hexagon:2611.00102v1

HADAMARD DIFFERENCE SETS IN GROUPS WITH A CYCLIC ODD QUOTIENT

DAVID NIEDBALA GIRAUDIN

Abstract. Let $u > 1$ be odd. We prove that the abelian group $C_2 \times C_{2u^2}$ contains no Hadamard difference set. Together with the recently announced proof of the circulant Hadamard conjecture, this shows that an abelian group of order $4u^2$ ($u > 1$ odd) whose odd Sylow subgroups are all cyclic never contains a Hadamard difference set, so Lander's conjecture holds for Hadamard difference sets in these groups. More generally, let G be a group of order $4u^2$ with a normal subgroup N such that $G/N \cong E \times C_{w^2}$, where $|E| = 4$, $w > 1$, $w \mid u$ and $\gcd(w, u/w) = 1$. If every prime divisor of u/w is self-conjugate modulo $\mathrm{rad}(w)$ (modulo $4\,\mathrm{rad}(w)$ when E is cyclic), then G contains no Hadamard difference set. The proof adapts the alternating character products used for the cyclic case.

1. Introduction

A *Hadamard* (or *Menon*) difference set is a (v, k, λ) difference set with parameters

$$(v, k, \lambda) = (4u^2,\ 2u^2 - u,\ u^2 - u),$$

of order $n = k - \lambda = u^2$. Throughout, u is an odd integer with $u > 1$. Then every group containing such a difference set has order $4u^2$, and its Sylow 2-subgroups have order 4; for abelian groups the Sylow 2-subgroup is C_4 or $C_2 \times C_2$. For background we refer to the surveys [1, 10] and to [4].

Lander's conjecture [5] asserts that if an abelian group G contains a (v, k, λ) difference set and a prime p divides $\gcd(v, n)$, then the Sylow p-subgroup of G is not cyclic. For Hadamard parameters with u odd, $\gcd(v, n) = u^2$. The conjecture is known when n is a power of a prime $p > 3$ [6] and, for Hadamard difference sets, for all orders $n \leq 529$, i.e. $u \leq 23$, by Feng, Leung, Schmidt and Smith [4], who also obtain strong restrictions for $u = 2^a 3^b$ (here u is even) with a cyclic Sylow 3-subgroup. For individual values of u, classical criteria (the exponent bound under self-conjugacy and the field descent bounds of Leung and Schmidt [7]) exclude many abelian groups; see Section 5.3. For groups of order $4p^{2f}$, $p \geq 5$ prime, with a quotient $C_{p^f} \times C_2 \times C_2$, nonexistence was proved by AbuGhneim and Smith [2], extending results of Iiams and Wan; very recently Schmidt [9] showed that no group of order $4p^2$ with $p \equiv 3 \pmod 4$, $p \geq 7$, contains a Hadamard difference set.

The cyclic case of Lander's conjecture for Hadamard parameters is the circulant Hadamard conjecture of Ryser and Turyn [11]. A proof of it was announced in September 2026 [8]. The purpose of this note is to show that the method of [8] applies, with a simpler final step, to the other abelian 2-part $C_2 \times C_2$, and more generally to every group of order $4u^2$ admitting a suitable abelian quotient. We do not know of a previous result excluding $C_2 \times C_{2u^2}$ for all odd $u > 1$.

Definition 1. Let $m \geq 1$ and let q be a prime with $q \nmid m$. We say that q is *self-conjugate modulo* m if $q^j \equiv -1 \pmod m$ for some integer $j \geq 0$. Equivalently, complex conjugation fixes every prime ideal above q in $\mathbb{Z}[\zeta_m]$.

Date: November 2026.

Theorem 2. *Let $u > 1$ be odd and let G be a group of order $4u^2$. Suppose that G has a normal subgroup N with*

$$G/N \cong E \times C_{w^2}, \qquad |E| = 4, \quad w > 1, \quad w \mid u, \quad \gcd(w, u/w) = 1,$$

and put $r = \mathrm{rad}(w)$. Assume that every prime divisor of u/w is self-conjugate modulo r if $E \cong C_2 \times C_2$, and modulo $4r$ if $E \cong C_4$. Then G contains no Hadamard difference set.

