Hadamard Difference Sets Related to Lander's Conjecture

Tao Feng
Department of Mathematics
Zhejiang University
P. R. China

Ka Hin Leung
Department of Mathematics
National University of Singapore
Singapore 119260

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

Ken W. Smith
Department of Mathematics and Statistics
Sam Houston State University
Huntsville, Texas 77340

September 11, 2013

Abstract

If a Hadamard difference set exists in $H \times K$, where H is an abelian 2-group and K is a cyclic 3-group, then $|H| > 4|K|$. Furthermore, Lander's conjecture holds for all Hadamard difference sets of order at most 529.

1 Introduction

A **$(\mathbf{v}, \mathbf{k}, \boldsymbol{\lambda}, \mathbf{n})$ difference set** in a finite group G of order v is a k-subset D of G, such that every nonidentity element g of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. As usual, we assume $1 < k < v/2$. Then $n = k - \lambda$ is a positive integer which is called the **order** of the difference set. For introductions to difference sets, see [1, 2, 7].

Lander [7, p. 224] proposed the following.

Conjecture 1.1 (Lander 1983) *Let G be an abelian group of order v containing a difference set of order n. If p is a prime dividing v and n, then the Sylow p-subgroup of G cannot be cyclic.*

In [8, Thm. 1.3], the following result was obtained.

Result 1.2 *Lander's conjecture is correct in the case where n is a power of a prime $p > 3$.*

In the case that n is not a prime power, there currently is not much reason to believe that Lander's conjecture holds. Promising candidates for putative counterexamples seem to be Hadamard difference sets. A **Hadamard difference set** is a difference set with parameters $(v, k, \lambda, n) = (4u^2, 2u^2 - u, u^2 - u, u^2)$ for some positive integer u.

In this paper, we study Hadamard difference sets with $u = 2^a 3^b$ in abelian groups with cyclic Sylow 3-subgroups. It is not known if any such difference sets exist, but the following necessary conditions for their existence are known. Let C_m denote the cyclic group of order m.

Result 1.3 *Suppose there is a Hadamard difference set with $u = 2^a 3^b$ in an abelian group $C_{3^{2b}} \times H$, where H is an abelian 2-group. Then the following hold.*

(*i*) *Let U be any subgroup of H such that* $\exp(H/U) \leq 4$. *Then* $|U| > 3^b$.

(*ii*) $\exp(H) \leq 2^{a+2}\sqrt{2}/3^{b-1}$.

The first part of Result 1.3 follows from [7, Thm. 4.3.3] and the second part from [10, Thm. 3.3.2]. In Section 5, we will obtain the new necessary condition $2^a > 3^b$.

The main value of this paper lies in Section 6, in which we obtain substantial information on some putative counterexamples to Lander's conjecture. This is used to rule out some sporadic cases, but the techniques will be useful, in particular, for the further investigation of Hadamard difference sets with $u = 2^a 3^b$ in abelian groups.

Suppose there is a Hadamard difference set of order u^2 with $u \leq 20$ in an abelian group G which has a cyclic Sylow p-subgroup for some prime p dividing u. Then, according to [4, Section 5], we have $u = 12$, $p = 3$, and G is one of the following groups:

(a) $C_9 \times C_8 \times C_8$,
(b) $C_9 \times C_{16} \times C_4$,
(c) $C_9 \times C_{16} \times C_2 \times C_2$.

We will rule out these three cases. To do this, we develop new methods to deal with "sophisticated characters" (see Section 3 for their definition). Analogues to sophisticated characters must occur for all putative counterexamples to Lander's conjecture (see Remark 5.2). Thus our methods are relevant to the further investigation of this problem.

By [11, Thm. 6] and [9, Thm. 3.1], there are no Hadamard difference sets of order u^2 with $21 \leq u \leq 23$ in abelian groups which have any cyclic Sylow p-subgroup for a prime p dividing u. Thus we get the following.

