frac{|H|v^2C^2}{4p\varphi(v)}.$$

Proof. Let p^a be the largest power of p dividing v and write $v = p^a w$. Note that $a \ge 2$, as $v \equiv 0 \pmod{p^2}$ by assumption. Let t be an integer with $\mathrm{ord}_{p^a}(t) = p$ and $t \equiv 1 \pmod{wh^*}$ and let σ be the automorphism of $\mathbb{Q}(\zeta_{vh^*})$ determined by $\zeta_{vh^*}^\sigma = \zeta_{vh^*}^t$. Note that the fixed field of σ is $\mathbb{Q}(\zeta_{vh^*/p})$. Hence, by (7), for every character χ of G with $\chi(g) = \zeta_v$, the ideal $\chi(D) \in \mathbb{Z}[\zeta_{vh^*/p}]$ is invariant under σ. As $\chi(D)\chi(D^{(-1)}) = |\chi(D)|^2 \equiv 0 \pmod{n}$ by (6), we conclude

$$\chi(D)^\sigma\overline{\chi(D)} \equiv 0 \pmod{n}. \tag{8}$$

Recall that g is a generator of V and let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_v][H]$ be the homomorphism determined by $\rho(g) = \zeta_v$ and $\rho(h) = h$ for $h \in H$. Note that $\chi(D^{(t)}) = \chi(D)^\sigma$ for all characters χ of G. Thus (8) implies

$$\chi(D^{(t)}D^{(-1)}) = \chi(D)^\sigma\overline{\chi(D)} \equiv 0 \pmod{n}$$

for every character χ of G with $\chi(g) = \zeta_v$. By the definition of ρ, this implies

$$\chi(\rho(D)^{(t)}\rho(D)^{(-1)}) \equiv 0 \pmod{n} \tag{9}$$

for all characters χ of H (recall that $\rho(D)$ is an element of $\mathbb{Z}[\zeta_v][H]$). As $(n, |H|) = 1$ by assumption, Result 2.1 and (9) imply

$$\rho(D)^{(t)}\rho(D)^{(-1)} \equiv 0 \pmod{n}. \tag{10}$$

Write $\rho(D)^{(t)}\rho(D)^{(-1)} = nE$ with $E \in \mathbb{Z}[\zeta_v][H]$. By (6), we have $\chi(EE^{(-1)}) = |\chi(E)|^2 = 1$ for all characters χ of H. Hence $EE^{(-1)} = 1$ by Result 2.1.

Write $E = \sum_{h\in H} e_h h$ with $e_h \in \mathbb{Z}[\zeta_v]$. As $EE^{(-1)} = 1$, we have

$$\sum_{h\in H} |e_h|^2 = 1. \tag{11}$$

This implies that, for all $h \in H$, every conjugate of e_h has absolute value at most 1. By Result 2.4, one of the e_h's must be a root of unity and all other e_h's must be zero. We conclude $E = \pm\zeta_v^j k$ for some integer j and $k \in H$.

Recall $\rho(D)^{(t)}\rho(D)^{(-1)} = nE$. Note that $\rho(D)\rho(D)^{(-1)} = n$ by (6) and Result 2.1. Using $E = \pm\zeta_v^j k$, we conclude

$$\rho(D)^{(t)} = \rho(D)^{(t)}\rho(D)\rho(D)^{(-1)}n^{-1} = E\rho(D) = \delta\zeta_v^j k\rho(D). \tag{12}$$

with $\delta = \pm 1$. Write $\zeta_v^j = \zeta_{p^a}^r\zeta_w^s$. By the definition of t, we have $t^p \equiv 1 \pmod{vh^*}$ and thus $\rho(D)^{(t^p)} = \rho(D)$. Using (12) repeatedly, we get

$$\rho(D) = \rho(D)^{(t^p)} = \delta^p\zeta_{p^a}^{r(t^p-1)/(t-1)}\zeta_w^{sp}k^p\rho(D).$$

Multiplying this equation with $\rho(D)^{(-1)}$ and using $\rho(D)\rho(D)^{(-1)} = n$, we get

$$\delta^p\zeta_{p^a}^{r(t^p-1)/(t-1)}\zeta_w^{sp}k^p = 1. \tag{13}$$

As $k \in H$ and $(p, |H|) = 1$, this implies $k = 1$. Furthermore (13) implies $(\delta\zeta_w^s)^p = 1$, as $(2w, p) = 1$. This, in turn, implies $\delta\zeta_w^s = 1$. Hence (13) simplifies to

$$\zeta_{p^a}^{r(t^p-1)/(t-1)} = 1. \tag{14}$$

As $\mathrm{ord}_{p^a}(t) = p$, we have $t \equiv 1 \pmod{p}$. Write $t = 1 + p^c x$ where p^c is the largest power of p dividing $t-1$. We have $c \geq 1$, as $t \equiv 1 \pmod{p}$. Moreover, by the Binomial Theorem, $t^p \equiv (1+p^c x)^p \equiv 1 + p^{c+1}x \pmod{p^{2c+1}}$, as p is odd. Thus the largest power of p dividing $t^p - 1$ is p^{c+1}. Hence p^2 does not divide $(t^p-1)/(t-1)$. Thus $r \equiv 0 \pmod{p^{a-1}}$ by (14). In summary, we have shown that (12) implies

$$\rho(D)^{(t)} = \zeta_{p^a}^{r'p^{a-1}}\rho(D)$$

for some integer r'. As $\mathrm{ord}_{p^a}(t) = p$, we have $t - 1 \not\equiv 0 \pmod{p^a}$ and thus there is an integer d with $(t-1)d + r'(p^{a-1}) \equiv 0 \pmod{p^a}$. Hence

$$(\zeta_{p^a}^d\rho(D))^{(t)} = \zeta_{p^a}^{td+r'p^{a-1}}\rho(D) = \zeta_{p^a}^d\rho(D). \tag{15}$$

Write

$$Y = \zeta_{p^a}^d\rho(D) = \sum_{h\in H} Y_h h$$

with $Y_h \in \mathbb{Z}[\zeta_{p^a w}]$. Note that (15) implies $Y_h^\sigma = Y_h$ and thus $Y_h \in \mathbb{Z}[\zeta_{p^{a-1}w}]$ for all $h \in H$.

Now write $D = \sum_{h\in H} D_h h$ with $D_h \in \mathbb{Z}[V]$. Moreover, write $V = P \times K$ where P is the Sylow p-subgroup of V. Note $|P| = p^a$ and $|K| = w$. Let b be a generator of P with $\rho(b) = \zeta_{p^a}$ and write

$$D_h = \sum_{i=0}^{p-1} D_{hi} b^i$$

with $D_{hi} \in \mathbb{Z}[\langle b^p\rangle K]$. We have

$$Y_h = \rho(D_h) = \sum_{i=0}^{p-1} \rho(D_{hi})\zeta_{p^a}^i.$$

Note $\rho(D_{hi}) \in \mathbb{Z}[\zeta_{p^{a-1}w}]$ and that $\{1, \ldots, \zeta_{p^a}^{p-1}\}$ is independent over $\mathbb{Q}(\zeta_{p^{a-1}w})$. As $Y_h \in \mathbb{Z}[\zeta_{v/p}]$, we conclude $\rho(D_{hi}) = 0$ for all $i > 0$ for all h. This implies

$$\rho(D) = \rho\left(\sum_{h\in H} D_h h\right) = \sum_{h\in H} \rho(D_{h0})h = \rho\left(\sum_{h\in H} D_{h0}h\right). \tag{16}$$

Write $Z = \sum_{h\in H} D_{h0}h$. Note $Z \in \mathbb{Z}[W \times H]$ where $W = \langle b^p\rangle K$. Furthermore, the coefficients of Z are in $[0, C]$, since the same is true for D by assumption. Note that (6) and (16) imply

$$|\chi(Z)|^2 = n \tag{17}$$

for all characters χ of G with $\chi(g) = \zeta_v$.

Write $Z = \sum_{k\in L} z_k k$ with $z_k \in \mathbb{Z}$ where $L = W \times H$. Note $0 \le z_k \le C$ for all k. Moreover, $|L| = v|H|/p$. Let $\ell = \sum_{k\in L} z_k$. The coefficient of 1 in $ZZ^{(-1)}$ is $\sum_{k\in L} z_k^2$. Thus

$$\frac{v|H|}{p}\sum_{k\in L} z_k^2 = \sum_{\chi\in\hat{L}} |\chi(Z)|^2 \tag{18}$$

by Result 2.1.

Let τ be any character of L whose order is divisible by v/p. Then τ is the restriction of a character χ of G whose order is divisible by v. Hence

$$|\tau(Z)|^2 = |\chi(Z)|^2 = n \tag{19}$$

by (17). Note that there are exactly $\varphi(v/p)|H| = \varphi(v)|H|/p$ characters of L whose order is divisible by v/p. Furthermore, we have $\chi_0(Z) = \ell$ where χ_0 denotes the trivial character of L. Thus (18) and (19) imply

$$\frac{v|H|}{p}\sum_{k\in L} z_k^2 \ge \ell^2 + \frac{n\varphi(v)|H|}{p}. \tag{20}$$

On the other hand, $\sum_{k\in L} z_k^2 \leq C\ell$ since $0 \leq z_k \leq C$. Thus

$$\frac{v|H|}{p}\sum_{k\in L} z_k^2 - \ell^2 \leq \frac{v|H|C\ell}{p} - \ell^2 \leq \frac{v^2|H|^2C^2}{4p^2}. \tag{21}$$

Combining (20) and (21), we get

$$\frac{n\varphi(v)|H|}{p} \leq \frac{v^2|H|^2C^2}{4p^2}$$

and thus the assertion. □

2.4 Some Notation

The following notation will be used repeatedly in this paper.

Notation 2.15. Let x, y be positive integers and let p be a prime.

- The largest nonnegative integer a such that p^a divides x is denoted by $\nu_p(x)$.
- The largest divisor of x which is coprime to y is denoted by $\omega(x, y)$.
- Write $x = x'p^{\nu_p(x)}$. We denote the order of p modulo x' by $\mathrm{ord}'_x(p)$.

3 Twisted Cyclotomic Integers from Circulant Hadamard Matrices

In this section, we show how circulant Hadamard matrices give rise to what we call "twisted cyclotomic integers". These numbers are intriguing, since they have small complex modulus, but live in fields with relatively large extension degree over $\mathbb{Q}$. These two properties tend to contradict each other, which allows us to derive necessary conditions for the existence of twisted cyclotomic integers in the next section.

Let $u > 1$ be be an odd integer and suppose a circulant Hadamard matrix of order $4u^2$ exists. Let G be a cyclic group of order $4u^2$. By Results 2.2 and 2.3, there is $D \in \mathbb{Z}[G]$ with coefficients $0, 1$ only, such that

$$DD^{(-1)} = u^2 + (u^2 - u)G. \tag{22}$$

Let d be a divisor of u and let U be a subgroup of G of order $2d^2$. Let $\rho : G \to G/U$ denote the natural epimorphism and write $E = \rho(D)$. Then all coefficients of E lie in the interval $[0, 2d^2]$, and we have

$$EE^{(-1)} = u^2 + 2(u^2 - u)d^2G. \tag{23}$$

by (22).

Set $v = u^2/d^2$. Note that G/U is a cyclic group of order $2v$ and that v is odd, as u is odd by assumption. Hence $\chi(E) \in \mathbb{Z}[\zeta_v]$ for every character χ of G/U. By (23), we have

$$|\chi(E)|^2 = u^2 \tag{24}$$

for every nontrivial character χ of G/U, as $\chi(G) = 0$.

From now on, we assume $(d, u/d) = 1$. Let p be a prime divisor of u/d.

Lemma 3.1. *Let E be as defined above. If*

$$\varphi(d^2) < \frac{p\varphi(u^2)}{2u^2}, \tag{25}$$

then there exists a nontrivial character χ of G/U such that $\chi(E)\eta \notin \mathbb{Z}[\zeta_{v/p}]$ for all roots of unity η in $\mathbb{Z}[\zeta_v]$.

Proof. Suppose the statement of the lemma does not hold. Then, for every nontrivial character χ of G/U, there exists a root of unity η_χ with

$$\chi(E)\eta_\chi \in \mathbb{Z}[\zeta_{v/p}]. \tag{26}$$

Recall that the coefficients of E all lie in the interval $[0, 2d^2]$. Note $v/p = u^2/(pd^2) \equiv 0 \pmod{p}$, as p divides u/d. In view of (24) and (26), we can apply Result 2.14 with $|H| = 2$ and $C = 2d^2$. This yields

$$u^2 \le \frac{2u^4(2d^2)^2}{4pd^4\varphi(u^2/d^2)}. \tag{27}$$

Note that $\varphi(u^2/d^2) = \varphi(u^2)/\varphi(d^2)$, as $(d, u/d) = 1$. Thus (27) implies $\varphi(d^2) \ge p\varphi(u^2)/(2u^2)$. This contradicts (25). □

Let χ be a character of G/U as given in Lemma 3.1 and set $Y = \chi(E)$. Then

$$|Y|^2 = u^2, \ Y \in \mathbb{Z}[\zeta_v], \ \text{ and } Y\eta \notin \mathbb{Z}[\zeta_{v/p}] \tag{28}$$

for all roots of unity η.

In the following, we use Notation 2.15. Write $\nu_p(v) = 2a$. Let t be an integer with

$$(u,t) = 1, \mathrm{ord}_{p^{2a}}(t) = p, \text{ and } t \equiv 1 \pmod{v/p^{2a}}. \tag{29}$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ be defined by $\zeta_v^\sigma = \zeta_v^t$. We first need to determine prime ideals of $\mathbb{Z}[\zeta_v]$ above $u\mathbb{Z}[\zeta_v]$ that are fixed by σ.

Lemma 3.2. *Let $q \neq p$ be a prime divisor of u. If*

$$\nu_p(\mathrm{ord}_{p^{2a}}(q)) > \nu_p(\mathrm{ord}'_{u/d}(q)), \tag{30}$$

then the prime ideals above $q\mathbb{Z}[\zeta_v]$ in $\mathbb{Z}[\zeta_v]$ are invariant under σ.