When $u/w = 1$ the self-conjugacy hypothesis is empty and $N = 1$. The case $G = C_4 \times C_{u^2}$ is the circulant Hadamard conjecture [8]. When $u/w > 1$ the group N, of order $(u/w)^2$, may be non-abelian, and G need not be abelian.

Corollary 3. *For every odd $u > 1$, the abelian group $C_2 \times C_{2u^2} \cong C_2 \times C_2 \times C_{u^2}$ contains no Hadamard difference set.*

Proof. Take $N = 1$ and $w = u$ in Theorem 2. □

Corollary 4. *Let G be an abelian group of order $4u^2$, $u > 1$ odd, and let I_c be the set of primes $p \mid u$ whose Sylow p-subgroup is cyclic. Suppose that there is a nonempty set $T \subseteq I_c$ such that every prime $q \mid u$ with $q \notin T$ is self-conjugate modulo $r_T = \prod_{p \in T} p$ (modulo $4r_T$ if the Sylow 2-subgroup is cyclic). Then G contains no Hadamard difference set; in particular, Lander's conjecture holds for Hadamard difference sets in G. This applies with $T = I_c$ whenever all odd Sylow subgroups of G are cyclic, i.e. $G \cong C_{4u^2}$ or $G \cong C_2 \times C_{2u^2}$.*

Proof. Write $G = E \times P_T \times Q$, where E is the Sylow 2-subgroup, P_T is the product of the Sylow p-subgroups with $p \in T$ and Q is the product of the other odd Sylow subgroups. Then $P_T \cong C_{w^2}$ with $w = \prod_{p \in T} p^{v_p(u)} > 1$, $\gcd(w, u/w) = 1$, $\mathrm{rad}(w) = r_T$, and the primes dividing u/w are the primes $q \mid u$ with $q \notin T$. Theorem 2 applies with $N = Q$. □

Remark 5. The self-conjugacy condition of Corollary 4 concerns the primes outside T (among them all primes with non-cyclic Sylow subgroups), and only modulo the radical r_T. It is of a different nature from the classical self-conjugacy hypotheses (Turyn's exponent bound and its refinements [11, 1, 10]), which require a prime p dividing u to be self-conjugate modulo the p-free part of the exponent of G.

The proof follows [8] closely. Section 2 recalls the local comparison of two character values; Section 3 proves that alternating products of character values are roots of unity of odd order, under the self-conjugacy hypothesis at the primes of u/w; Section 4 contains the binary step for both possible 2-parts. Section 5 explains why the hypotheses cannot simply be dropped from the argument and describes the ancillary computations.

2. Group rings and local lemmas

For a finite group H and a commutative ring $R \subseteq \mathbb{C}$ closed under complex conjugation, $R[H]$ carries the involution $x = \sum x_h h \mapsto x^* = \sum \overline{x_h}\, h^{-1}$. A subset D of a group G of order $4u^2$ which is a Hadamard difference set gives

$$h := G - 2D \in \mathbb{Z}[G] \qquad \text{with} \qquad hh^* = 4u^2.$$

(Conversely, such an h with coefficients ± 1 comes from a Hadamard difference set or from the complement of one.) Indeed $DD^* = n + \lambda G$ with $n = u^2$, and $(G - 2D)(G - 2D)^* = (4u^2 - 4k + 4\lambda)G + 4n = 4u^2$. Every coefficient of h is ± 1.

For an abelian group P and a character χ of P we write $\chi(x) = \sum_z x_z \chi(z)$; evaluation is a ring homomorphism and $\chi(x^*) = \overline{\chi(x)}$.