Corollary 1.4 *Lander's conjecture holds for all Hadamard difference sets of order at most* 529.

2 Preliminaries

We will need the following notation and standard facts. By φ we denote the Euler totient function. Let G be a finite abelian group. A subset S of G will be identified with the element $\sum_{g\in S} g$ of the group ring $\mathbb{Z}[G]$. For $B = \sum_{g\in G} b_g g \in \mathbb{Z}[G]$, we write $|B| = \sum_{g\in G} b_g$ and $B^{(-1)} = \sum_{g\in G} b_g g^{-1}$. The integers b_g are called the **coefficients** of B.

Write $e = \exp(G)$ and $\zeta_e = \exp(2\pi i/e)$. We denote the group of complex characters of G by $\hat{G}$. We say that $\chi \in \hat{G}$ is **trivial** on a subgroup H of G if $\chi(g) = 1$ for all $g \in H$. We call $\chi, \tau \in \hat{G}$ **equivalent**, if there is $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})$ with $\tau(g) = \chi(g)^\sigma$ for all $g \in G$.

The following Results 2.1, 2.2, and 2.4 are standard, see [2, Vol. I, Chapter VI].

Result 2.1 *Let D be a k-subset of an abelian group G of order v. Then D is a (v, k, λ, n) difference set in G if and only if $DD^{(-1)} = n + \lambda G$ in $\mathbb{Z}[G]$. This holds if and only if*

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

for all nontrivial characters χ of G.

Result 2.2 *Let G be a finite abelian group and $D = \sum_{g\in G} d_g g \in \mathbb{C}[G]$. Then*

$$d_g = \frac{1}{|G|} \sum_{\chi\in\hat{G}} \chi(Dg^{-1})$$

for all $g \in G$.

Definition 2.3 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.

Result 2.4 *Suppose that $A \in \mathbb{Z}[\zeta_m]$ satisfies $|A|^2 \equiv 0 \bmod t^{2b}$, where b, t are positive integers, and t is self-conjugate modulo m. Then $A \equiv 0 \bmod t^b$.*

We will need the following result of Kronecker. See [3, Section 2.3, Thm. 2] for a proof.

Result 2.5 *An algebraic integer all of whose conjugates have absolute value* 1 *is a root of unity.*

Note that Result 2.5 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.

The following is [10, Thm. 2.3.2].

Result 2.6 (F-bound) *Let* $Y \in \mathbb{Z}[\zeta_m]$ *be of the form*

$$Y = \sum_{i=0}^{m-1} a_i \xi_m^i$$

with $0 \leq a_i \leq C$ *for some constant* C *and suppose that* $|Y|^2 = n$ *is an integer. Then*

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

The next result is a special case of [10, Thm. 2.2.2].

Result 2.7 *Let* $m = p^a m'$ *where* p *is an odd prime prime,* $(p, m') = 1$*, and* $m \equiv 0 \pmod 4$*. Let* h *be primitive element modulo* p*. Suppose that* $Y \in \mathbb{Z}[\zeta_m]$ *satisfies* $|Y|^2 = p^b$ *for some* $b \geq 1$*. Then there are an integer* j*, a divisor* u *of* $p-1$*, and* $Z \in \mathbb{Z}[\xi_{m'}]$ *such that*

$$Y\zeta_m^j \in \mathbb{Z}[\xi_{m'}] \quad \text{or} \quad X = \zeta_m^j Z \sum_{i=1}^{p-1} \zeta_u^i \zeta_p^{h^i}.$$

Furthermore, $|Z|^2 = p^{b-1}$*.*

We will need the following observation on character values of group ring elements.