Proof. Write $h = \operatorname{ord}'_{v/p^{2a}}(q)$ and $k = \operatorname{ord}'_{u/d}(q)$ (here we use Notation 2.15). We claim

$$\nu_p(h) \le \nu_p(k). \tag{31}$$

It is a well-known fact and straightforward to prove that $\operatorname{ord}_{x^2}(y)/\operatorname{ord}_x(y)$ divides x for all positive integers x, y with $(x, y) = 1$. Hence $\operatorname{ord}'_{u^2/(d^2p^{2a})}(q)/\operatorname{ord}'_{u/(dp^a)}(q)$ divides $\omega(u/(dp^a), q)$. Furthermore, note that $v/p^{2a} = u^2/(d^2p^{2a})$. Thus we can write

$$\operatorname{ord}'_{v/p^{2a}}(q) = \operatorname{ord}'_{u^2/(d^2p^{2a})}(q) = e \operatorname{ord}'_{u/(dp^a)}(q)$$

for some integer e dividing $\omega(u/(dp^a), q)$. Moreover, $\omega(u/(dp^a), q)$ and thus e is not divisible by p, as $\nu_p(u) = a$. Hence

$$\nu_p(h) = \nu_p\left(\operatorname{ord}'_{v/p^{2a}}(q)\right) = \nu_p\left(\operatorname{ord}'_{u/(dp^a)}(q)\right) \le \nu_p\left(\operatorname{ord}'_{u/d}(q)\right) = \nu_p(k).$$

This proves (31).

By assumption (30) and (31), we have

$$\nu_p(h) \le \nu_p(k) < \nu_p(\operatorname{ord}_{p^{2a}}(q)).$$

This implies $\operatorname{ord}_{p^{2a}}(q^h) \equiv 0 \pmod{p}$. Since $\mathbb{Z}^*_{p^{2a}}$ is cyclic, it follows that the subgroup of $\mathbb{Z}^*_{p^{2a}}$ generated by q^h contains all elements of order p in $\mathbb{Z}^*_{p^{2a}}$. Recall that t is an integer satisfying (29). Since t is of order p in $\mathbb{Z}^*_{p^{2a}}$, there is an integer j with

$$t \equiv q^{hj} \pmod{p^{2a}}. \tag{32}$$

On the other hand, we have $t \equiv 1 \pmod{\omega(v/p^{2a}, q)}$ and $q^{hj} \equiv 1 \pmod{\omega(v/p^{2a}, q)}$ by the definition of h. Thus

$$t \equiv q^{hj} \pmod{\omega(v, q)}.$$

by (32). Hence, by Result 2.8, the prime ideals above $q\mathbb{Z}[\zeta_v]$ in $\mathbb{Z}[\zeta_v]$ are indeed invariant under σ. □

Remark 3.3. Inequality (30) relates the subgroup of $\mathbb{Z}^*_{p^{2a}}$ generated by q to the subgroup of $\mathbb{Z}^*_{\omega(v/p^{2a},q)}$ generated by q. In fact, (30) is equivalent to $\operatorname{ord}_{p^{2a}}(q^{\operatorname{ord}'_{v/p^{2a}}(q)}) \equiv 0 \pmod{p}$.

Let m be a divisor of u with $m \equiv 0 \pmod{p^a}$ such that (30) is satisfied for every prime factor $q \ne p$ of m. Note that $t \equiv 1 \pmod{v/p^{2a}}$ and thus

$$t \equiv 1 \equiv p^{\operatorname{ord}_{v/p^{2a}}(p)} \pmod{v/p^{2a}}.$$

Hence, by Result 2.8, the prime ideals above $p\mathbb{Z}[\zeta_v]$ in $\mathbb{Z}[\zeta_v]$ are invariant under σ. Combined with Lemma 3.2, this shows that all prime ideals above $m\mathbb{Z}[\zeta_v]$ in $\mathbb{Z}[\zeta_v]$ are invariant under σ.

Recall $Y\overline{Y} = u^2$. Hence $Y\overline{Y} \equiv 0 \pmod{m^2}$, which implies $Y^\sigma\overline{Y} \equiv 0 \pmod{m^2}$, as the prime ideals above $m\mathbb{Z}[\zeta_v]$ in $\mathbb{Z}[\zeta_v]$ are invariant under σ. We conclude that $X = Y^\sigma\overline{Y}/m^2$ is an algebraic integer, i.e., $X \in \mathbb{Z}[\zeta_{u^2/d^2}]$. Note $|X|^2 = u^4/m^4$. For the purpose of our applications, we need m to be large. Thus we will choose m as large as possible, i.e., include all prime factors q of u in m which satisfy (30). On the other hand, we do not want X to lie in a field $\mathbb{Q}(\zeta_k)$ with small k. The following lemma addresses the latter issue.

Lemma 3.4. *We have $X\eta \notin \mathbb{Z}[\zeta_{v/p}]$ for all roots of unity η. Moreover,*

$$\mathrm{N}(X) = \frac{u^{2p}}{m^{2p}},$$

where N *denotes the norm of $\mathbb{Q}(\zeta_v)$ relative to $\mathbb{Q}(\zeta_{v/p})$.*

Proof. Suppose there is a root of unity ξ such that $Z = X\xi \in \mathbb{Z}[\zeta_{u^2/(pd^2)}]$. Note that

$$ZY = Y^\sigma\overline{Y}Y\xi/m^2 = Y^\sigma\xi u^2/m^2. \tag{33}$$

Applying N to (33), we get

$$Z^p\mathrm{N}(Y) = \mathrm{N}(Y^\sigma)\mathrm{N}(\xi)u^{2p}/m^{2p} = \mathrm{N}(Y)\mathrm{N}(\xi)\left(\frac{u^2}{m^2}\right)^p.$$

Since $\mathrm{N}(Y) \neq 0$, this implies $Z^p \equiv 0 \pmod{(u^2/m^2)^p}$ and hence $Z \equiv 0 \pmod{u^2/m^2}$. Thus $Z = \theta u^2/m^2$ for some root of unity θ by Result 2.4, as $|Z| = u^2/m^2$. Hence

$$\frac{Y^\sigma\overline{Y}}{m^2} = X = Z\overline{\xi} = \frac{\overline{\xi}\theta u^2}{m^2}.$$

Recall that $Y\overline{Y} = u^2$, i.e., $u^2/\overline{Y} = Y$. Thus

$$Y^\sigma = \frac{\overline{\xi}\theta u^2 m^2}{\overline{Y}m^2} = \frac{\overline{\xi}\theta u^2}{\overline{Y}} = Y\overline{\xi}\theta. \tag{34}$$

Recall $Y \in \mathbb{Z}[\zeta_v]$. Thus $\overline{\xi}\theta$ is root of unity in $\mathbb{Z}[\zeta_v]$ and there are integers i, j and $\delta \in \{-1, 1\}$ with $\overline{\xi}\theta = \delta\zeta_{p^{2a}}^i\zeta_{v/p^{2a}}^j$. Note that $\zeta_{p^{2a}}^\sigma = \zeta_{p^{2a}}^t$ and $\zeta_{v/p^{2a}}^\sigma = \zeta_{v/p^{2a}}$ by the definition of σ. Using (34) repeatedly, we get

$$Y = Y^{\sigma^p} = Y\delta\zeta_{p^{2a}}^{i(t^p-1)/(t-1)}\zeta_{v/p^{2a}}^{jp}.$$

This implies

$$\delta\zeta_{p^{2a}}^{i(t^p-1)/(t-1)}\zeta_{v/p^{2a}}^{jp} = 1. \tag{35}$$

Taking both sides of (35) to the power v, we get $\delta^v = 1$ and thus $\delta = 1$, as v is odd. Now take both sides of (35) to the power p^{2a}. This shows $\zeta_{v/p^{2a}}^{jp^{2a+1}} = 1$ and hence $\zeta_{v/p^{2a}}^j = 1$, since $(p, v/p^{2a}) = 1$. So (35) implies

$$\zeta_{p^{2a}}^{i(t^p-1)/(t-1)} = 1.$$

The same argument as in the proof of Result 2.14 (please refer to the paragraph after equation (14)) shows that p^2 does not divide $(t^p-1)/(t-1)$ and thus $i \equiv 0 \pmod{p^{2a-1}}$. Hence, as $t-1 \not\equiv 0 \pmod{p^{2a}}$, there is an integer d such that $\zeta_{p^{2a}}^{i+dt} = \zeta_{p^{2a}}^{d}$. In summary, we have

$$(\zeta_{p^{2a}}^{d} Y)^{\sigma} = \delta \zeta_{p^{2a}}^{i+dt} \zeta_{v/p^{2a}}^{j} Y = \zeta_{p^{2a}}^{d} Y, \tag{36}$$

as $\delta = \zeta_{v/p^{2a}}^{j} = 1$ and $\zeta_{p^{2a}}^{i+dt} = \zeta_{p^{2a}}^{d}$. By (36), we have a $Y\zeta_{p^{2a}}^{d} \in \mathbb{Z}[\zeta_{u^2/(pd^2)}]$, contradicting (28).

Note that $\mathrm{N}(Y^{\sigma}) = \mathrm{N}(Y)$ and recall $|Y|^2 = u^2$. Hence $\mathrm{N}\left(Y^{\sigma}\overline{Y}\right) = \mathrm{N}\left(Y\overline{Y}\right) = \mathrm{N}(u^2) = u^{2p}$ and thus

$$\mathrm{N}(X) = \mathrm{N}\left(\frac{Y^{\sigma}\overline{Y}}{m^2}\right) = \frac{u^{2p}}{m^{2p}}.$$

□

Summarizing the results of this section, we have the following.

Theorem 3.5. *Let $u > 1$ be an odd integer and suppose that a circulant Hadamard matrix of order $4u^2$ exists. Let d be a divisor of u with $(d, u/d) = 1$ and let p be a prime divisor of u/d such that*

$$\varphi(d^2) < \frac{p\varphi(u^2)}{2u^2}. \tag{37}$$

Let p^a be the largest power of p dividing u and write $v = u^2/d^2$. Let m be a divisor of u with $m \equiv 0 \pmod{p^a}$ such that

$$\nu_p(\mathrm{ord}_{p^{2a}}(q)) > \nu_p(\mathrm{ord}'_{u/d}(q))$$

for every prime factor $q \neq p$ of m. Then there is $X \in \mathbb{Z}[\zeta_v]$ with

$$|X|^2 = \frac{u^4}{m^4} \text{ and } X\eta \notin \mathbb{Z}[\zeta_{v/p}] \tag{38}$$

for all roots of unity η. Furthermore,

$$\mathrm{N}_{\mathbb{Q}(\zeta_v)/\mathbb{Q}(\zeta_{v/p})}(X) = \frac{u^{2p}}{m^{2p}}, \tag{39}$$

where $\mathrm{N}_{\mathbb{Q}(\zeta_v)/\mathbb{Q}(\zeta_{v/p})}$ denotes the norm of $\mathbb{Q}(\zeta_v)$ relative to $\mathbb{Q}(\zeta_{v/p})$.

4 Cyclotomic Integers in $\mathbb{Q}(\zeta_{p^a})$ whose Complex Moduli are Integers

Let p be an odd prime and let v be a positive integer. In order to study the twisted cyclotomic integers constructed in the previous section, we need to find a condition ensuring that $Y\overline{Y} = v^2$, $Y \in \mathbb{Z}[\zeta_{p^a}]$, has only trivial solutions. Here we call a solution Y trivial if it has the form $Y = \eta v$ where η is a root of unity. We first review the relevant results in the literature. The following result is implicitly contained in the proof of [13, Thm. 2.2.3].

Result 4.1. *Let p be an odd prime, let a be a positive integer, and let f be a divisor of $p-1$. Suppose $Y \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $Y\overline{Y} = v^2$ where v is a positive integer with $(v,p)=1$. Moreover, let $q_1,\dots,q_s$ be the distinct prime divisors of v and suppose that*

$$\nu_p(\mathrm{ord}_{p^a}(q_i)) \geq a-1 \tag{40}$$

for $i=1,\dots,s$. If Y is contained in the subfield K of $\mathbb{Q}(\zeta_{p^a})$ with $[\mathbb{Q}(\zeta_{p^a}):K]=f$ and

$$f > \frac{2v(p-1)}{p}, \tag{41}$$

then $Y = \pm v$.

For $a=1$, Result 4.1 was first discovered by Chan [5, Lemmas 2.3, 2.4]. Note that, in this case, condition (40) is always satisfied. In [13, Thm. 2.2.3], Chan's result was extended to the case $a>1$ by a field descent argument based on assumption (40).

In the present paper, however, it turns out that we only have to deal with cases where $a>1$ and (40) is *not* satisfied. Thus we require a version of Result 4.1 without assumption (40). In this vain, we previously had obtained the following result, which is implicitly contained in the proof of [9, Lemma 3.4].

Result 4.2. *Let p be an odd prime, let a be a positive integer, and let f be a divisor of $p-1$. Suppose $Y \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $Y\overline{Y} = v^2$ where v is a positive integer with $(v,p)=1$. If Y is contained in the subfield K of $\mathbb{Q}(\zeta_{p^a})$ with $[\mathbb{Q}(\zeta_{p^a}):K]=f$ and*

$$f > v^2, \tag{42}$$

then $Y = \pm v$.

Note that Result 4.2 does not require assumption (40). Condition (42), however, is much more restrictive than (41). In summary, for the study of twisted cyclotomic integers, Result 4.1 is useless due to assumption (40) and Result 4.2 is almost useless because of assumption (42).

In this section, we resolve these difficulties. In Theorem 4.5, we show that v^2 can be replaced by $2v-1$ in Result 4.2. Hence, quite surprisingly, with rare exceptions, Result 4.1 holds even if assumption (40) is not satisfied. In fact, Theorem 4.5 is best possible in the following sense: Let $p=4v-1$ be a prime and set $Y = \left(\sum_{b=1}^{p-1}\zeta_p^{b^2}\right)/2$. Then $Y\overline{Y}=v$ and Y is contained in the subfield K of $\mathbb{Q}(\zeta_p)$ with $[\mathbb{Q}(\zeta_p):K]=2v-1$. Thus the assertion of Theorem 4.5 becomes false if the assumption $f>2v-1$ is replaced by $f \geq 2v-1$.

We start with two preliminary combinatorial lemmas.