Lemma 6. *Let p be a prime, $L \geq 1$ with $p \nmid L$, and let A be the localization of $\mathbb{Z}[\zeta_L]$ at a prime ideal above p. Then A is a discrete valuation ring with uniformizer p. For $k \geq 1$ let ξ be a primitive p^k-th root of unity and $D = (p-1)p^{k-1}$. Then $A[\xi]$ is a discrete valuation ring with uniformizer $\xi - 1$, it is free over A with basis $1, \xi, \ldots, \xi^{D-1}$, and p is a unit times $(\xi-1)^D$. Consequently, if v denotes the valuation of $A[\xi]$ normalized by $v(p) = 1$, then for $z \in A[\xi]$ and $\ell \geq 0$ we have $v(z) \geq \ell \iff z \in p^\ell A[\xi]$, and for $R = \sum_{j<D} r_j X^j \in A[X]$,*

$$R(\xi) \in p^\ell A[\xi] \iff r_j \in p^\ell A \text{ for all } j.$$

Proof. These are standard facts: p is unramified in $\mathbb{Q}(\zeta_L)$ and totally ramified in $\mathbb{Q}(\zeta_L, \xi)/\mathbb{Q}(\zeta_L)$, with $\Phi_{p^k}(1+Y)$ Eisenstein over A; see e.g. [12, Ch. 2], or the self-contained proof in [8, Lemma 2.1]. The valuation statement holds because $p^\ell A[\xi] = (\xi-1)^{\ell D} A[\xi]$ is the set of elements of valuation at least ℓ, and the last statement follows from $p^\ell A[\xi] = \bigoplus_j p^\ell A\, \xi^j$. □

Lemma 7 (Character comparison [8, Lemma 3.1])**.** *Let A be as in Lemma 6, $e \geq 1$, and let $F, K \in A[C_{p^e}]$ satisfy $FK = p^e b$ with $b \in A^\times$. Let ρ be a primitive p-th root of unity. Then $F(\rho)/F(1)$ and $K(\rho)/K(1)$ are units of $A[\rho]$ congruent to 1 modulo $\rho - 1$.*

Proof. Here $F(1)$, $F(\rho)$ denote the images of F under the ring homomorphisms determined by $X \mapsto 1$ and $X \mapsto \rho$, X the chosen generator. Since $F(1)K(1) = F(\rho)K(\rho) = p^e b \neq 0$, all four values are nonzero, and the two ratios are inverse to each other; it suffices to prove the claim for one of them. We argue by induction on e.

If $e = 1$, the valuations of $F(1)$ and $K(1)$ in A sum to 1, so one of them, say $F(1)$, is a unit. As $F(\rho) \equiv F(1) \pmod{\rho - 1}$, the ratio $F(\rho)/F(1)$ is a unit congruent to 1.

Let $e \geq 2$ and let ξ be a primitive p^e-th root of unity. In the discrete valuation ring $A[\xi]$, normalized by $v(p) = 1$, we have $v(F(\xi)) + v(K(\xi)) = e \geq 2$, so after exchanging F and K we may assume $v(F(\xi)) \geq 1$, i.e. $F(\xi) \in pA[\xi]$. Write $F = Q\Phi_{p^e} + R$ in $A[X]$ with $\deg R < D$. Since $R(\xi) = F(\xi)$, Lemma 6 gives $R \in pA[X]$. Let $\pi : A[C_{p^e}] \to A[C_{p^{e-1}}]$ be the projection sending X to a generator. Since $\pi(\Phi_{p^e}) = \sum_{j<p} X^{jp^{e-1}} \mapsto p$, we get $\pi(F) \in pA[C_{p^{e-1}}]$. Put $F' = \pi(F)/p$ and $K' = \pi(K)$. Then $F'K' = p^{e-1}b$ (cancellation of p is legitimate since $A[C_{p^{e-1}}]$ is a free A-module), and since evaluation at 1 and at ρ factors through π (as $\rho^{p^{e-1}} = 1$), the two ratios are unchanged. The induction hypothesis applies to (F', K'). □

Remark 8. The hypothesis that the p-adic valuation of the scalar equals the exponent e of the group order is essential: for an odd prime p, $J = \sum_{z \in C_p} z$ and $F = p - 2J$ one has $FF^* = p^2$ in $\mathbb{Z}[C_p]$, but $F(\rho)/F(1) = -1$ [8, Remark 3.2].