Lemma 2.8 *Let* W *be an abelian group and let* $E = \sum_{g \in W} a_g g \in \mathbb{Z}[W]$*. Let* U *be a subgroup of* W *and write* $U^\perp = \{\chi \in \hat{W} : \chi(g) = 1 \text{ for all } g \in U\}$*. Then*

$$\sum_{\tau \in U^\perp} \chi\tau(E) = |U^\perp| \chi \left(\sum_{g \in U} a_g g \right)$$

for every $\chi \in \hat{W}$*.*

Proof Note that $\sum_{\tau\in U^\perp}\tau(g)=0$ for $g\in W\setminus U$. Hence

$$\begin{aligned}\sum_{\tau\in U^\perp}\chi\tau(E) &= \sum_{\tau\in U^\perp}\sum_{g\in W}a_g\chi(g)\tau(g)\\ &= \sum_{g\in W}a_g\chi(g)\left(\sum_{\tau\in U^\perp}\tau(g)\right)\\ &= |U^\perp|\sum_{g\in U}a_g\chi(g)\\ &= |U^\perp|\chi\left(\sum_{g\in U}a_g g\right).\end{aligned}$$

□

Let m and n be positive integers. We say that $Y\in\mathbb{Z}[\zeta_m]$ is an ***n*-Weil number** if $|Y|^2=n$. The following result classifies the Weil numbers which play a role in this paper. For convenience, we categorize these numbers into three types. The Weil numbers of "naive type" will be the those which are equal to a root of unity times an integer. "Gauss type" Weil numbers are those which are not naive, but divisible by the Gauss sum $\zeta_3-\zeta_3^2$. Finally, Weil numbers of "sophisticated type" are those which are not divisible the the Gauss sum $\zeta_3-\zeta_3^2$. As the further sections will show, it is exactly the sophisticated Weil numbers which make the situation interesting and difficult (thus their name).

For the proof of the classification of the relevant Weil numbers, we need some standard facts from algebraic number theory, in particular, on prime ideal factorization in cyclotomic fields. We refer the reader to [6] for the necessary background.

Lemma 2.9 *Let $u=2^a3^b$ and $e=2^r3^s$, where a,b,r,s are positive integers. Write $X=1+\zeta_8+\zeta_8^3$. Suppose that $Y\in\mathbb{Z}[\zeta_e]$ satisfies the $|Y|^2=u^2$. Then there is an integer i such that $Y\zeta_e^i$ is one of the following.*

(*i*) *u (naive type),*

(*ii*) *$2^a(\zeta_3-\zeta_3^2)^cX^{2b-c}$ or $2^a(\zeta_3-\zeta_3^2)^c\bar{X}^{2b-c}$ for some c with $1\le c\le 2b-1$ (Gauss type),*

(iii) $2^a X^{2b}$ *or* $2^a \bar{X}^{2b}$ (*sophisticated type*).

Proof Note that $(\mathbb{Z}/3^s\mathbb{Z})^*$ is cyclic of order $2 \cdot 3^{s-1}$. It is straightforward to verify that $\mathrm{ord}_{3^s}(2) = 2 \cdot 3^{s-1}$ (alternatively, this follows from [10, Lem. 1.4.11]). Hence $\mathrm{ord}_{3^s}(2^{3^{s-1}}) = 2 = \mathrm{ord}_{3^s}(-1)$. As $(\mathbb{Z}/3^s\mathbb{Z})^*$ is cyclic, this implies

$$2^{3^{s-1}} \equiv -1 \pmod{3^s}.$$

By Definition 2.3, this shows that 2 is self-conjugate modulo e. Hence $Y \equiv 0 \pmod{2^a}$ by Result 2.4. Write $Y = 2^a Z$ with $Z \in \mathbb{Z}[\zeta_e]$. Then $|Z|^2 = 3^{2b}$.

Next, we show that we may assume $r \geq 3$. If $r \leq 2$, then 3 is self-conjugate modulo e, as $3 \equiv -1 \pmod 4$. Hence $Z \equiv 0 \pmod{3^b}$ by Result 2.4. Thus $Y = u\eta$ for some $\eta \in \mathbb{Z}[\zeta_e]$. Since $|Y|^2 = u^2$, we conclude $|\eta| = 1$. Hence η is a root of unity by Result 2.5. This implies $Y = \zeta_e^f u$ for some integer f and thus Y is of naive type. Hence we can assume $r \geq 3$.