Lemma 4.3. *Let $b_0, \ldots, b_{p-1}$ be integers and set $t = |\{i : b_i \neq 0\}|$. If $t > 0$, then*

$$p\sum_{i=0}^{p-1} b_i^2 - (\sum_{i=0}^{p-1} b_i)^2 \geq \frac{p-t}{t}(\sum_{i=0}^{p-1} b_i)^2.$$

Proof. We may assume $b_i = 0$ for $i \geq t$. Using Cauchy-Schwarz, we get

$$t\sum_{i=0}^{p-1} b_i^2 = t\sum_{i=0}^{t-1} b_i^2 \geq (\sum_{i=0}^{t-1} b_i)^2 = (\sum_{i=0}^{p-1} b_i)^2.$$

Therefore,

$$p\sum_{i=0}^{p-1} b_i^2 - (\sum_{i=1}^{p-1} b_i)^2 \geq (p-t)\sum_{i=0}^{p-1} b_i^2 \geq \frac{p-t}{t}(\sum_{i=0}^{p-1} b_i)^2.$$

□

Lemma 4.4. *Let $b_0, \ldots, b_{p-1}$ be integers and let T be the largest positive integer such that exist $i_1, \ldots, i_T$ with $0 \leq i_1 < \cdots < i_T \leq p-1$ and $b_{i_1} = \cdots = b_{i_T}$. Then*

$$p\sum_{i=0}^{p-1} b_i^2 - (\sum_{i=0}^{p-1} b_i)^2 \geq \max\{T(p-T), p(p-T)/2\}.$$

Proof. Observe that

$$p\sum_{i=0}^{p-1} b_i^2 - (\sum_{i=0}^{p-1} b_i)^2 = \sum_{j<k}(b_j - b_k)^2. \tag{43}$$

By the definition of T, there is an integer b such that there are exactly T numbers b_i that are all equal to b and the remaining b_i's are not equal to b. Without loss of generality, we may assume $b_0 = \cdots = b_{T-1} = b$ and $b_T, \ldots, b_{p-1} \neq b$. Hence $b_j \neq b_k$ whenever $0 \leq j \leq T-1$ and $T \leq k \leq p-1$. Note that $(b_j - b_k)^2 \geq 1$ if $b_j \neq b_k$, as the b_i's are integers by assumption. Thus

$$\sum_{j<k}(b_j - b_k)^2 \geq \sum_{j=0}^{T-1}\sum_{k=T}^{p-1}(b_j - b_k)^2 \geq T(p-T). \tag{44}$$

On the other hand, by the definition of T, for every j with $0 \leq j \leq p-1$, there are at least $p-T$ indices k with $b_j - b_k \neq 0$. Therefore,

$$\sum_{j<k}(b_j - b_k)^2 = \frac{1}{2}\sum_{j,k=0}^{p-1}(b_j - b_k)^2 \geq \frac{p(p-T)}{2}. \tag{45}$$

The assertion of the lemma follows from (43–45). □

The following is the central result of this section.

Theorem 4.5. *Let p be an odd prime, let a be a positive integer, and let f be a divisor of $p-1$. Suppose $Y \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $Y\overline{Y} = v^2$ where v is a positive integer with $(v,p)=1$. If Y is contained in the subfield K of $\mathbb{Q}(\zeta_{p^a})$ with $[\mathbb{Q}(\zeta_{p^a}) : K] = f$ and*

$$f > 2v - 1, \tag{46}$$

then $Y = \pm v$.

Proof. Let t be an integer with $(p,t)=1$ and $\mathrm{ord}_{p^a}(t) = \mathrm{ord}_p(t) = f$. Let σ be the automorphism of $\mathbb{Q}(\zeta_{p^a})$ determined by $\zeta_{p^a}^\sigma = \zeta_{p^a}^t$. Note that K is the fixed field of σ. Hence

$$Y^\sigma = Y. \tag{47}$$

First suppose that f is even. Then $\sigma^{f/2}$ is the unique involution in $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})$, which is complex conjugation. Hence (47) implies $\overline{Y} = Y$. As $Y\overline{Y} = v^2$ by assumption, we conclude $Y = \pm v$. Thus the assertion of Theorem 4.5 holds.

From now on, we assume that f is odd. To exploit (47), we use the integral basis of $\mathbb{Q}(\zeta_{p^a})$ over $\mathbb{Q}(\zeta_p)$ defined in Lemma 2.5. Hence we write

$$Y = Y_0 + \sum_{k \in B} \sum_{j=0}^{f-1} Y_{k,j} \zeta_{p^a}^{t^j k}. \tag{48}$$

with $Y_{k,j} \in \mathbb{Z}[\zeta_p]$. Note

$$Y^\sigma = Y_0^\sigma + \sum_{k \in B} \sum_{j=0}^{f-1} Y_{k,j}^\sigma \zeta_{p^a}^{t^{j+1} k}.$$

Moreover, $\zeta_{p^a}^{t^f k} = \zeta_{p^a}^k$, as $\mathrm{ord}_{p^a}(t) = f$. For convenience, we set $Y_{k,f} = Y_{k,0}$ for $k \in B$. Since $Y^\sigma = Y$ and $\{1\} \cup \bigcup_{k\in B} \{\zeta_{p^a}^{t^j k} : j = 0, \ldots, f-1\}$ is linearly independent over $\mathbb{Q}(\zeta_p)$, we conclude that

$$Y_0^\sigma = Y_0 \text{ and } Y_{k,j+1} = Y_{k,j}^\sigma \text{ for all } i \in B \text{ and } j = 0, \ldots, f-1. \tag{49}$$

For convenience, we write Y_k for $Y_{k,0}$. By (48) and (49), we have

$$Y = Y_0 + \sum_{k \in B} \sum_{j=0}^{f-1} \left(Y_k \zeta_{p^a}^k \right)^{\sigma^j}. \tag{50}$$

Write $Y_0 = \sum_{i=0}^{p-1} c_i \zeta_p^i$ and $Y_k = \sum_{i=0}^{p-1} c_{ki} \zeta_p^j$ with $c_i \in \mathbb{Z}$ and $c_{ki} \in \mathbb{Z}$ for all i, k. As $\sum_{i=0}^{p-1} \zeta_p^i = 0$, the c_i's and c_{ki}'s are not uniquely determined, but that will not affect our arguments. The main idea of our proof is deriving constraints on the c_i's and c_{ki}'s stemming from $|Y|^2 = v^2$.

Claim 1 We have

$$v^2(p-1) = p \sum_{i=0}^{p-1} c_i^2 - \left(\sum_{i=0}^{p-1} c_i \right)^2 + f \sum_{k=1}^{e} \left(p \sum_{i=0}^{p-1} c_{ki}^2 - \left(\sum_{i=0}^{p-1} c_{ki} \right)^2 \right). \tag{51}$$

Note that each of the terms $\left(p\sum_{i=0}^{p-1}c_i^2-\left(\sum_{i=0}^{p-1}c_i\right)^2\right)$ and $\left(p\sum_{i=0}^{p-1}c_{ki}^2-\left(\sum_{i=0}^{p-1}c_{ki}\right)^2\right)$, $k=1,\dots,e$, is nonnegative by Cauchy-Schwarz. This fact will be used repeatedly to obtain lower bounds for the right hand side of (51).

To prove Claim 1, first notice that, by the definition of B, there are integers $\gamma(j,k)$ such that

$$\{(\zeta_{p^a}^k)^{\sigma^j}\zeta_{p^{a-1}}^{\gamma(j,k)} : j=0,\dots,f-1, k\in B\}=\{1,\zeta_{p^a},\dots,\zeta_{p^a}^{p^{a-1}-1}\}.$$

Let $\mathcal{M}$ be the function defined in Result 2.12. Note that $\mathcal{M}(Y)=v^2$, as $|Y|^2=v^2$. Thus Result 2.12 (a) and (50) imply

$$\begin{aligned}
v^2 &= \mathcal{M}(Y)\\
&= \mathcal{M}\left(Y_0+\sum_{k\in B}\sum_{j=0}^{f-1}\left(Y_k\zeta_{p^a}^k\right)^{\sigma^j}\right)\\
&= \mathcal{M}(Y_0)+\mathcal{M}\left(\sum_{k\in B}\sum_{j=0}^{f-1}\left(Y_k^{\sigma^j}\zeta_{p^{a-1}}^{-\gamma(j,k)}\right)(\zeta_{p^a}^k)^{\sigma^j}\zeta_{p^{a-1}}^{\gamma(j,k)}\right)\\
&= \mathcal{M}(Y_0)+\sum_{k\in B}\sum_{j=0}^{f-1}\mathcal{M}\left(Y_k^{\sigma^j}\zeta_{p^{a-1}}^{-\gamma(j,k)}\right)\\
&= \mathcal{M}(Y_0)+\sum_{k\in B}\sum_{j=0}^{f-1}\mathcal{M}(Y_k)\\
&= \mathcal{M}(Y_0)+f\sum_{k\in B}\mathcal{M}(Y_k).
\end{aligned} \tag{52}$$

Using Result 2.12 (b), we get

$$\mathcal{M}(Y_0)=\frac{1}{p-1}\sum_{i<j}(c_i-c_j)^2=\frac{1}{p-1}\left(p\sum_{i=0}^{p-1}c_i^2-\left(\sum_{i=0}^{p-1}c_i\right)^2\right)$$

and similar expressions for the $\mathcal{M}(Y_k)$'s. Together with (52), this proves Claim 1.

Recall $Y_0=\sum_{i=0}^{p-1}c_i\zeta_p^i$. We add a multiple of $\sum_{i=0}^{p-1}\zeta_p^i=0$ to Y_0, if necessary, so that there is at least one $k>0$ with $c_k=0$.

Claim 2 We can assume $|c_0|<v$.

Suppose $|c_0|\geq v$. Replacing Y by $-Y$, if necessary, we have $c_0\geq v$. Recall that $Y_0^\sigma=Y_0$ by (49). As $c_k=0$ and the orbits of σ on $\{\zeta_p,\dots,\zeta_p^{p-1}\}$ all have length f, we conclude that there are at least f indices $i>0$ with $c_i=0$. Let $M=\{i: c_i\neq 0\}$. We just have shown $|M|\leq p-f$. Furthermore, it is straightforward to verify

$$p\sum_{i=0}^{p-1}c_i^2-\left(\sum_{i=0}^{p-1}c_i\right)^2=(p-|M|)\sum_{i\in M}c_i^2+\sum_{\substack{i,j\in M\\ i<j}}(c_i-c_j)^2. \tag{53}$$

To get a lower bound for the right hand side of (53), we now show

$$(c_0 - c_i)^2 + (p - |M|)c_i^2 \geq v^2 \tag{54}$$

for all $i \in M$, $i \neq 0$, with equality if and only if $c_0 = v$ and $c_i = 0$. Note that the minimum of the function $g(x) = (c_0 - x)^2 + fx^2$ over $x \in \mathbb{R}$ occurs for $x = c_0/(f+1)$.

First suppose $c_0 \leq f + 1$. Note that (46) implies $f > 2v$, as f is odd by assumption. As the minimum of $g(x)$ over $x \in \mathbb{Z}$ occurs for $x = 0$ or $x = 1$, we have $g(c_i) \geq \min\{c_0^2, (c_0 - 1)^2 + f\} \geq v^2$, as $c_0 \geq v$ and $f > 2v$. Furthermore, $g(c_i) = v^2$ if and only if $c_i = 0$ and $x = 0$.

Now suppose $c_0 > f + 1$. Then

$$g\left(\frac{c_0}{f+1}\right) \geq \left(c_0 - \frac{c_0}{f+1}\right)^2 = \frac{c_0^2 f^2}{(f+1)^2} > f^2 > 4v^2,$$

as $f > 2v$ by assumption.

In summary, we have shown $g(c_i) \geq v^2$ with equality if and only of $c_0 = v$ and $c_i = 0$. As $p - |M| \geq f$, this proves (54).

Now suppose that we have equality in (54) for all $i \in M$, $i \neq 0$. Then $c_0 = v$ and $c_i = 0$ for $i = 1, \ldots, p-1$, i.e., $Y_0 = v$. Thus $\mathcal{M}(Y_0) = v^2$. By (52), however, we have $\mathcal{M}(Y_0) + f \sum_{k \in B} \mathcal{M}(Y_k) = v^2$. Hence $\sum_{k \in B} \mathcal{M}(Y_k) = 0$ and this, in view of (5), implies $Y_i = 0$ for all $i > 0$. Thus $Y = Y_0 = v$, which implies the assertion of Theorem 4.5.

Hence we can assume $(c_0 - c_i)^2 + (p - |M|)c_i^2 > v^2$ for at least one $i \in M$, $i \neq 0$. Thus, using $c_0 \geq v$, (53), and (54), we get

$$\begin{aligned} p\sum_{i=0}^{p-1} c_i^2 - \left(\sum_{i=0}^{p-1} c_i\right)^2 &\geq (p - |M|)c_0^2 + \sum_{\substack{i \in M \\ i \neq 0}} \left((p - |M|)c_i^2 + (c_0 - c_i)^2\right) \\ &> (p - |M|)v^2 + (|M| - 1)v^2 \\ &= (p-1)v^2. \end{aligned}$$

But this implies that the right hand side of (51) is larger than $(p-1)v^2$, a contradiction. This completes the proof of Claim 2.

Write $\Gamma = \sum_{i=0}^{p-1} c_i + f \sum_{k \in B} \sum_{i=0}^{p-1} c_{ki}$.

Claim 3. $\Gamma = \pm v + \lambda p$ with $\lambda \in \mathbb{Z}$ and $|\lambda| < v$.