Lemma 9 ([8, Lemma 3.3])**.** (i) (Kronecker) *An algebraic integer all of whose complex conjugates have absolute value* 1 *is a root of unity.*

(ii) *Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_M]$ above the prime ℓ. A root of unity $\zeta \in \mathbb{Z}[\zeta_M]$ with $\zeta \equiv 1 \pmod{\mathfrak{p}}$ has ℓ-power order.*

Proof. (i) is classical. For (ii), if the order of ζ is $\ell^a m$ with $\ell \nmid m$, then $\eta = \zeta^{\ell^a}$ has order m and $\eta \equiv 1 \pmod{\mathfrak{p}}$; if $m > 1$, then $0 = 1 + \eta + \cdots + \eta^{m-1} \equiv m \pmod{\mathfrak{p}}$, contradicting $\ell \nmid m$. □

3. Alternating character products

Fix odd integers $u > 1$ and $w > 1$ with $w \mid u$ and $\gcd(w, u/w) = 1$. Let I be the set of primes dividing w, $r = \prod_{p \in I} p$, and let $P = C_{w^2}$, written as the product of its cyclic Sylow subgroups $P_p \cong C_{p^{e_p}}$ with $e_p = 2v_p(w) = v_p(u^2)$. Fix $m_0 \in \{1, 4\}$ and put

$$B = \mathbb{Z}[\zeta_{m_0 r}], \qquad K_0 = \mathbb{Q}(\zeta_{m_0 r}).$$

For each $p \in I$ fix a generator X_p of P_p and a primitive p-th root of unity $\rho_p \in B$. For $S \subseteq I$ let χ_S be the character of P with $\chi_S(X_p) = \rho_p$ for $p \in S$ and $\chi_S(X_p) = 1$ for $p \notin S$. For $x \in \mathbb{Z}[\zeta_{m_0}][P]$ put $x_S = \chi_S(x) \in B$ and $\varepsilon_S = (-1)^{|S|}$.

Proposition 10 (cf. [8, Proposition 3.4])**.** *Assume that every prime divisor of u/w is self-conjugate modulo $m_0 r$. Let $x \in \mathbb{Z}[\zeta_{m_0}][P]$ satisfy $xx^* = u^2$. Then*

$$\Delta(x) = \prod_{S \subseteq I} x_S^{\varepsilon_S}$$

is a root of unity in B whose order is a power of p for every $p \in I$. In particular its order is odd.

Proof. Applying χ_S to $xx^* = u^2$ gives $x_S \overline{x_S} = u^2$; in particular $x_S \neq 0$ and $\Delta(x) \in K_0^\times$. Since B is a Dedekind domain, it suffices to show $v_\mathfrak{p}(\Delta(x)) \geq 0$ for every nonzero prime $\mathfrak{p}$ of B. Let ℓ be the rational prime below $\mathfrak{p}$.

Case $\ell \nmid u$. Then u^2 is a unit at $\mathfrak{p}$, hence so is every x_S, and $v_\mathfrak{p}(\Delta(x)) = 0$.

Case $\ell = q \mid u/w$. Then $q \nmid m_0 r$, so q is unramified in K_0, and complex conjugation fixes $\mathfrak{p}$ by the self-conjugacy hypothesis. Hence $v_\mathfrak{p}(\overline{x_S}) = v_{\overline{\mathfrak{p}}}(x_S) = v_\mathfrak{p}(x_S)$, and $x_S \overline{x_S} = u^2$ gives $v_\mathfrak{p}(x_S) = v_q(u)$ for every S. Since $\sum_{S \subseteq I} \varepsilon_S = (1-1)^{|I|} = 0$, we get $v_\mathfrak{p}(\Delta(x)) = 0$.

Case $\ell = p \in I$. Put $L = m_0 r/p$, so $p \nmid L$ and $A_0 := \mathbb{Z}[\zeta_L] \subseteq B$ contains ζ_{m_0} and all ρ_q, $q \in I \backslash \{p\}$. Let A be the localization of A_0 at $\mathfrak{p} \cap A_0$. Fix $S \subseteq I \setminus \{p\}$. Evaluating every component P_q, $q \neq p$, by χ_S and keeping X_p as a variable defines a ring homomorphism $\mathbb{Z}[\zeta_{m_0}][P] \to A_0[P_p]$ compatible with the involutions; let F, K be the images of x, x^*. Then

$$FK = u^2 = p^{e_p} b, \qquad b = u^2/p^{e_p} \in \mathbb{Z}, \quad p \nmid b,$$

so $b \in A^\times$, and $P_p \cong C_{p^{e_p}}$ with $e_p \geq 2$. By Lemma 7,

$$\frac{x_{S \cup \{p\}}}{x_S} = \frac{F(\rho_p)}{F(1)} \in A[\rho_p]^\times, \qquad \frac{x_{S \cup \{p\}}}{x_S} \equiv 1 \pmod{\rho_p - 1}.$$