Recall that $Z \in \mathbb{Z}[\zeta_e]$ and $|Z|^2 = 3^{2b}$. By Result 2.7, there is an integer j such that

$$Z\zeta_e^j \in \mathbb{Z}[\zeta_{2^r}] \text{ or } Z = \zeta_e^j(\zeta_3 - \zeta_3^2)T \text{ with } T \in \mathbb{Z}[\zeta_{2^r}]. \tag{1}$$

We now need to consider the prime ideal factorization of $3\mathbb{Z}[\zeta_{2^r}]$ in $\mathbb{Z}[\zeta_{2^r}]$. By [10, Lem. 1.4.11], we have $\mathrm{ord}_{2^r}(3) = 2^{r-2}$. Thus the number of prime ideals above $3\mathbb{Z}[\zeta_{2^r}]$ is $\varphi(2^r)/\mathrm{ord}_{2^r}(3) = 2$. Write $3\mathbb{Z}[\zeta_{2^r}] = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of $\mathbb{Z}[\zeta_{2^r}]$. Recall that $X = 1 + \zeta_8 + \zeta_8^3$. Note that $|X|^2 = 3$ and thus

$$(X\mathbb{Z}[\zeta_{2^r}])(\overline{X}\mathbb{Z}[\zeta_{2^r}]) = 3\mathbb{Z}[\zeta_{2^r}] = \mathfrak{p}_1\mathfrak{p}_2.$$

Hence we may assume

$$\mathfrak{p}_1 = X\mathbb{Z}[\zeta_{2^r}] \text{ and } \mathfrak{p}_2 = \overline{X}\mathbb{Z}[\zeta_{2^r}]. \tag{2}$$

Recall that $Z\zeta_e^j \in \mathbb{Z}[\zeta_{2^r}]$ or $Z = \zeta_e^j(\zeta_3 - \zeta_3^2)T$ with $T \in \mathbb{Z}[\zeta_{2^r}]$ by (1). First suppose that

$$Z\zeta_e^j \in \mathbb{Z}[\zeta_{2^r}]. \tag{3}$$

Recall that and $|Z|^2 = 3^{2b}$. As $3\mathbb{Z}[\zeta_{2^r}] = \mathfrak{p}_1\mathfrak{p}_2$, this implies

$$Z\mathbb{Z}[\zeta_{2^r}] = \mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}$$

for some nonnegative integers d_1, d_2 with $d_1+d_2 = 2b$. Using (2), we conclude that $Z = \alpha X^{d_1}\bar{X}^{d_2}$ for some $\alpha \in \mathbb{Z}[\zeta_{2^r}]$. As $|Z|^2 = 3^{2b}$ and $|X|^2 = 3$, we have $|\alpha| = 1$. Thus α is a root of unity by Result 2.5. Hence there is an integer k such that

$$Y\zeta_e^k = 2^a Z\zeta_e^k = 2^a X^{d_1}\bar{X}^{d_2}. \tag{4}$$

If $d_2 = 0$, then $d_1 = 2b$ and Y is of sophisticated type. Similarly, if $d_2 = 0$, then Y is also of sophisticated type. Now suppose $d := \min(d_1, d_2) > 0$. If $d = b$, then $Y\zeta_e^k = 2^a 3^b$ and thus Y is of naive type. Hence we may assume $d < b$. Note that $|\zeta_3 - \zeta_3^2|^2 = -(\zeta_3 - \zeta_3^2)^2$. Thus

$$|X|^{2d} = 3^d = |\zeta_3 - \zeta_3^2|^{2d} = (-1)^d(\zeta_3 - \zeta_3^2)^{2d}.$$