Recall that, by (50),

$$\begin{aligned} Y &= \sum_{i=0}^{p-1} c_i \zeta_p^i + \sum_{k \in B} \sum_{j=0}^{f-1} \left(\left(\sum_{i=0}^{p-1} c_{ki} \zeta_p^j \right) \zeta_{p^a}^k \right)^{\sigma^j} \\ &= \sum_{i=0}^{p-1} c_i \zeta_{p^a}^{p^{a-1}i} + \sum_{k \in B} \sum_{j=0}^{f-1} \sum_{i=0}^{p-1} c_{ki} \zeta_{p^a}^{p^{a-1}jt+kt}. \end{aligned}$$

Write

$$D(x)=\sum_{i=0}^{p-1}c_ix^{p^{a-1}i}+\sum_{k\in B}\sum_{j=0}^{f-1}\sum_{i=0}^{p-1}c_{ki}x^{p^{a-1}jt+kt}.$$

Let $\rho:\mathbb{Z}[x]\to\mathbb{Z}[\zeta_{p^a}]$ be the homomorphism determined by $\rho(x)=\zeta_{p^a}$. Note that the kernel of ρ is

$$\left\{h(x)(1+x^{p^{a-1}}+\cdots+x^{(p-1)p^{a-1}}):h\in\mathbb{Z}[x]\right\}.$$

As $|Y|^2=v^2$, we have $\rho(D(x)D(x^{p^a-1}))=Y\overline{Y}=v^2$. Thus

$$D(x)D(x^{p^a-1})=v^2+h(x)(1+x^{p^{a-1}}+\cdots+x^{(p-1)p^{a-1}}). \tag{55}$$

for some $h\in\mathbb{Z}[x]$. Note $\Gamma=D(1)$. Hence $\Gamma^2=D(1)^2=v^2+h(1)p\equiv v^2\pmod p$ by (55). This implies $\Gamma=\pm v\pmod p$ and thus $\Gamma=\pm v+\lambda p$ for some integer λ. To prove Claim 3, it remains to show $|\lambda|<v$.

Recall $Y_0=\sum_{i\in M}c_i\zeta_p^i$, $|M|\le p-f$, and $c_i=0$ for $i\notin M$. Thus, using Lemma 4.3 and (51), we get

$$(p-1)v^2\ge p\sum_{i=0}^{p-1}c_i^2-\left(\sum_{i=0}^{p-1}c_i\right)^2\ge\frac{f}{p-f}\left(\sum_{i=0}^{p-1}c_i\right)^2.$$

This implies

$$\left|\sum_{i=0}^{p-1}c_i\right|\le v\sqrt{\frac{(p-1)(p-f)}{f}}<\frac{vp}{\sqrt{f}}. \tag{56}$$

Recall $Y_k=\sum_{i=0}^{p-1}c_{ki}\zeta_p^j$. As stated above, the c_{ki}'s are not uniquely determined. For each k, we may, however, choose the c_{ki}'s such that of $N_k=|\{i:c_{ki}\neq 0\}|$ is minimal. Note that this implies that $p-N_k$ is the maximum number such that $p-N_k$ of the numbers c_{ki}, $i=0,\ldots,p-1$, are equal.

First suppose $N_k\ge(p+1)/2$ and thus $p-N_k\le(p-1)/2$ for some k. Then

$$(p-1)v^2\ge f\left(p\sum_{i=0}^{p-1}c_{ki}^2-\left(\sum_{i=0}^{p-1}c_{ki}\right)^2\right)\ge\frac{f(p-1)^2}{4} \tag{57}$$

by Lemma 4.4 and (51). Note that $f\le(p-1)/2$, as p is an odd prime and f is an odd divisor of $p-1$. Thus (57) implies $v^2\ge f(p-1)/4\ge f^2/2$. But this is impossible, as $f>2v$ by assumption.

We have shown $N_k\le(p-1)/2$ for all k. Hence Lemma 4.3 and (51) imply

$$(p-1)v^2\ge f\left(p\sum_{i=0}^{p-1}c_{ki}^2-\left(\sum_{i=0}^{p-1}c_{ki}\right)^2\right)\ge\frac{f(p-N_k)}{N_k}\left(\sum_{i=0}^{p-1}c_{ki}\right)^2\ge f\left(\sum_{i=0}^{p-1}c_{ki}\right)^2. \tag{58}$$

Set $x_k = \sum_{i=0}^{p-1} c_{ki}$. Using (58) and $2v < f \leq (p-1)/2$, we get

$$|x_k| \leq \frac{v\sqrt{p-1}}{\sqrt{f}} < \frac{f\sqrt{p-1}}{2\sqrt{f}} = \frac{\sqrt{f(p-1)}}{2} < \frac{p-1}{2}. \tag{59}$$

The trivial fact $\sum_{i=0}^{p-1} c_{ki}^2 \geq |x_k|$ and (59) imply

$$\begin{aligned} p\sum_{i=0}^{p-1} c_{ki}^2 - \left(\sum_{i=0}^{p-1} c_{ki}\right)^2 &\geq p|x_k| - x_k^2 \\ &\geq p|x_k| - \frac{p-1}{2}|x_k| \\ &= \frac{p+1}{2}|x_k|. \end{aligned} \tag{60}$$

Using (51) and (60), we get $(p-1)v^2 \geq \frac{f(p+1)}{2} \sum_{k\in B} |x_k|$ and thus

$$\sum_{k\in B} |x_k| \leq \frac{2(p-1)v^2}{f(p+1)} < v, \tag{61}$$

as $f > 2v$ by assumption.

Recall $\Gamma = \sum_{i=0}^{p-1} c_i + f\sum_{k\in B}\sum_{i=0}^{p-1} c_{ki} = \pm v + \lambda p$ and $x_k = \sum_{i=0}^{p-1} c_{ki}$ and that we assume $v \geq 2$. Using (56) and (61), we get

$$|\lambda| \leq \frac{1}{p}(v + |\Gamma|) \leq \frac{1}{p}\left(v + \frac{vp}{\sqrt{f}} + fv\right) = \left(\frac{f+1}{p} + \frac{1}{\sqrt{f}}\right)v < v,$$

as $f \geq 2v+1 \geq 5$ and $p \geq 2f+1 \geq 10$. This proves Claim 3.

Claim 4 We may assume $\lambda > 0$ and $c_0 = v + \lambda - f$ or $c_0 = -v + \lambda$.

Recall $Y_0 = \sum_{i=0}^{p-1} c_i \zeta_p^i$ and that $Y_0^\sigma = Y_0$ by (49). Note hat $Y_0^\sigma = Y_0$ implies $c_i = c_j$ if i and j are in the same orbit of $x \mapsto x^t$ on $\mathbb{Z}/p\mathbb{Z}$. As $\mathrm{ord}_p(t) = f$, this implies $\sum_{i=1}^{p-1} c_i \equiv 0 \pmod{f}$. We conclude $\sum_{i=0}^{p-1} c_i \equiv c_0 \pmod{f}$ and hence $\Gamma \equiv c_0 \pmod{f}$.

By Claim 3, we thus get $c_0 \equiv \pm v + \lambda p \pmod{f}$. Note that $p \equiv 1 \pmod{f}$. This implies $c_0 \equiv \pm v + \lambda \pmod{f}$. Thus $c_0 = \pm v + \lambda + \alpha f$ for some integer α. Replacing Y by $-Y$ if necessary, we may assume $0 \leq \lambda < v$. Therefore, $2v > \pm v + \lambda > -v$. If $\alpha \geq 1$, we conclude $c_0 > v$ as $f > 2v$. If $\alpha \leq -2$, then $c_0 < -2v$. But by Claim 2, $-v < c_0 < v$. Therefore, $\alpha \in \{0, -1\}$. If $\alpha = 0$, then $c_0 = -v + \lambda$, as $c_0 = v + \lambda$ is impossible by Claim 2. Similarly, $c_0 = v + \lambda - f$ if $\alpha = -1$. This proves Claim 4.

Recall $\sum_{i=1}^{p-1} c_i = fc$. Write $d = \sum_{k\in B}\sum_{i=0}^{p-1} c_{ki}$. Then $\Gamma = c_0 + fc + fd$ and

$$|d| \leq \sum_{k\in B} |x_k| < v \tag{62}$$

by (61). (Recall that $x_k = \sum_{i=0}^{p-1} c_{ki}$.)

Claim 5

$$\sum_{i=1}^{p-1}(c_i - c_0)^2 \geq (p-1)\left(v - \frac{fd}{p-1}\right)^2. \tag{63}$$

We consider the two cases occurring in Claim 4.

Case 1 $c_0 = v + \lambda - f$. By Claim 3, $\Gamma = \pm v + \lambda p$. If $\Gamma = -v + \lambda p$, then $-v + \lambda \equiv c_0 \equiv v + \lambda \pmod f$ by assumption. But this implies $2v \equiv 0 \pmod f$ which contradicts $f > 2v$. Hence we have

$$\Gamma = v + \lambda p = c_0 + fc + fd = v + \lambda - f + fc + fd$$

and thus $\lambda(p-1) = fc + fd - f$. As $\sum_{i=1}^{p-1} c_i = fc$, we get

$$\begin{aligned}
\sum_{i=1}^{p-1}(c_i - c_0)^2 &\geq \sum_{i=1}^{p-1}\left(\frac{fc}{p-1} - c_0\right)^2 \\
&= (p-1)\left(\frac{fc}{p-1} - v - \lambda + f\right)^2 \\
&= (p-1)\left(\frac{fc}{p-1} - v - \frac{fc + fd - f}{p-1} + f\right)^2 \\
&= (p-1)\left(\frac{f - fd}{p-1} - v + f\right)^2 \\
&= (p-1)\left(\left(f - v + \frac{f}{p-1}\right) - \frac{fd}{p-1}\right)^2.
\end{aligned}$$

Since and $f > 2v$, we have $f - v + \frac{f}{p-1} > v$. Moreover, $\frac{fd}{p-1} < v$ by (62). Hence $f - v + \frac{f}{p-1} - \frac{fd}{p-1} > v - \frac{fd}{p-1} > 0$ and thus

$$\sum_{i=1}^{p-1}(c_i - c_0)^2 > (p-1)\left(v - \frac{fd}{p-1}\right)^2.$$

Case 2 $c_0 = -v + \lambda$. In this case, $\Gamma = -v + \lambda p = -v + \lambda + fc + fd$ and thus $\lambda(p-1) = fc + fd$. We get

$$\begin{aligned}
\sum_{i=1}^{p-1}(c_i - c_0)^2 &\geq \sum_{i=1}^{p-1}\left(\frac{fc}{p-1} - c_0\right)^2 \\
&= (p-1)\left(\frac{fc}{p-1} + v - \lambda\right)^2 \\
&= (p-1)\left(\frac{fc}{p-1} + v - \frac{fc + fd}{p-1}\right)^2 \\
&= (p-1)\left(v - \frac{fd}{p-1}\right)^2.
\end{aligned}$$

This completes the proof of Claim 5.

Claim 6 $d = 0$ and

$$\sum_{i=1}^{p-1}(c_i - c_0)^2 = (p-1)v^2. \tag{64}$$

By (51) and (63), we obtain

$$(p-1)v^2 \geq (p-1)\left(v - \frac{fd}{p-1}\right)^2.$$

This implies $d \geq 0$. To prove Claim 6, it suffices to show $d = 0$, as Claim 6 then follows from Claim 5. Suppose $d > 0$. Recall $x_k = \sum_{i=0}^{p-1} c_{ki}$ and $d = \sum_{k\in B}\sum_{i=0}^{p-1} c_{ki} = \sum_{k\in B} x_k$. As $d > 0$, there is a subset B' of B such that such that $x_k > 0$ for $k \in B'$ and $\sum_{k\in B'} x_{k_j} \geq d$. Since the c_{ki}'s are integers, we get

$$\begin{aligned}
\sum_{k\in B'}\left(p\sum_{i=0}^{p-1} c_{ki}^2 - \left(\sum_{i=0}^{p-1} c_{ki}\right)^2\right) &= \sum_{k\in B'}\left(-x_k^2 + p\sum_{i=0}^{p-1} c_{ki}^2\right) \\
&\geq \sum_{j=1}^{\ell}\left(-x_k^2 + p\sum_{i=0}^{p-1} c_{ki}\right) \\
&= -\sum_{k\in B'} x_{k_j}^2 + p\sum_{k\in B'} x_k \\
&\geq -\left(\sum_{k\in B'} x_k\right)^2 + p\sum_{k\in B'} x_k,
\end{aligned} \tag{65}$$

where the last inequality holds because of $x_k > 0$ for all $k \in B'$. Recall $\sum_{k\in B'} x_k \geq d$. We have $\sum_{k\in B'} x_k < v$ by (61) and the function $x \mapsto -x^2 + px$ is increasing for $0 \leq x \leq v$, as $v < f/2 < p/4$ by assumption. Thus (65) implies

$$\sum_{k\in B'}\left(p\sum_{i=0}^{p-1} c_{ki}^2 - \left(\sum_{i=0}^{p-1} c_{ki}\right)^2\right) \geq -d^2 + pd. \tag{66}$$

Note that

$$p\sum_{i=0}^{p-1} c_i^2 - \left(\sum_{i=0}^{p-1} c_i\right)^2 = \sum_{i<j}(c_i - c_j)^2 \geq \sum_{i=1}^{p-1}(c_i - c_0)^2. \tag{67}$$

Combining (51), (63), (66), and (67), we get

$$\begin{aligned}
(p-1)v^2 &\geq (p-1)\left(v - \frac{fd}{p-1}\right)^2 + f(-d^2 + pd) \\
&= (p-1)v^2 + \frac{f^2d^2}{p-1} - 2vfd + f(-d^2 + pd).
\end{aligned}$$

This implies $-2vfd + f(-d^2 + pd) \le 0$, i.e., $2v \ge p - d$. Recall that $2v < f \le (p-1)/2$ by assumption and $d < v$ by (61). Combining these inequalities, we find

$$2v \ge p - d > p - v > p - f/2 > (p-1)/2 \ge f > 2v,$$

a contradiction. We thus conclude $d = 0$, which proves Claim 6.

We are finally ready to finish the proof of Theorem 4.5. From (67) and (64), we get

$$p\sum_{i=0}^{p-1} c_i^2 - \left(\sum_{i=0}^{p-1} c_i\right)^2 \ge (p-1)v^2. \tag{68}$$

But (51) and (68) imply

$$p\sum_{i=0}^{p-1} c_{ki}^2 - \left(\sum_{i=0}^{p-1} c_{ki}\right)^2 = 0$$

and thus $Y_k = 0$ for all $k \in B$, i.e., $Y = Y_0$.