Since $A[\rho_p] \subseteq B_\mathfrak{p}$ and $\rho_p - 1 \in \mathfrak{p}$, each such ratio is a unit of $B_\mathfrak{p}$ congruent to 1 modulo $\mathfrak{p}$. Pairing S with $S \cup \{p\}$,

$$\Delta(x) = \prod_{S \subseteq I \setminus \{p\}} \Big(\frac{x_S}{x_{S \cup \{p\}}} \Big)^{\varepsilon_S},$$

so $\Delta(x) \in B_\mathfrak{p}^\times$ and $\Delta(x) \equiv 1 \pmod{\mathfrak{p}}$.

Thus $\Delta(x) \in B$. For every embedding $\sigma : K_0 \to \mathbb{C}$ we have $\sigma(\overline{y}) = \overline{\sigma(y)}$ (K_0 is abelian), hence $|\sigma(x_S)| = u$ for all S, and $|\sigma(\Delta(x))| = u^{\sum \varepsilon_S} = 1$. By Lemma 9(i), $\Delta(x)$ is a root of unity. For $p \in I$ choose a prime $\mathfrak{p} \mid p$; by the last case $\Delta(x) \equiv 1 \pmod{\mathfrak{p}}$, so its order is a power of p by Lemma 9(ii). □

Remark 11. If $|I| \geq 2$ the proposition gives $\Delta(x) = 1$. For $u = w = p^a$ the order can be p: $x = p^a X_p$ gives $\Delta(x) = \rho_p^{-1}$ [8, Section 3].

4. Proof of Theorem 2

Let $D \subseteq G$ be a Hadamard difference set, $h = G - 2D$, and let $\bar{h} \in \mathbb{Z}[G/N]$ be the image of h. Then $\bar{h}\bar{h}^* = 4u^2$, and every coefficient of $\bar{h}$ is a sum of $|N| = (u/w)^2$ signs, hence an odd integer. Identify $G/N = E \times P$ with $P = C_{w^2}$, and let $I, r, \chi_S, \varepsilon_S$ be as in Section 3. Put

$$J = \sum_{z \in P} z \in \mathbb{Z}[P].$$

For $S \neq \varnothing$, χ_S is a nontrivial character, so $J_S = 0$; and $J_\varnothing = w^2$.

We shall use the following elementary device [8, Lemma 4.1]. Let O be a discrete valuation ring with maximal ideal $\mathfrak{n}$ and residue field $k = O/\mathfrak{n}$, and let $0 \neq t \in \mathfrak{n}$. Then $1 + tO$ is a subgroup of $O^\times$ and

$$\lambda_t : 1 + tO \to (k, +), \qquad \lambda_t(1 + tL) = L \bmod \mathfrak{n} \tag{1}$$

is a homomorphism, because $\big((1+tL)(1+tM)-1\big)/t = L+M+tLM$ and $\big((1+tL)^{-1}-1\big)/t = -L/(1+tL)$.

4.1. **The case $E \cong C_2 \times C_2$.** Write $E = \{1, y_1, y_2, y_1y_2\}$ and

$$\bar h = H_0 + y_1H_1 + y_2H_2 + y_1y_2H_3, \qquad H_j \in \mathbb{Z}[P],$$

where all coefficients of all H_j are odd. For the four characters ψ of E, put $x^\psi = \frac12\psi(\bar h) \in \mathbb{Z}[P]$:

$$c = \tfrac{H_0+H_1+H_2+H_3}{2}, \quad d_1 = \tfrac{H_0-H_1+H_2-H_3}{2}, \quad d_2 = \tfrac{H_0+H_1-H_2-H_3}{2}, \quad d_3 = \tfrac{H_0-H_1-H_2+H_3}{2}.$$