Using (4), we conclude

$$Y\zeta_e^k = 2^a|X|^{2d}X^{d_1-d}\bar{X}^{d_2-d} = 2^a(-1)^d(\zeta_3 - \zeta_3^2)^{2d}X^{d_1-d}\bar{X}^{d_2-d}.$$

Note that $d_1 = d$ or $d_2 = d$. First suppose that $d_1 = d$. Then $2b = d_1 + d_2 = d + d_2$ and

$$Y\zeta_e^k(-1)^d = 2^a(\zeta_3 - \zeta_3^2)^{2d}\bar{X}^{d_2-d} = 2^a(\zeta_3 - \zeta_3^2)^{2d}\bar{X}^{2b-2d}.$$

As $d < b$, we conclude that Y is of Gauss type. Similarly, if $d_2 = d$, then Y is also of Gauss type. In summary, we have shown that the assertion of the Lemma is correct if (3) holds.

Now suppose that

$$Z = \zeta_e^j(\zeta_3 - \zeta_3^2)T \text{ with } T \in \mathbb{Z}[\zeta_{2^r}].$$

Then $|T|^2 = 3^{2b-1}$ and a similar argument as above shows that $T = \zeta_{2^r}^k X^{d_1}\bar{X}^{d_2}$ for some integer k and nonnegative integers d_1, d_2 with $d_1+d_2 = 2b-1$. Again, by a similar argument as above,

$$Y = 2^a Z = 2^a\zeta_e^j(\zeta_3 - \zeta_3^2)T = 2^a\zeta_e^j\zeta_{2^r}^k(\zeta_3 - \zeta_3^2)X^{d_1}\bar{X}^{d_2}$$

is of Gauss type. □

3 Setup

Let $u = 2^a 3^b$, where a and b are positive integers, and $G = H \times K$, where H is an abelian group of order 2^{2a+2} and $K \cong C_{3^{2b}}$. Let z be a generator of K and let P be the subgroup of order 3 of K. Suppose that G contains a $(4u^2, 2u^2 - u, u^2 - u, u^2)$ difference set D. We write

$$\begin{aligned} D &= \sum_{i=0}^{3^{2b-1}-1} D_i z^i, \\ D_i &= D_{i0} + D_{i1} z^{3^{2b-1}} + D_{i2} z^{2 \cdot 3^{2b-1}} \end{aligned}$$

for $i = 0, 1, 2$ with $D_i \subset H \times P$ and $D_{ij} \subset H$.

Write $e = \exp(G)$. For any nontrivial character χ of G, we have $\chi(D) \in \mathbb{Z}[\zeta_e]$ and $|\chi(D)|^2 = u^2$ by Result 2.1. Hence $\chi(D)$ is one of the Weil numbers listed in Lemma 2.9.

Throughout this paper, we fix the putative difference set D. This allows us to speak of naive, Gauss type, and sophisticated characters without explicit reference to D. For instance, by a "sophisticated character", we mean a character χ such that $\chi(D)$ is of sophisticated type.

4 Building Set Property

Let χ be a character of G which is nontrivial on $H \times P$. We say that χ has the "building set property" (c.f. [5]) if there is $i \in \{0, \ldots, 3^{2b-1} - 1\}$ with $|\chi(D_i)| = u^2$ and $\chi(D_j) = 0$ for all $j \neq i$.