By (51), (67), and (64), we have

$$(p-1)v^2 = \sum_{i<j}(c_i - c_j)^2 = \sum_{i=1}^{p-1}(c_i - c_0)^2$$

and thus $\sum_{0<i<j}(c_i - c_j)^2 = 0$. This implies $c_1 = c_2 = \ldots = c_{p-1}$. Hence $Y_0 = c_0 + c_1\sum_{i=1}^{p-1}\zeta_p^i = c_0 - c_1 \in \mathbb{Z}$. As $|Y_0|^2 = |Y|^2 = v^2$, we conclude $Y = \pm v$. This completes the proof of Theorem 4.5. □

To make use of Theorem 4.5, we need to show that cyclotomic integers $Y \in \mathbb{Q}(\zeta_{p^a})$ with $Y\overline{Y} = v^2$ (up to multiplication with a root of unity) are contained in suitable subfields of $\mathbb{Q}(\zeta_{p^a})$. This is the purpose of the following lemma.

Lemma 4.6. *Let p be an odd prime and let a, v be positive integers with $(v,p) = 1$. Suppose that $Y \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $|Y|^2 = v^2$. Let $q_1, \ldots, q_k$ are be distinct prime divisors of v and set*

$$f = \gcd(\mathrm{ord}_p(q_1), \ldots, \mathrm{ord}_p(q_k)).$$

Let K be the subfield of $\mathbb{Q}(\zeta_{p^a})$ with $[\mathbb{Q}(\zeta_{p^a}) : K] = f$. We have $Y\eta \in K$ for some root of unity η.

Proof. The proof is essentially the same as part of the proof of [9, Lemma 3.4]. For the convenience of the reader, we include a proof here. If $f = 1$, there is nothing to show. Thus suppose $f > 1$. Let t be an integer with $(p,t) = 1$ and $\mathrm{ord}_{p^a}(t) = \mathrm{ord}_p(t) = f$. Let σ be the automorphism of $\mathbb{Q}(\zeta_{p^a})$ determined by $\zeta_{p^a}^\sigma = \zeta_{p^a}^t$. Note that K is the fixed field of σ.

Let q be any prime divisor of v. By the definition of f, there is an integer $j(q)$ such that $\mathrm{ord}_{p^a}(q^{j(q)}) = f = \mathrm{ord}_{p^a}(t)$. As the multiplicative group $\mathbb{Z}_{p^a}^*$ modulo p^a is cyclic, this implies that $q^{j(q)}$ and t generate the same subgroup of $\mathbb{Z}_{p^a}^*$. Thus there is an integer $m(q)$ with $t \equiv q^{j(q)m(q)} \pmod{p^a}$. Hence the prime ideals of $\mathbb{Z}[\zeta_{p^a}]$ above $q\mathbb{Z}[\zeta_{p^a}]$ are invariant under σ by Result 2.8. Since this is true for every prime divisor q of v, we conclude that all prime ideals of $\mathbb{Z}[\zeta_{p^a}]$ above $v\mathbb{Z}[\zeta_{p^a}]$ are invariant under σ. Hence, by Result 2.7, there are roots of unity η, τ such that $(Y\tau)^\sigma = \pm\eta(Y\tau)$ and every prime divisor of the order of η divides $t-1$. But p does not divide $t-1$, as $\mathrm{ord}_p(t) = f > 1$. As $\eta \in \mathbb{Z}[\zeta_{p^a}]$, this implies $\eta = \pm 1$. Thus, replacing Y by $Y\tau$, if necessary, we may assume

$$Y^\sigma = \delta Y \tag{69}$$

with $\delta = \pm 1$.

First suppose that f is even. Then $\sigma^{f/2}$ is the complex conjugation in $\mathbb{Q}(\zeta_{p^a})$ and thus $\overline{Y} = Y^{\sigma^{f/2}} = \delta^{f/2} Y$ by (69). As $Y\overline{Y} = v^2$ by assumption, we conclude $\delta^{f/2}Y^2 = v^2$. As $\delta = \pm 1$, this implies $Y = \zeta_4^j v$ for some integer j. Since $\zeta_4 \notin \mathbb{Q}(\zeta_{p^a})$, we infer that j is even. Hence $Y = \pm v$ and thus, in particular, $Y \in K$.

Now suppose that f is odd. Applying σ repeatedly to (69), we get $Y^{\sigma^f} = \delta^f Y$. But σ^f is the identity, as $f = \mathrm{ord}_{p^a}(t)$. Hence $\delta^f = 1$ and thus $\delta = 1$, as f is odd. Therefore, $Y^\sigma = Y$ by (69), i.e., $Y \in K$. □

The following theorem combines the results of this section and strengthens the conclusion by employing Turyn's Result 2.10.

Theorem 4.7. *Let p be an odd prime and let a, v be positive integers with $(v,p) = 1$. Suppose that $X \in \mathbb{Z}[\zeta_{p^a}]$ satisfies $|X|^2 = v^2$. Write $v = v_0 v_1$ such that* $\mathrm{ord}_p(q) \equiv 0 \pmod 2$ *for all prime divisors q of v_0 and* $\mathrm{ord}_p(q) \equiv 1 \pmod 2$ *for all prime divisors q of v_1. If $v_1 = 1$ or*

$$v_1 > 1 \text{ and } \gcd(\mathrm{ord}_p(q_1), \dots, \mathrm{ord}_p(q_k)) > 2v_1 - 1, \tag{70}$$

where $q_1, \dots, q_k$ are the distinct prime divisors of v_1, then $X = \eta v$ for some root of unity η.

Proof. We first use Result 2.10 to show $X \equiv 0 \pmod{v_0}$. Let q be a prime divisor of v_0 and let q^b be the largest power of q dividing v_0. We claim

$$X \equiv 0 \pmod{q^b}. \tag{71}$$

By assumption, $\mathrm{ord}_p(q)$ is even. Thus $\mathrm{ord}_{p^a}(q)$ is also even, say $\mathrm{ord}_{p^a}(q) = 2e$. Hence q^e is an involution in the multiplicative group modulo p^a. As -1 is the only involution in this group, we have $q^e \equiv -1 \pmod{p^a}$. Thus q is self-conjugate modulo p^a. We have

$|X|^2 = v^2 \equiv 0 \pmod{q^{2b}}$ by assumption. Result 2.10 implies $X \equiv 0 \pmod{q^b}$, which proves (71). As (71) holds for every prime divisor q of v_0, we indeed have $X \equiv 0 \ (\bmod\ v_0)$.

Write

$$X = v_0 Y$$

where $Y \in \mathbb{Z}[\zeta_{p^a}]$ and $|Y|^2 = v_1^2$. To prove Theorem 4.7, we have to show $Y = \eta v_1$ for some root of unity η.

First suppose $v_1 = 1$. Then $v_0 = v$, $|Y| = |X|/v = 1$, and thus Y is a root of unity by Result 2.4. This proves the assertion in the case $v_1 = 1$. Thus we may assume $v_1 > 1$.

Recall that $q_1, \ldots, q_k$ are the prime divisors of v_1. Set $f = \gcd(\operatorname{ord}_p(q_1), \ldots, \operatorname{ord}_p(q_k))$. Let K be the subfield of $\mathbb{Q}(\zeta_{p^a})$ with $[\mathbb{Q}(\zeta_{p^a}) : K] = f$. As $|Y|^2 = v_1^2$, we have $Y\eta \in K$ for some root of unity η by Lemma 4.6. As $f > 2v_1 - 1$ by assumption (70), Theorem 4.5 implies $Y\eta = \pm v_1$. This completes the proof of Theorem 4.7. □

5 Necessary Conditions for the Existence of Twisted Cyclotomic Integers

We consider a solution of $Y\overline{Y} = v^2$ to be trivial if it has the form $Y = \eta v$ where η is a root a root of unity. Theorem 4.7 provides a necessary condition for the existence of nontrivial solutions to $Y\overline{Y} = v^2$. In fact, this condition is so strong that it yields the desired contradictions in most applications we are interested in. Thus it is essential to study cyclotomic integers which satisfy the conditions of Theorem 3.5, but are not contained in a field of the form $\mathbb{Q}(\zeta_{p^a})$. The following theorem provides valuable information on the structure of such cyclotomic integers.

Lemma 5.1. *Let p be an odd prime and let a, w be positive integers with $a \geq 2$ and $(p, w) = 1$. Suppose $X \in \mathbb{Z}[\zeta_{p^a w}] \setminus \mathbb{Z}[\zeta_{p^{a-1} w}]$ satisfies $|X|^2 = n$ where n is a positive integer. Write*

$$X = \sum_{i=0}^{p-1} A_i \zeta_{p^a}^i$$

with $A_i \in \mathbb{Z}[\zeta_{p^{a-1} w}]$. Let d be a divisor of w. If

$$A_i \in \mathbb{Z}[\zeta_{p^{a-1} d}] \tag{72}$$

for $i = 1, \ldots, p-1$, then

$$A_0 \in \mathbb{Z}[\zeta_{p^{a-1} d}]. \tag{73}$$

Proof. Note

$$n = |X|^2 = \sum_{i,j=0}^{p-1} A_i \overline{A_j} \zeta_{p^a}^{i-j} = \sum_{k=0}^{p-1} \zeta_{p^a}^k \left(\sum_{l=k}^{p-1} A_l \overline{A_{l-k}} + \overline{\zeta_{p^{a-1}}} \sum_{l=0}^{k-1} A_l \overline{A_{p-k+l}} \right).$$

As $\{\zeta_{p^a}^k : k = 0, \ldots, p-1\}$ is independent over $\mathbb{Q}(\zeta_{p^{a-1}w})$, we infer

$$\sum_{l=0}^{p-1} A_l\overline{A_l} = n, \tag{74}$$

$$\sum_{l=k}^{p-1} A_l\overline{A_{l-k}} + \overline{\zeta_{p^{a-1}}} \sum_{l=0}^{k-1} A_l\overline{A_{p-k+l}} = 0 \tag{75}$$

for $k = 1, \ldots, p-1$. From (72) and (74), we conclude

$$A_0\overline{A_0} = n - \sum_{i=1}^{p-1} A_i\overline{A_i} \in \mathbb{Z}[\zeta_{p^{a-1}d}]. \tag{76}$$

Note that

$$A_k\overline{A_0} + \overline{\zeta_{p^{a-1}}}A_0\overline{A_{p-k}} = -\sum_{l=k+1}^{p-1} A_l\overline{A_{l-k}} - \overline{\zeta_{p^{a-1}}}\sum_{l=1}^{k-1} A_l\overline{A_{p-k+l}} \tag{77}$$

for $k = 1, \ldots, p-1$ by (75). Denote the right hand side of (77) by T_k. As T_k does not contain any term involving A_0, we have $T_k \in \mathbb{Z}[\zeta_{p^{a-1}d}]$ by (72).

Suppose $A_j \neq 0$ for some j with $1 \leq j \leq p-1$. If $A_{p-j} = 0$, then (77) implies $A_0 = \overline{T_j}/\overline{A_j} \in \mathbb{Q}(\zeta_{p^{a-1}d})$, contradicting (73). Hence

$$A_{p-j} \neq 0 \text{ for all } j > 0 \text{ with } A_j \neq 0. \tag{78}$$

Now suppose $A_j \neq 0$ and $A_k \neq 0$ for some $j, k > 0$ with $j \neq p-k$. We have

$$\begin{aligned} A_j\overline{A_0} + \overline{\zeta_{p^{a-1}}}A_0\overline{A_{p-j}} &= T_j, \\ A_k\overline{A_0} + \overline{\zeta_{p^{a-1}}}A_0\overline{A_{p-k}} &= T_k \end{aligned} \tag{79}$$

by (77). We now view (79) as a linear system with variables A_0 and $\overline{A_0}$. Suppose $A_j\overline{A_{p-k}} \neq A_k\overline{A_{p-j}}$. Then the determinant of the coefficient matrix of the linear system (79) is nonzero. As $A_j, A_k, A_{p-j}, A_{p-k}, T_j, T_k \in \mathbb{Q}(\zeta_{p^{a-1}d})$, this implies $A_0 \in \mathbb{Q}(\zeta_{p^{a-1}d}) \cap \mathbb{Z}[\zeta_{p^{a-1}d}] = \mathbb{Z}[\zeta_{p^{a-1}d}]$, contradicting (73). We conclude

$$A_j\overline{A_{p-k}} = A_k\overline{A_{p-j}} \tag{80}$$

for all $j, k > 0$ with $A_j \neq 0$ and $A_k \neq 0$.

As $X \notin \mathbb{Z}[\zeta_{p^{a-1}w}]$ by assumption, there is k with $1 \leq k \leq p-1$ and $A_k \neq 0$. Set $\alpha = \overline{A_{p-k}}/A_k$. Note that $\alpha \in \mathbb{Q}(\zeta_{p^{a-1}d})$ by (72). Moreover,

$$\overline{A_{p-j}} = \frac{A_j\overline{A_{p-k}}}{A_k} = \alpha A_j \tag{81}$$

for all $j > 0$ with $A_j \neq 0$ by (80). But (81) also holds for those $j > 0$ with $A_j = 0$, since $A_{p-j} = 0$ in this case by (78). Hence (81) holds for $j = 1, \ldots, p-1$.