Each coefficient is half a sum of four odd integers, hence an integer. Since ψ is real-valued, evaluation at ψ commutes with *, so $cc^* = d_id_i^* = u^2$. We have the exact identities

$$d_i - c = -2b_i, \qquad b_1 = \tfrac{H_1+H_3}{2},\ b_2 = \tfrac{H_2+H_3}{2},\ b_3 = \tfrac{H_1+H_2}{2} \in \mathbb{Z}[P], \tag{2}$$

and

$$b_1 + b_2 + b_3 = H_1 + H_2 + H_3 = J + 2V, \qquad V \in \mathbb{Z}[P], \tag{3}$$

because each coefficient of $H_1 + H_2 + H_3$ is a sum of three odd integers.

Apply Proposition 10 with $m_0 = 1$ (the hypothesis is that every prime divisor of u/w is self-conjugate modulo r): $\Delta(c)$ and $\Delta(d_i)$ are roots of unity of odd order, hence so is $R_i = \Delta(d_i)/\Delta(c)$.

Let $\mathfrak{m}$ be a prime of $B = \mathbb{Z}[\zeta_r]$ above 2, $O = B_\mathfrak{m}$, $\mathfrak{n} = \mathfrak{m}O$, $k = O/\mathfrak{n}$. As r is odd, 2 is unramified in B and $\mathfrak{n} = 2O$. Each c_S is a unit of O since $c_S\overline{c_S} = u^2$ is odd. By (2),

$$r_{i,S} := \frac{(d_i)_S}{c_S} = 1 + 2L_{i,S}, \qquad L_{i,S} = -\frac{(b_i)_S}{c_S} \in O,$$

so $r_{i,S} \in 1+2O$ and $R_i = \prod_S r_{i,S}^{\varepsilon_S} \in 1+2O$. A root of unity of odd order congruent to 1 modulo $\mathfrak{m}$ equals 1 by Lemma 9(ii) (with $\ell = 2$). Hence $R_i = 1$, and applying λ_2,

$$\sum_{S\subseteq I} \varepsilon_S \frac{(b_i)_S}{c_S} \equiv 0 \pmod{\mathfrak{n}} \qquad (i = 1, 2, 3).$$

Summing over i and using (3),

$$0 \equiv \sum_{S\subseteq I} \varepsilon_S \frac{J_S + 2V_S}{c_S} \equiv \sum_{S\subseteq I} \varepsilon_S \frac{J_S}{c_S} = \frac{w^2}{c_\varnothing} \pmod{\mathfrak{n}}.$$

But $w^2/c_\varnothing$ is a unit of O. This contradiction proves the theorem when $E \cong C_2 \times C_2$.

4.2. **The case $E \cong C_4$.** This is the argument of [8, Section 4], which we include for completeness, now with $P = C_{w^2}$ and the scalar u^2. Let Z generate E and write $\bar h = H_0 + ZH_1 + Z^2H_2 + Z^3H_3$ with all coefficients of the $H_j \in \mathbb{Z}[P]$ odd. Put

$$c = \tfrac{H_0+H_1+H_2+H_3}{2}, \quad d = \tfrac{H_0-H_1+H_2-H_3}{2}, \quad g = \tfrac{H_0-H_2}{2} + i\,\tfrac{H_1-H_3}{2},$$

the halves of the evaluations of $\bar h$ at $Z = 1, -1, i$. They lie in $\mathbb{Z}[P]$, $\mathbb{Z}[P]$, $\mathbb{Z}[i][P]$ and satisfy $cc^* = dd^* = gg^* = u^2$. With $b = (H_1 + H_3)/2$ one has

$$d - c = -2b, \qquad g - c = (i-1)b - (H_2 + iH_3), \qquad H_2 + iH_3 = (1+i)J + 2U,$$

with $U \in \mathbb{Z}[i][P]$ (each coefficient $\alpha + i\beta$ of $H_2 + iH_3$ has α, β odd). Apply Proposition 10 with $m_0 = 4$ (the hypothesis is that every prime divisor of u/w is self-conjugate modulo $4r$; note $\mathbb{Z}[P] \subseteq \mathbb{Z}[i][P]$). Then $R = \Delta(d)/\Delta(c)$ and $W = \Delta(g)/\Delta(c)$ are roots of unity of odd order in $B = \mathbb{Z}[\zeta_{4r}]$.