Lemma 4.1 *Let χ be a character of G whose order is divisible by 3^{2b}. Then χ has the building set property.*

Proof Write $f = \exp(H)$. Note that

$$\chi(D) = \sum_{i=0}^{3^{2b-1}-1} \chi(D_i)\chi(z)^i$$

with $\chi(D_i) \in \mathbb{Z}[\zeta_{3f}]$. Recall that we write $e = \exp(G)$ and that we have $X \in \mathbb{Z}[\zeta_8]$ in Lemma 2.9 and thus $X(\zeta_3 - \zeta_3^2) \in \mathbb{Z}[\zeta_{24}]$. Hence

$$\chi(D)\zeta_e^j \in \mathbb{Z}[\zeta_{3f}] \tag{5}$$

for some integer j for Lemma 2.9. Note that $\chi(z)$ is a primitive 3^{2b}th root of unity. Thus $\{\chi(z)^i : i = 0, \ldots, 3^{2b-1} - 1\}$ is linearly independent over $\mathbb{Q}(\zeta_{3f})$. Together with (5), this implies that there is at most one i with $\chi(D_i) \neq 0$.

□

Lemma 4.2 *Let ϕ be a character of G which is trivial on K and let τ be a character of G of order 3^{2b}. We have*

(i) $\phi(D_i) + \phi\tau(D_i) + \phi\tau^2(D_i) \equiv 0 \pmod 3$,

(ii) $\phi(D_i) \equiv 0 \pmod{2^a}$

for $i = 0, \ldots, 3^{2b-1} - 1$.

Proof Note that the restriction of τ to $H \times P$ is a character of $H \times P$ of order 3. By Lemma 2.8 (with $W = H \times P$ and $U = H$), we have

$$3\phi(D_{i0}) = \phi(D_i) + \phi\tau(D_i) + \phi\tau^2(D_i).$$

This implies (i).

Let α be a character of G of order 3^{2b-1}. Note that $\langle\alpha\rangle = (H \times P)^\perp$. By Lemma 2.8 (with $W = G$ and $U = H \times P$), we have

$$3^{2b-1}\phi(D_i) = \sum_{i=0}^{3^{2b-1}-1} \phi\alpha^i(D).$$

But $\phi\alpha^i(D) \equiv 0 \pmod{2^a}$ for all i by Lemma 2.9. This implies (ii). □

We now show that sophisticated characters have a property which is even stronger than the building set property. In the proof, we use some standard facts from algebraic number theory. We refer the reader to [6] for the necessary background.

Lemma 4.3 *Let χ be a character of order dividing $f = \exp(H)$ and assume that χ is of sophisticated type. Then there are $i \in \{0, \ldots, 3^{2b-1} - 1\}$ and $j \in \{0, 1, 2\}$ such that $\chi(D_{ij}) \neq 0$ and $\chi(D_{rs}) = 0$ for all pairs $(r, s) \neq (i, j)$.*

Proof If f divides 4, then there is no sophisticated character by Lemma 2.9. Thus f is divisible by 8.

Replacing D by a translate, if necessary, we can assume $\chi(D_{00}) \neq 0$. Let τ be a character of G of order 3^{2b}. By Lemma 2.8, we have

$$3^{2b}\chi(D_{00}) = \sum_{k=0}^{3^{2b}-1} \chi\tau^k(D). \tag{6}$$

Note that $\chi(g) \equiv \chi\tau^k(g) \pmod{1 - \zeta_{3^{2b}}}$ for all $g \in G$ and thus

$$\chi(D) \equiv \chi\tau^k(D) \pmod{1 - \zeta_{3^{2b}}} \tag{7}$$

for all k. Recall that $e = \exp(G) = 3^{2b}f$.

As in the proof of Lemma 2.9, we see that $3\mathbb{Z}[\zeta_f] = (X\mathbb{Z}[\zeta_f])(\bar{X}\mathbb{Z}[\zeta_f])$ and $X\mathbb{Z}[\zeta_f]$ and $\bar{X}\mathbb{Z}[\zeta_f]$ are prime ideals of $\mathbb{Z}[\zeta_f]$. Both of these prime ideals are totally ramified in $\mathbb{Q}(\zeta_e)/\mathbb{Q}(\zeta_f)$. Hence there is a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_e]$ with

$$X\mathbb{Z}[\zeta_e] = \mathfrak{p}^{\varphi(3^{2b})} \text{ and } \bar{X}\mathbb{Z}[\zeta_e] = \bar{\mathfrak{p}}^{\varphi(3^{2b})}. \tag{8}$$