Write $Z = \sum_{i=1}^{p-1} A_i \zeta_{p^a}^i$ and note that $X = A_0 + Z$. Using (81), we compute

$$\begin{aligned}\overline{Z} &= \sum_{i=1}^{p-1} \overline{A_i} \zeta_{p^a}^{-i} \\ &= \overline{\zeta_{p^{a-1}}} \sum_{i=1}^{p-1} \overline{A_i} \zeta_{p^a}^{p-i} \\ &= \overline{\zeta_{p^{a-1}}} \sum_{i=1}^{p-1} \overline{A_{p-i}} \zeta_{p^a}^{i} \\ &= \alpha \overline{\zeta_{p^{a-1}}} \sum_{i=1}^{p-1} A_i \zeta_{p^a}^{i} \\ &= \alpha \overline{\zeta_{p^{a-1}}} Z.\end{aligned}$$

Recall that $|X|^2 = n$. Hence

$$\begin{aligned} n &= A_0\overline{A_0} + Z\overline{A_0} + \overline{Z}A_0 + Z\overline{Z} \\ &= A_0\overline{A_0} + Z(\overline{A_0} + \alpha\overline{\zeta_{p^{a-1}}}A_0) + \alpha\overline{\zeta_{p^{a-1}}}Z^2. \end{aligned} \tag{82}$$

Note that (82) is a quadratic equation in the variable Z with coefficients from $\mathbb{Q}(\zeta_{p^{a-1}w})$. This implies that the degree of the extension $\mathbb{Q}(\zeta_{p^{a-1}w}, Z)/\mathbb{Q}(\zeta_{p^{a-1}w})$ is at most 2. But $Z = X - A_0 \in \mathbb{Q}(\zeta_{p^a w}) \setminus \mathbb{Q}(\zeta_{p^{a-1}w})$, as $X \in \mathbb{Q}(\zeta_{p^a w}) \setminus \mathbb{Q}(\zeta_{p^{a-1}w})$ by assumption and $A_0 \in \mathbb{Q}(\zeta_{p^{a-1}w})$. Thus the degree of the extension $\mathbb{Q}(\zeta_{p^{a-1}w}, Z)/\mathbb{Q}(\zeta_{p^{a-1}w})$ is divisible by p. This is a contradiction, as p is odd. □

In order to make use of Lemma 5.1, we need the following lemma which uses automorphisms to obtain a lower bound for Cassel's $\mathcal{M}$-function.

Lemma 5.2. *Let $w = r^a v$ where r is an odd prime and a, v are positive integers with $(r, v) = 1$. Let t be and integer with $(w, t) = 1$ and write $f = \operatorname{ord}_r(t)$. Define $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_w)/\mathbb{Q})$ by $\zeta_w^\sigma = \zeta_w^t$. Suppose $X \in \mathbb{Z}[\zeta_w] \setminus \mathbb{Z}[\zeta_{r^{a-1}v}]$ satisfies $X^\sigma = \delta X$ for some $\delta \in \mathbb{Z}[\zeta_{r^{a-1}v}]$. Then*

$$\mathcal{M}(X) \geq \begin{cases} \frac{f(r-f)}{r-1} & \text{if } f < r-1, \\ \frac{r+1}{4} & \text{if } f = r-1. \end{cases} \tag{83}$$

Remark 5.3. In the case where $v = 1$ and $f = r - 1$ in Lemma 5.2, it is possible to prove $\mathcal{M}(X) \geq r-1$ (instead of $\mathcal{M}(X) \geq (r+1)/4$). This can be used to obtain an improvement of our main result, Theorem 6.1. As the required argument is quite complicated, however, and we have not found any additional cases of circulant Hadamard matrices it would rule out, we skip that.

Proof of Lemma 5.2. Write $X = \sum_{i=0}^{r-1} X_i \zeta_{r^a}^i$ with $X_i \in \mathbb{Z}[\zeta_{r^{a-1}v}]$. As $X \notin \mathbb{Z}[\zeta_{r^{a-1}v}]$, there is $j > 0$ with $X_j \neq 0$. Let $k : \{0, \ldots, r-1\} \to \{0, \ldots, r-1\}$ be the map such that $k(i)$

is the unique integer with $0 \le k(i) \le r-1$ and $ti \equiv k(i) \pmod{r}$. Note that all orbits of k on $\{1,\dots,r-1\}$ have length f, since $\mathrm{ord}_r(t) = f$. By assumption,

$$X^\sigma = \sum_{i=0}^{r-1} X_i^\sigma \zeta_{r^a}^{ti} = \sum_{i=0}^{r-1} (X_i^\sigma \zeta_{r^a}^{ti-k(i)}) \zeta_{r^a}^{k(i)} = \delta X = \sum_{i=0}^{r-1} (\delta X_i) \zeta_{r^a}^{i}. \tag{84}$$

Case 1 $a \ge 2$. Note that $X_i^\sigma \zeta_{r^a}^{ti-k(i)} \in \mathbb{Z}[\zeta_{r^{a-1}v}]$, as $X_i \in \mathbb{Z}[\zeta_{r^{a-1}v}]$ and $ti \equiv k(i) \pmod{r}$. Moreover, $\delta \in \mathbb{Z}[\zeta_{r^{a-1}v}]$ by assumption, and $\{1, \zeta_{r^a}, \dots, \zeta_{r^a}^{r-1}\}$ is linearly independent over $\mathbb{Q}(\zeta_{r^{a-1}v})$. Hence (84) implies $X_i^\sigma \zeta_{r^a}^{ti-k(i)} = \delta X_{k(i)}$ for $i = 0, \dots, r-1$. Thus, as $X_j \ne 0$, we have $X_{k(j)} \ne 0$ as well. Consequently, $X_j, X_{k(j)}, \dots, X_{k^{f-1}(j)}$ are all nonzero. Applying Result 2.12 (a) and (5), we obtain $\mathcal{M}(X) \ge \sum_{i=0}^{f-1} \mathcal{M}(X_{k^i(j)}) \ge f$. This implies (83).

Case 2 $a = 1$. Note that the representation of X as $\sum_{i=0}^{r-1} X_i \zeta_{r^a}^i$ is not unique, but we may assume the representation is chosen such that $T = |\{i : X_i \ne 0\}|$ is minimum among all possible representations of X. It follows that, for each fixed i, there are at most $r - T$ indices k with $X_k = X_i$ (otherwise, the representation $X = \sum_{k=0}^{r-1} (X_k - X_i)\zeta_r^k$ would have less than T nonzero $(X_k - X_i)$'s). Thus, for any fixed i, the number of indices k with $X_i - X_k \ne 0$ is at least T. Therefore, by Result 2.12 (b) and (5), we obtain

$$(r-1)\mathcal{M}(X) = \sum_{i<k} \mathcal{M}(X_i - X_k) = \frac{1}{2}\sum_{i \ne k} \mathcal{M}(X_i - X_k) \ge \frac{rT}{2}.$$

If $T \ge (r+1)/2$, then we conclude $\mathcal{M}(X) \ge r(r+1)/4(r-1)) > (r+1)/4$. This implies (83).

Now suppose $T < (r+1)/2$. Then $T \le (r-1)/2$, as r is odd. Let $\mathcal{S} = \{i : X_i \ne 0\}$. Then $|\mathcal{S}| = T \le (r-1)/2$. Note that $\zeta_r^{ti} = \zeta_r^{k(i)}$. As $X^\sigma = \delta X$, we have

$$X^\sigma = \sum_{i \in \mathcal{S}} X_i^\sigma \zeta_r^{it} = \sum_{i \in \mathcal{S}} X_i^\sigma \zeta_r^{k(i)} = \delta \sum_{i \in \mathcal{S}} X_i \zeta_r^i. \tag{85}$$

Moreover, $\delta \in \mathbb{Z}[\zeta_v]$, $X_i \in \mathbb{Z}[\zeta_v]$, and $X_i^\sigma \in \mathbb{Z}[\zeta_v]$ for all i, since $a = 1$. As $|\mathcal{S}| \le (r-1)/2$, the set

$$\mathcal{T} = \{\zeta_r^i : i \in \mathcal{S}\} \cup \{\zeta_r^{k(i)} : i \in \mathcal{S}\}$$

contains at most $r-1$ elements of $\{\zeta_r^i : i = 0, \dots, r-1\}$. Hence $\mathcal{T}$ is linearly independent over $\mathbb{Q}(\zeta_v)$. Therefore, (85) implies $\{k(i) : i \in \mathcal{S}\} = \mathcal{S}$. Thus, as $j > 0$ and $X_j \ne 0$, we conclude that $\mathcal{S}$ contains a whole orbit of k on $\{1, \dots, r-1\}$. Hence $|\mathcal{S}| \ge f$. Moreover,

$$(r-1)\mathcal{M}(X) = \sum_{i<k} \mathcal{M}(X_i - X_k) \ge \sum_{i \in \mathcal{S}} \sum_{k \notin \mathcal{S}} \mathcal{M}(X_i - X_k) \ge |\mathcal{S}|(r - |\mathcal{S}|). \tag{86}$$

As $f \le |\mathcal{S}| \le (r-1)/2$ and the function $g(x) = x(r-x)$ is increasing for $1 \le x \le r/2$, (86) implies $\mathcal{M}(X) \ge f(r-f)/(r-1)$. This proves (83) for $f < r-1$.

Finally, if $f = r-1$, we set $t' = t^2$ and apply (83) with t replaced by t' and σ replaced by σ^2. As $\mathrm{ord}_r(t') = (r-1)/2$, this shows $\mathcal{M}(X) \ge (r-1)(r+1)/4(r-1) = (r+1)/4$. This completes the proof of Lemma 5.2. □

In the following theorem, we combine Lemmas 5.1 and 5.2 to obtain a lower bound on the complex modulus of cyclotomic integers. We remark that we use Notation 2.15 again.

Theorem 5.4. *Let p be an odd prime and let a, w be positive integers, where $a \geq 2$, w is odd, and $(w,p) = 1$. Suppose $X \in \mathbb{Z}[\zeta_{p^a w}]$ satisfies $|X|^2 = n$ where n is a positive integer with $(n,p) = 1$. Furthermore, suppose that*

$$X\eta \notin \mathbb{Z}[\zeta_{p^{a-1}w}] \text{ and } X\eta \notin \mathbb{Z}[\zeta_{p^a}] \tag{87}$$

for all roots of unity η. Let t be an integer with $(t,pw) = 1$ and write $f = \mathrm{ord}_{p^a}(t)$. Suppose $f > 1$, that f divides $p-1$, and that, for every prime divisor q of n, there is an integer s_q with

$$q^{s_q} \equiv t \pmod{\omega(p^a w, q)}. \tag{88}$$

Let S be the set of prime divisors of w and set

$$f_s = \min\left\{\frac{s-1}{2}, \frac{\mathrm{ord}_{ps}(t)}{\mathrm{ord}_p(t)}\right\}$$

for $s \in S$. If $\nu_2(\mathrm{ord}_p(t)) \geq 1$, set

$$S' = \{s \in S : \nu_2(\mathrm{ord}_s(t)) = \nu_2(\mathrm{ord}_p(t))\},$$

otherwise, set $S' = \emptyset$. Then $S \setminus S'$ is nonempty and

$$n \geq \mathrm{ord}_p(t) \min\left\{\frac{f_s(s-f_s)}{s-1} : s \in S \setminus S'\right\}. \tag{89}$$

Proof. Note that $\mathrm{ord}_p(t) = \mathrm{ord}_{p^a}(t) = f$, as f divides $p-1$ by assumption. Define $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^a w})/\mathbb{Q})$ by $\tau(\zeta_{p^a w}) = \zeta_{p^a w}^t$. By assumption (88) and Result 2.8, all prime ideals of $\mathbb{Z}[\zeta_{p^a w}]$ above $n\mathbb{Z}[\zeta_{p^a w}]$ are invariant under τ. Hence, by Result 2.7, there are roots of unity $\xi_1, \xi_2 \in \mathbb{Z}[\zeta_{p^a w}]$ such that $(X\xi_1)^\tau = \pm\xi_2(X\xi_1)$ and every prime divisor of the order of ξ_2 divides $t-1$. Note that the order of ξ_2 is not divisible by p, as $\mathrm{ord}_p(t) > 1$ by assumption and thus p does not divide $t-1$. In particular, $\zeta_2 \in \mathbb{Z}[\zeta_{p^{a-1}w}]$.

Write

$$Y = X\xi_1 = \sum_{i=0}^{p-1} A_i \zeta_{p^a}^i \tag{90}$$

with $A_i \in \mathbb{Z}[\zeta_{p^{a-1}w}]$ and $\delta = \pm\xi_2$. Note $Y^\tau = \delta Y$. Let $k : \{0,\dots,p-1\} \to \{0,\dots,p-1\}$ be the function such that $k(i)$ $it \equiv k(i) \pmod{p}$. As $Y^\tau = \delta Y$, we have

$$\sum_{i=0}^{p-1}\left(A_i^\tau \zeta_{p^a}^{it-k(i)}\right)\zeta_{p^a}^{k(i)} = \sum_{i=0}^{p-1}(\delta A_i)\zeta_{p^a}^i$$

and thus

$$A_i^\tau \zeta_{p^a}^{it-k(i)} = \delta A_{k(i)} \tag{91}$$

for $i = 0, \ldots, p-1$, as $\{1, \zeta_{p^a}, \ldots, \zeta_{p^a}^{p-1}\}$ is linearly independent over $\mathbb{Q}(\zeta_{p^{a-1}w})$.

Since $Y \notin \mathbb{Z}[\zeta_{p^{a-1}w}]$ by assumption (87), we have $A_j \neq 0$ for some j with $1 \leq j \leq p-1$. Moreover, (91) implies

$$A_{k^i(j)} = \eta_i A_j, \; i = 0, \ldots, f-1, \tag{92}$$

for some root of unity η_i (depending on i). Note that (92) implies $\mathcal{M}(A_{k^i(j)}) = \mathcal{M}(A_j)$ for $j = 0, \ldots, f-1$. By Result 2.12 (a), we obtain

$$n = \mathcal{M}(X) \geq \sum_{i=0}^{f-1} \mathcal{M}(A_{k^i(j)}) = f\mathcal{M}(A_j). \tag{93}$$

To prove (89), we need to find a lower bound for $\mathcal{M}(A_j)$.

Claim Let r be a prime divisor of w and write $b = \nu_r(w)$. If $A_j \notin \mathbb{Z}[\zeta_{p^{a-1}w/r^b}]$, then

$$\mathcal{M}(A_j) \geq \frac{f_r(r - f_r)}{r - 1}. \tag{94}$$

Let $\sigma = \tau^f$. As $Y^\tau = \delta\sigma$, we have

$$Y^\sigma = (\delta Y^\tau)^{\tau^{f-1}} = \cdots = \left(\prod_{i=0}^{f-1} \delta^{\tau^i}\right) Y. \tag{95}$$

Moreover, σ fixes ζ_{p^a}, since $f = \mathrm{ord}_{p^a}(t)$. Hence, using the usual independence argument, we see that (95) implies $A_j^\sigma = \eta A_j$, where $\eta = \prod_{i=0}^{f-1} \delta^{\tau^i}$. Recall $\delta = \pm\xi_2$ and that every prime divisor of the order of ξ_2 divides $t-1$. In particular, the order of δ is not divisible by p.