Let $\mathfrak{m}$ be a prime of B above 2, $O = B_{\mathfrak{m}}$, $\mathfrak{n} = \mathfrak{m}O$. Here $1+i$ is a uniformizer of O, the image of i in k is 1, and every c_S is a unit. Using $i - 1 = i(1 + i)$ and $2 = (1 + i)(1 - i)$,

$$\frac{d_S}{c_S} = 1 + 2L_{r,S}, \quad L_{r,S} = -\frac{b_S}{c_S}; \qquad \frac{g_S}{c_S} = 1 + (1+i)L_{w,S}, \quad L_{w,S} = i\frac{b_S}{c_S} - \frac{J_S}{c_S} - (1-i)\frac{U_S}{c_S}.$$

Hence $R, W \equiv 1 \pmod{\mathfrak{m}}$, so $R = W = 1$ by Lemma 9(ii). Applying λ_2 and λ_{1+i},

$$\sum_S \varepsilon_S L_{r,S} \equiv 0, \qquad \sum_S \varepsilon_S L_{w,S} \equiv 0 \pmod{\mathfrak{n}}.$$

Since $L_{r,S} + L_{w,S} = (i-1)\frac{b_S}{c_S} - \frac{J_S}{c_S} - (1-i)\frac{U_S}{c_S} \equiv -\frac{J_S}{c_S} = \frac{J_S}{c_S} \pmod{\mathfrak{n}}$ (the residue field has characteristic 2), adding gives $w^2/c_\varnothing \equiv 0 \pmod{\mathfrak{n}}$, a contradiction. This completes the proof of Theorem 2. □

5. Remarks on the hypotheses and computations

5.1. **The exponent condition.** The argument needs the p-part of the cyclic quotient to have order exactly $p^{v_p(u^2)}$ (Remark 8). This is not a technicality: Hadamard difference sets exist in $C_2 \times C_2 \times C_3 \times C_3$ and in $C_4 \times C_3 \times C_3$ (explicit $(36, 15, 6)$ difference sets are verified in the ancillary script). Projecting the first one onto $C_2 \times C_2 \times C_3$, whose 3-part has order $3 < 9 = u^2$, one finds $\Delta(c) = -1$, $\Delta(d_1) = 1$, $\Delta(d_2) = \Delta(d_3) = -1$, so $R_1 = -1 \neq 1$: some alternating products have even order, and the argument correctly breaks down.

5.2. **The self-conjugacy condition.** At a prime $\mathfrak{p}$ above $q \mid u/w$ the comparison lemma is not available, and without self-conjugacy the values x_S may lie above different primes over q. The following example (which is not itself in the setting of Proposition 10, where the scalar is u^2 and $P = C_{w^2}$) illustrates this local phenomenon: in $\mathbb{Z}[i][C_3]$ the element $x = -i + (1+i)X + (1+i)X^2$ satisfies $xx^* = 5$, while $x(1) = 2 + i$ and $x(\rho) = -1 - 2i$ generate the two distinct primes above 5 in $\mathbb{Z}[i]$; the quotient $x(1)/x(\rho)$ is not integral. Here 5 is not self-conjugate modulo 12 (it is modulo 3).

5.3. **Comparison with classical criteria.** For an individual u, many of the groups covered by Corollary 4 were already excluded by classical results. We mention two criteria for $G = C_2 \times C_{2u^2}$, u odd. When u is a prime power the first one alone excludes G, since the p-free part of $\exp G$ is 2 and every odd prime is self-conjugate modulo 2; we therefore assume that u is not a prime power.

(i) The exponent bound under self-conjugacy (Turyn [11]; Arasu, Davis and Jedwab [3]; see [10, Thm. 2.5]): if a prime $p \mid u$ with $p^a \| u$ is self-conjugate modulo the p-free part $2(u/p^a)^2$ of $\exp G$, the cyclic Sylow p-subgroup, of exponent $p^{2a} > p^a$, is impossible.