First suppose that the order of η is divisible by r. Then r divides the order of ξ_2 and thus r divides $t-1$. This implies $\mathrm{ord}_{pr}(t) = \mathrm{ord}_p(t)$ and $f_r = 1$. Hence (94) holds by (5), as $A_j \neq 0$.

On the other hand, if r does not divide the order of η, then $\eta \in \mathbb{Z}[\zeta_{w/r^b}]$, as the order of δ is not divisible by p. Moreover, since $A_j \in \mathbb{Z}[\zeta_{p^{a-1}w}]$ by the definition of the A_i's and $A_j \notin \mathbb{Z}[\zeta_{p^{a-1}w/r^b}]$ by the assumption of the claim, there is a nonnegative integer c such that $A_j \in \mathbb{Z}[\zeta_{p^{a-1}w/r^c}] \setminus \mathbb{Z}[\zeta_{p^{a-1}w/r^{c+1}}]$. Hence we can apply Lemma 5.2 to A_j and this shows that (94) holds. This completes the proof of the claim.

Finally, by (93) and (94), to prove Theorem 5.4, it suffices to show that

$$A_j \notin \mathbb{Z}[\zeta_{p^{a-1}w/r^{\nu_r(w)}}] \tag{96}$$

for some $j > 0$ and some $r \in S \setminus S'$.

Set $v = \prod_{s \in S'} s^{\nu_s(w)}$. Suppose (96) does not hold, i.e., $A_j \in \mathbb{Z}[\zeta_{p^{a-1}w/r^{\nu_r(w)}}]$ for all $j > 0$ and all $r \in S \setminus S'$. Then $A_0 \in \mathbb{Z}[\zeta_{p^{a-1}w/r^{\nu_r(w)}}]$ for all $j > 0$ and all $r \in S \setminus S'$ by Lemma 5.1. This implies $Y \in \mathbb{Z}[\zeta_{p^a v}]$. Hence it suffices to show $Y \notin \mathbb{Z}[\zeta_{p^a v}]$.

Suppose $Y \in \mathbb{Z}[\zeta_{p^a v}]$. Let s be a prime divisor of v. As $s \in S'$, we have

$$\nu_2(\text{ord}_s(t)) = \nu_2(\text{ord}_p(t)) \geq 1$$

by the definition of S'. Hence there is an integer $x \geq 1$ such that

$$\text{ord}_p(t) = 2^x y_p \text{ and } \text{ord}_s(t) = 2^x y_s \tag{97}$$

where y_p and y_s are odd integers. Set

$$z = 2^{x-1} y_p p^{a-1} \prod_{r \in S'} y_r r^{\nu_s(v)-1}.$$

Using the fact that p and v are odd by assumption, it is straightforward to verify that

$$t^z \equiv -1 \pmod{p^a} \text{ and } t^z \equiv -1 \pmod{s} \tag{98}$$

for all $s \in S'$. Note that (88) and (98) imply that n is self-conjugate modulo $p^a v$. Recall that we assume $Y \in \mathbb{Z}[\zeta_{p^a v}]$ and $|Y|^2 = n$. Thus Proposition 2.11 implies

$$Y\beta = w^2 \prod_{i=1}^{k} G_{p_i} \tag{99}$$

for integer w and some root of unity β, where the p_i's are distinct prime divisors of $(n, p^a v)$. Recall that $(n, p) = 1$ by assumption. Hence each p_i divides v. Thus, as $G_{p_i} \in \mathbb{Z}[\zeta_{p_i}]$, the right hand side of (99) is contained in $\mathbb{Z}[\zeta_v]$. Hence (99) implies $X\xi_1\eta = Y\eta \in \mathbb{Z}[\zeta_v]$, contradicting assumption (87). □

6 Necessary Conditions for the Existence of Circulant Hadamard Matrices

We are now ready to prove the main result of this paper. We use Notation 2.15 again.

Theorem 6.1. *Let $u > 1$ be an odd integer and suppose that a circulant Hadamard matrix of order $4u^2$ exists. Let d be a divisor of u with $(d, u/d) = 1$ and let p be a prime divisor of u/d such that*

$$\varphi(d^2) < \frac{p\varphi(u^2)}{2u^2}. \tag{100}$$

Let p^a be the largest power of p dividing u/d. Let m be a divisor of u with $m \equiv 0 \pmod{p^a}$ such that

$$\nu_p(\text{ord}_{p^{2a}}(q)) > \nu_p(\text{ord}'_{u/d}(q)) \tag{101}$$

for all prime divisors $q \neq p$ of m.

Let t be an integer coprime to u/d such that $\mathrm{ord}_p(t) > 1$ *and, for every prime divisor q of u/m, there is an integer s_q with*

$$q^{s_q} \equiv t \pmod{\omega(u^2/d^2, q)}. \tag{102}$$

Let S be the set of prime divisors of $u/(dp^a)$. If $\nu_2(\mathrm{ord}_p(t)) \geq 1$*, set*

$$S' = \{s \in S : \nu_2(\mathrm{ord}_s(t)) = \nu_2(\mathrm{ord}_p(t))\}$$

and $S' = \emptyset$ otherwise. For $s \in S \setminus S'$, set

$$f_s = \min\left\{\frac{\mathrm{ord}_{ps}(t)}{\mathrm{ord}_p(t)}, \frac{s-1}{2}\right\}.$$

Then

$$\mathrm{ord}_p(t) \leq \frac{u^4}{m^4} \max\left\{\left\{\frac{2m^2}{u^2}\right\} \cup \left\{\frac{(s-1)}{f_s(s-f_s)} : s \in S \setminus S'\right\}\right\}. \tag{103}$$

Remark 6.2. For the application of Theorem 6.1 to a specific u, it is necessary to identify appropriate values for p, m, and t. First of all, p usually is chosen as one of the largest prime divisors of u (each possible p has to be tested). Once p is chosen, we take m as large as possible, i.e., we include all prime factors of u in m which satisfy (101). The choice of t is more complicated. Usually, we choose t such that $\mathrm{ord}_p(t)$ is as large as possible among those t which satisfy (102). Nevertheless, in the frequently occurring case where u/m is a prime power, say $u/m = q^b$, we simply can take an integer t with $t \equiv q \pmod{\omega(u^2/d^2, q)}$ and $t \equiv 1 \pmod{q^{2b}}$ (which exists due to the Chinese remainder theorem).

Proof of Theorem 6.1. By Theorem 3.5, there is $X \in \mathbb{Z}[\zeta_{u^2/d^2}]$ with

$$|X|^2 = \frac{u^4}{m^4} \text{ and } X\eta \notin \mathbb{Z}[\zeta_{u^2/(pd^2)}] \tag{104}$$

for all roots of unity η.

First suppose $X\eta \in \mathbb{Z}[\zeta_{p^{2a}}]$ for some root of unity η. Note that p does not divide u/m, as $m \equiv 0 \pmod{p^a}$. Moreover, $u/d \equiv 0 \pmod{p}$ by assumption. Thus, by (102), for every prime divisor q of u/m, there is an integer s_q with $q^{s_q} \equiv t \pmod{p}$. This implies $\mathrm{ord}_p(q) \equiv 0 \pmod{\mathrm{ord}_p(t)}$ and thus

$$\gcd(\mathrm{ord}_p(q_1), \ldots, \mathrm{ord}_p(q_t)) \equiv 0 \pmod{\mathrm{ord}_p(t)}, \tag{105}$$

where the q_i's are the distinct prime divisors of u/m. Note that $X\eta \neq u^2/m^2$ for all roots of unity η by (104). Thus, in view of (105), Theorem 4.7 implies $2u^2/m^2 \geq \mathrm{ord}_p(t)$, i.e.,

$$\mathrm{ord}_p(t) \leq \frac{u^4}{m^4}\frac{2m^2}{u^2}.$$

Hence (103) holds.

Now suppose $X\eta \notin \mathbb{Z}[\zeta_{p^{2a}}]$ for all roots of unity η. Then we have

$$|X|^2 = \frac{u^4}{m^4}, \quad X\eta \notin \mathbb{Z}[\zeta_{u^2/(pd^2)}], \text{ and } X\eta \notin \mathbb{Z}[\zeta_{p^{2a}}] \tag{106}$$

for all roots of unity η. In view of (102) and (106), we can apply Theorem 5.4 to X, which shows that (103) holds. □

In the numerous cases where u/m is a prime power, say q^b, we obtain the following improvement of Theorem 6.1. The difference to Theorem 6.1 is that the number $(q-1)/(f_q(q-f_q))$ is not included in (109) in the set over which the maximum is taken. Note that all numbers in this set are at most 1. Hence those numbers in the set are critical which are relatively close to 1. In most cases, q is relatively small and thus $(q-1)/(f_q(q-f_q))$ is relatively close to 1. Therefore, removing $(q-1)/(f_q(q-f_q))$ from the set sometimes significantly reduces the value of the maximum.

Theorem 6.3. *Let $u > 1$ be an odd integer and suppose that a circulant Hadamard matrix of order $4u^2$ exists. Let d be a divisor of u with $(d, u/d) = 1$ and let p be a prime divisor of u/d such that*

$$\varphi(d^2) < \frac{p\varphi(u^2)}{2u^2}. \tag{107}$$

Let p^a be the largest power of p dividing u/d. Let $q \neq p$ be a prime dividing u such that

$$\nu_p(\mathrm{ord}_{p^{2a}}(r)) > \nu_p(\mathrm{ord}'_{u/d}(r)) \tag{108}$$

for every prime divisor r of u with $r \neq p$ and $r \neq q$.

Let q^b be the largest power of q dividing u, and let S be the set of prime divisors of u/d which are different from p. If $\nu_2(\mathrm{ord}_p(t)) \geq 1$, set

$$S' = \{s \in S : \nu_2(\mathrm{ord}_s(t)) = \nu_2(\mathrm{ord}_p(t))\}$$

and $S' = \emptyset$ otherwise. For $s \in S \setminus S'$, set

$$f_s = \min\left\{\frac{\mathrm{ord}_{ps}(q)}{\mathrm{ord}_p(q)}, \frac{s-1}{2}\right\}.$$

Then

$$\mathrm{ord}_p(q) \leq q^{4b} \max\left\{\left\{\frac{2}{q^2}\right\} \cup \left\{\frac{(s-1)}{f_s(s-f_s)} : s \in S \setminus (S' \cup \{q\})\right\}\right\}. \tag{109}$$

Proof. Let t be an integer with $t \equiv q \pmod{\omega(u^2/d^2, q)}$ and $t \equiv 1 \pmod{q^{2b}}$. Note $\mathrm{ord}_s(t) = \mathrm{ord}_s(q)$ for all prime divisors $s \neq q$ of u/d. We use Theorem 6.1 with $m = u/q^b$ and the t we just have defined. Note that the essential difference between (109) and (103) is that the number $(q-1)/(f_q(q-f_q))$ is not included in (109) in the set over which the maximum is taken. Thus the value of the maximum on the right hand side of (109) may be smaller than that on the right hand side of (103), and we have to justify this improvement.

First of all, if q does not divide u/d, then the right hand sides of (103) and (109) coincide and thus (109) follows from Theorem 6.1.

Hence we can assume that q divides u/d. As in the proof of Theorem 6.1, we see that there is $X \in \mathbb{Z}[\zeta_{u^2/d^2}]$ with

$$|X|^2 = \frac{u^4}{m^4} = q^{4b} \text{ and } X\eta \notin \mathbb{Z}[\zeta_{u^2/(pd^2)}] \tag{110}$$

for all roots of unity η. Furthermore,

$$\mathrm{N}(X) = \frac{u^{2p}}{m^{2p}} = q^{2bp} \tag{111}$$

by Theorem 3.5, where N denotes the norm of $\mathbb{Q}(\zeta_{u^2/d^2})$ relative to $\mathbb{Q}(\zeta_{u^2/(pd^2)})$.

If there is a root of unity τ such that $X\tau \in \mathbb{Z}[\zeta_{u^2/(d^2q^{2b})}]$, then, following the same argument as in the proof of Theorem 6.1, we do not need to include the number $(q-1)/(f_q(q-f_q))$ in (109) in the set over which the maximum is taken. Hence (109) follows from Theorem 5.4 in this case.

Thus we can assume

$$X\tau \notin \mathbb{Z}[\zeta_{u^2/(d^2q^{2b})}] \tag{112}$$

for all roots of unity τ. Recall $|X|^2 = q^{4b}$. Result 2.13 and (112) imply

$$X \ = \zeta_{u^2/d^2}^{j} G(\chi) Z \tag{113}$$

for some integer j, where χ is a multiplicative character of $\mathbb{F}_q$, $Z \in \mathbb{Z}[\zeta_{u^2/(d^2q^{2b})}]$, and $|Z|^2 = q^{4b-1}$. Note that χ cannot be the trivial character. Otherwise, $\chi(x) = 1$ for all $x \in \mathbb{F}_q \setminus \{0\}$, which implies $G(\chi) = -1$ and thus $|Z|^2 = |X|^2/|G(\chi)|^2 = q^{4b}$, contradicting $|Z|^2 = q^{4b-1}$.

Let x denote the order of χ. Note that x divides $q-1$. Furthermore, as χ is nontrivial, we have $x \geq 2$. Let β be a primitive element of $\mathbb{F}_q$ with $\chi(\beta) = \zeta_x$. Note $G(\chi) \in \mathbb{Z}[\zeta_{qx}]$.

Let α be the automorphism of $\mathbb{Q}(\zeta_{qx})$ defined by $\zeta_q^\alpha = \zeta_q^\beta$ and $\zeta_x^\alpha = \zeta_x$. Then

$$\begin{aligned} G(\chi)^\alpha &= \left(\sum_{x\in\mathbb{F}_q} \chi(x)\zeta_q^x\right)^\alpha \\ &= \left(\sum_{i=1}^{q-1} \chi(\beta^i)\zeta_q^{\beta^i}\right)^\alpha \\ &= \sum_{i=1}^{q-1} \zeta_x^i \zeta_q^{\alpha^{i+1}} \\ &= \zeta_x^{-1} \sum_{i=1}^{q-1} \zeta_x^{i+1} \zeta_q^{\alpha^{i+1}} \\ &= \zeta_x^{-1} \sum_{i=1}^{q-1} \zeta_x^{i} \zeta_q^{\alpha^{i}} \\ &= \zeta_x^{-1} G(\chi). \end{aligned} \tag{114}$$

As $G(\chi) \in \mathbb{Z}[\zeta_{u^2/d^2}]$ and thus $G(\chi)^\alpha \in \mathbb{Z}[\zeta_{u^2/d^2}]$, we have

$$\zeta_x = G(\chi)/G(\chi)^\alpha \in \mathbb{Z}[\zeta_{u^2/d^2}]. \tag{115}$$

by (114).

Now suppose $x > 2$. Note that x is not divisible by 4 by (115), since u^2/d^2 is odd. Thus x has an odd prime divisor, say x_0. Note that x_0 divides u^2/d^2 by (115). Recall that x divides $q-1$. Thus x_0 also divides $q-1$. If $x_0 = p$, then $\operatorname{ord}_p(q) = 1$ and (109) trivially holds. If $x_0 \neq p$, then $x_0 \in S \setminus S'$, as $\operatorname{ord}_{x_0}(q) = 1$ and, moreover, $f_{x_0} = 1$. Hence the maximum on the right hand side of (109) equals 1 and (109) follows from Theorem 6.1 (note that the maximum in (103) is at most 1 in any case).

So we may assume $x = 2$. We claim

$$Z\eta \notin \mathbb{Z}[\zeta_{u^2/(pd^2q^{2b})}] \tag{116}$$

for all roots of unity η. As $x = 2$, we have

$$G(\chi) \in \mathbb{Z}[\zeta_q]. \tag{117}$$

Suppose $Z\eta \in \mathbb{Z}[\zeta_{u^2/(pd^2q^{2b})}]$ for some root of unity η. Then

$$G(\chi)Z\eta \in \mathbb{Z}[\zeta_{u^2/(pd^2)}] \tag{118}$$

by (117), since q divides u/d by assumption. Recall $X \in \mathbb{Z}[\zeta_{u^2/d^2}]$. Combining (113) and (118), we get

$$X\zeta_{u^2/d^2}^{-j}\eta = G(\chi)Z\eta \in \mathbb{Z}[\zeta_{u^2/(pd^2)}].$$

But this contradicts (110). This proves (116).

Next, we claim

$$Z\eta \notin \mathbb{Z}[\zeta_{p^{2a}}] \tag{119}$$

for all roots of unity η. Recall that N denotes the norm of $\mathbb{Q}(\zeta_{u^2/d^2})$ relative to $\mathbb{Q}(\zeta_{u^2/(pd^2)})$. By (111) and (113), we have

$$q^{2bp} = \mathrm{N}(X) = \mathrm{N}(\zeta_{u^2/d^2}^{j})\mathrm{N}(G(\chi))\mathrm{N}(Z). \tag{120}$$

Note that

$$\mathrm{N}(G(\chi)) = G(\chi)^p, \tag{121}$$

as $G(\chi) \in \mathbb{Z}[\zeta_q] \subset \mathbb{Q}(\zeta_{u^2/(pd^2)})$.

Now suppose $Z\eta \in \mathbb{Z}[\zeta_{p^{2a}}]$ for some root of unity η. Note that we can assume that η has odd order, since $Z \in \mathbb{Z}[\zeta_{u^2/d^2}]$ and u^2/d^2 is odd. Thus $\gamma := \zeta_{u^2/d^2}^{-j}\eta$ is a root of unity of odd order. By (120) and (121), we have

$$q^{2bp}\mathrm{N}(\gamma) = G(\chi)^p\mathrm{N}(Z\eta). \tag{122}$$

Let z be a primitive root modulo q^{2b} and let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{u^2/d^2})/\mathbb{Q})$ be given by $\zeta_{q^{2b}}^{\sigma} = \zeta_{q^{2b}}^{z}$ and $\zeta_{u^2/(d^2q^{2b})}^{\sigma} = \zeta_{u^2/(d^2q^{2b})}$. As $x = 2$, we have

$$G(\chi)^{\sigma} = -G(\chi) \tag{123}$$

by (114). Furthermore, note $\mathrm{N}(Z\eta)^{\sigma} = \mathrm{N}(Z\eta)$, as $Z\eta \in \mathbb{Z}[\zeta_{p^{2a}}]$ by assumption and p^{2a} divides $u^2/(d^2q^{2b})$. Thus

$$\mathrm{N}(\gamma)^{\sigma} = -\mathrm{N}(\gamma) \tag{124}$$

by (122) and (123), as p is odd. But (124) is impossible, since $\mathrm{N}(\gamma)$ is a root of unity of odd order. This proves (119).

In summary, we have shown

$$Z \in \mathbb{Z}[\zeta_{u^2/(d^2q^{2b})}],\ |Z| = q^{2b-1},\ Z\eta \notin \mathbb{Z}[\zeta_{u^2/(pd^2q^{2b})}],\ \text{and } Z\eta \notin \mathbb{Z}[\zeta_{p^{2a}}]$$

for all roots of unity η. Hence

$$q^{2b-1} \geq \mathrm{ord}_p(q) \min\left\{\frac{f_s(s-f_s)}{s-1} : s \in T\right\} \tag{125}$$

by Theorem 5.4, where T is the set of prime divisors s of u/d which are different from p and q and do not satisfy $\nu_2(\mathrm{ord}_s(q)) = \nu_2(\mathrm{ord}_p(q)) \geq 1$. Since $T = S \setminus (S' \cup \{q\})$, where S and S' are the sets defined in the statement of Theorem 6.3, we see that (125) implies (109). This completes the proof. □

Theorem 6.4. *There is no Barker sequence of length ℓ with* $13 < \ell \leq 4 \cdot 10^{33}$.

Proof. Suppose a Barker sequence of length ℓ with $13 < \ell \leq 4 \cdot 10^{33}$ exists. Then $l = 4u^2$ with $u = 5 \cdot 13 \cdot 29 \cdot 41 \cdot 2953 \cdot 138200401$ by [3, Thm. 1]. But this is impossible by Theorem 6.3 (see Table 1 below for the details). □

Finally, we present some computational results which illustrate the application of the results in this section. In [3], a total of 19 open cases of Barker sequences of length $\ell = 4u^2$ with $13 < \ell \leq 10^{50}$ was identified. All these 19 cases can be ruled out using Theorem 6.3. Table 1 contains relevant numerical data. The columns for p, q^b, d, q^{4b}, and $\mathrm{ord}_p(q)$ contain the values used in Theorem 6.3 to rule out the corresponding case. The column "max" gives the value of the maximum on the right hand side of (109). The column "LHS/RHS" contains the quotient of the left hand side and the right hand side in (109). By Theorem 6.3, the fact that this quotient is larger than 1 implies that in all these cases there is no circulant Hadmard matrix of order $4u^2$ and thus no Barker sequence of length $4u^2$. The values in the last three columns of Table 1 are rounded to two significant decimal digits and given in scientific notation.

A total of 237,807 open cases of Barker sequences with length $\ell \leq 10^{100}$ was identified in [3]. Theorem 6.3 rules out 229,682 of these 237,807 cases. The computational data (similar to Table 1) for this search are available from the authors upon request. The smallest of the 237,807 cases given in [3] which is not ruled out by Theorem 6.3 is $u = 30109 \cdot 1128713 \cdot 2167849 \cdot 268813277$.

Concerning circulant Hadamard matrices, 1371 open cases with $u \leq 10^{13}$ were found in [3]. Theorem 6.3 rules out 423 of these cases. Table 2 contains relevant numerical data for the 20 smallest u's for which circulant Hadamard matrices of order $4u^2$ are ruled out by Theorem 6.3. The format of Table 2 is the same as that of Table 1. The data for the remaining cases are available from the authors upon request. The smallest case of circulant Hadamard matrices which has not been ruled out still is $u = 11715 = 3 \cdot 5 \cdot 11 \cdot 71$.

Acknowledgement The second author is grateful to Dieter Jungnickel for his hospitality during a visit at the Universität Augsburg from August 2014 to March 2015, when most of this research was done.

Table 1

Factorization of u	p	q^b	d	q^{4b}	$\mathrm{ord}_p(q)$	max	LHS/RHS
5·13·29·41·2953·138200401	138200401	41	1885	2.8e+06	9.6e+05	2.4e-02	1.4e+01
5·5·53·193·4877·53471161	53471161	5	1325	3.9e+05	1.3e+07	3.7e-02	9.2e+02
5·5·13·53·193·4877·53471161	53471161	5	325	3.9e+05	1.3e+07	7.4e-02	4.6e+02
5·53·97·193·4877·53471161	53471161	5	265	6.2e+02	1.3e+07	8.0e-02	2.7e+05
5·5·53·97·193·4877·53471161	53471161	5	1325	3.9e+05	1.3e+07	7.4e-02	4.6e+02
5·13·53·97·193·4877·53471161	53471161	5	3445	6.2e+02	1.3e+07	8.0e-02	2.7e+05
5·5·13·53·97·193·4877·53471161	53471161	5	325	3.9e+05	1.3e+07	7.4e-02	4.6e+02
5·29·41·2953·1025273·138200401	138200401	41	5945	2.8e+06	9.6e+05	1.4e-03	2.5e+02
13·29·41·2953·1025273·138200401	138200401	41	377	2.8e+06	9.6e+05	2.4e-02	1.4e+01
5·17·613·1974353·188748146801	188748146801	5	52105	6.2e+02	1.2e+10	8.0e-02	2.4e+08
5·13·29·41·2953·1025273·138200401	138200401	41	1885	2.8e+06	9.6e+05	2.4e-02	1.4e+01
5·41·193·2953·53471161·138200401	138200401	41	205	2.8e+06	9.6e+05	2.1e-02	1.6e+01
5·13·29·41·2953·53471161·138200401	138200401	41	1885	2.8e+06	9.6e+05	2.4e-02	1.4e+01
53·97·4794006457·76704103313	76704103313	97	5141	8.9e+07	3.8e+10	2.1e-04	2.0e+06
5·5·193·24697·53471161·412835053	53471161	5	4825	3.9e+05	1.3e+07	3.2e-03	1.1e+04
5·13·123397·1974353·188748146801	188748146801	5	65	6.2e+02	1.2e+10	8.0e-02	2.4e+08
5·5333·612142549·188748146801	188748146801	5	26665	6.2e+02	1.2e+10	8.0e-02	2.4e+08
5·53·97·193·4877·2914393·53471161	53471161	5	265	6.2e+02	1.3e+07	8.0e-02	2.7e+05
5·5·41·193·2953·53471161·138200401	138200401	41	1025	2.8e+06	9.6e+05	2.1e-02	1.6e+01

Table 2

Factorization of u	p	q^b	d	q^{4b}	$\mathrm{ord}_p(q)$	max	LHS/RHS
3·5·11·67·20771	20771	5	33	6.2e+02	1.0e+04	2.0e-01	8.3e+01
5·7·11·67·20771	20771	5	77	6.2e+02	1.0e+04	2.0e-01	8.3e+01
3·5·31·67·20771	20771	5	3	6.2e+02	1.0e+04	3.6e-01	4.7e+01
3·5·7·11·31·20771	20771	5	33	6.2e+02	1.0e+04	5.0e-01	3.3e+01
3·5·7·11·67·20771	20771	5	33	6.2e+02	1.0e+04	5.0e-01	3.3e+01
5·7·47·67·20771	20771	5	35	6.2e+02	1.0e+04	8.3e-02	2.0e+02
5·11·31·67·20771	20771	5	11	6.2e+02	1.0e+04	3.6e-01	4.7e+01
5·13·31·79·20771	20771	5	31	6.2e+02	1.0e+04	3.3e-01	5.0e+01
5·31·653·40487	40487	5	31	6.2e+02	4.0e+04	2.0e-01	3.2e+02
3·5·7·31·67·20771	20771	5	21	6.2e+02	1.0e+04	3.6e-01	4.7e+01
3·5·7·31·79·20771	20771	5	21	6.2e+02	1.0e+04	3.6e-01	4.7e+01
5·13·31·79·40487	40487	5	13	6.2e+02	4.0e+04	3.6e-01	1.8e+02
3·5·7·47·67·20771	20771	5	21	6.2e+02	1.0e+04	2.0e-01	8.3e+01
3·5·11·31·67·20771	20771	5	33	6.2e+02	1.0e+04	3.6e-01	4.7e+01
3·5·11·31·71·20771	20771	5	33	6.2e+02	1.0e+04	1.0e+00	1.7e+01
5·7·13·43·491531	491531	7	65	2.4e+03	2.5e+05	1.9e-01	5.4e+02
3·5·13·31·79·20771	20771	5	3	6.2e+02	1.0e+04	3.6e-01	4.7e+01
3·5·11·47·67·20771	20771	5	33	6.2e+02	1.0e+04	2.0e-01	8.3e+01
13·431·863·2393	863	13	13	2.9e+04	8.6e+02	1.2e-02	2.6e+00
3·5·31·653·40487	40487	5	31	6.2e+02	4.0e+04	2.0e-01	3.2e+02

References

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

[2] Z. I. Borevich, I. R. Shafarevich: *Number Theory.* Academic Press 1966.

[3] P. Borwein, M. J. Mossinghoff: Wieferich pairs and Barker sequences, II. *LMS J. Comput. Math.* **17** (2014), 24–32.

[4] J. W. S. Cassels: On a conjecture of R. M. Robinson about sums of roots of unity. *J. Reine Angew. Math.* **238** (1969) 112–131.

[5] W. K. Chan: Necessary Conditions for Menon Difference Sets. *Des. Codes Crypt.* **3** (1993), 147–154.

[6] 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.

[7] K. Ireland, M. I. Rosen: *A Classical Introduction to Modern Number Theory* (2nd edition). Springer 1990.

[8] K. H. Leung, B. Schmidt: The Field Descent Method. *Des. Codes Crypt.* **36** (2005), 171–188.

[9] K. H. Leung, B. Schmidt: New restrictions on possible orders of circulant Hadamard matrices. *Des. Codes Crypt.* **64** (2012), 143–151.

[10] M. Mossinghoff: Wieferich pairs and Barker sequences. *Des. Codes Crypt.* **53** (2009), 149–163.

[11] H. J. Ryser: *Combinatorial Mathematics.* Wiley 1963.

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

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

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

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