(ii) The field descent bound of Leung and Schmidt [7, Thm. 4.3] with $A = C_{u^2}$ and $H = C_2 \times C_2$ (so that $\gcd(|A|, |H|) = \gcd(n, |H|) = 1$): $n = u^2 \leq |H|F^2/(4\varphi(F)) = F^2/\varphi(F)$, where $F = \gcd\big(u^2, F(2u^2, u^2)\big)$.

By our computation (ancillary script, Part F), these two criteria exclude $C_2 \times C_{2u^2}$ for every odd $u < 11715$ that is not a prime power, and among $u \leq 2 \cdot 10^5$ exactly $u \in \{11715, 16401, 82005\}$ survive. For the cyclic group C_{4u^2} we combined the exponent bound (with p-free part $4(u/p^a)^2$) with the bound $u\varphi(u) \leq F(u^2, u)$ of [7, Cor. 4.5]; the same three values survive, in agreement with [7, Cor. 4.5], which excludes circulant Hadamard matrices of order $4 < v < 548\,964\,900 =$

$4 \cdot 11715^2$. We have not applied other known criteria, so the novelty of Corollary 3 lies in its uniformity in u rather than in any particular small case.

5.4. **Ancillary computations.** The script `anc/verify_hds.py` (exact integer arithmetic, except for a floating-point pre-filter whose survivors are all checked exactly; about one minute in total; it requires `numpy`)

- checks the identities (2), (3) and those of the cyclic case on random sign arrays;
- enumerates all $x \in \mathbb{Z}[C_9]$ and all $x \in \mathbb{Z}[i][C_9]$ with $xx^* = 9$ (there are 108 and 432 of them) and verifies Proposition 10 for each of them: $\Delta(x)$ is integral, is a root of unity of order 1 or 3, and is congruent to 1 above 3;
- verifies the two $(36, 15, 6)$ difference sets and the computations of Section 5;
- counts the abelian groups of order $4u^2$, u odd, $u \leq 105$, covered by Corollary 4: of 424 groups, 204 have no cyclic odd Sylow subgroup, 104 have all odd Sylow subgroups cyclic, 53 others are covered through the self-conjugacy hypothesis (for some choice of T), and 63 satisfy the hypothesis of Lander's conjecture but are not covered;
- carries out the comparison of Section 5.3.

References

[1] J. A. Davis and J. Jedwab, *A survey of Hadamard difference sets*, in: Groups, Difference Sets, and the Monster (K. T. Arasu, J. F. Dillon, K. Harada, S. Sehgal, R. Solomon, eds.), de Gruyter, 1996, 145–156.

[2] O. A. AbuGhneim and K. W. Smith, *Tightening Turyn's bound for Hadamard difference sets*, J. Algebraic Combin. **27** (2008), 187–203.

[3] K. T. Arasu, J. A. Davis and J. Jedwab, *A nonexistence result for abelian Menon difference sets using perfect binary arrays*, Combinatorica **15** (1995), 311–317.

[4] T. Feng, K. H. Leung, B. Schmidt and K. W. Smith, *Hadamard difference sets related to Lander's conjecture*, J. Algebra **403** (2014), 29–47.

[5] E. S. Lander, *Symmetric Designs: an Algebraic Approach*, London Math. Soc. Lecture Note Ser. **74**, Cambridge University Press, 1983.

[6] K. H. Leung, S. L. Ma and B. Schmidt, *Nonexistence of abelian difference sets: Lander's conjecture for prime power orders*, Trans. Amer. Math. Soc. **356** (2004), 4343–4358.

[7] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), 171–188.

[8] OpenAI, *The circulant Hadamard conjecture*, preprint, September 23, 2026, `https://github.com/openai/math`.

[9] B. Schmidt, *Nonexistence of Hadamard difference sets in groups of order $4p^2$ with $p \equiv 3 \pmod 4$, $p \geq 7$*, preprint, October 2026, arXiv:2610.37417.

[10] D. Jungnickel and B. Schmidt, *Difference sets: an update*, in: Geometry, Combinatorial Designs and Related Structures (Proc. First Pythagorean Conf.), London Math. Soc. Lecture Note Ser. **245**, Cambridge University Press, 1997, 89–112.

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

[12] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. **83**, Springer, 1997.

ORCID: 0009-0009-1526-1178