Furthermore, we have $\mathfrak{p}\bar{\mathfrak{p}} = (1 - \zeta_{3^{2b}})\mathbb{Z}[\zeta_e]$, as $X\bar{X}\mathbb{Z}[\zeta_e] = 3\mathbb{Z}[\zeta_e] = (1 - \zeta_{3^{2b}})^{\varphi(3^{2b})}\mathbb{Z}[\zeta_e]$. Since χ is of sophisticated type, we have

$$\chi(D)\mathbb{Z}[\zeta_e] = 2^a X^{2b}\mathbb{Z}[\zeta_e] \text{ or } \chi(D)\mathbb{Z}[\zeta_e] = 2^a \bar{X}^{2b}\mathbb{Z}[\zeta_e] \tag{9}$$

by Lemma 2.9. By (8) and (9), either $\mathfrak{p}$ or $\bar{\mathfrak{p}}$ does not divide $\chi(D)\mathbb{Z}[\zeta_e]$. Hence we can assume that $\mathfrak{p}$ does not divide $\chi(D)\mathbb{Z}[\zeta_e]$. Note that $\mathfrak{p}$ divides $(1 - \zeta_{3^{2b}})\mathbb{Z}[\zeta_e]$, as $\mathfrak{p}\bar{\mathfrak{p}} = (1 - \zeta_{3^{2b}})\mathbb{Z}[\zeta_e]$. By (7), we conclude $\chi\tau^k(D) \notin \mathfrak{p}$ for all k. Hence $\chi\tau^k(D)$ is of sophisticated type, too, and

$$\chi\tau^k(D) = \zeta_e^{j(k)}\chi(D)$$

for some integers $j(k)$ by Lemma 2.9. If $j(k) \not\equiv 0 \pmod{f}$, then $\chi(D) - \chi\tau^k(D) = (1 - \zeta_e^{j(k)})\chi(D) \notin \mathfrak{p}$. This contradicts (7) and hence there are integers $l(k)$ such that

$$\chi\tau^k(D) = \zeta_{3^{2b}}^{l(k)}\chi(D) \tag{10}$$

for all k. Write

$$T = \sum_{k=0}^{3^{2b}-1} \zeta_{3^{2b}}^{l(k)}.$$

From (6) and (10), we get

$$\chi(D)T \equiv 0 \pmod{3^{2b}}. \tag{11}$$

As $\chi(D)$ is of sophisticated type, we may assume $\chi(D) = 2^a X^{2b}$. Recall that we have shown that $X\mathbb{Z}[\zeta_f]$ and $\bar{X}\mathbb{Z}[\zeta_f]$ are distinct prime ideals of $Z[\zeta_f]$. Hence $X\mathbb{Z}[\zeta_e]$ and $\bar{X}\mathbb{Z}[\zeta_e]$ are coprime. As $X\bar{X} = 3$, we conclude

$$T \equiv 0 \pmod{\bar{X}^{2b}} \tag{12}$$

from (11). Define $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})$ by $\zeta_{3^{2b}}^{\sigma} = \zeta_{3^{2b}}$ and $\zeta_f^{\sigma} = \bar{\zeta_f}$. Applying σ to (12) shows $T \equiv 0 \pmod{X^{2b}}$ and thus

$$T \equiv 0 \pmod{3^{2b}}. \tag{13}$$

Note that $T \neq 0$, since $T\chi(D) = 3^{2b}\chi(D_{00})$ by (6) and $\chi(D_{00}) \neq 0$. Let N denote the absolute norm of $\mathbb{Q}(\zeta_{3^{2b}})$. Note that $T^{\sigma} \equiv 0 \pmod{3^{2b}}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{3^{2b}})/\mathbb{Q})$ by (13). Thus

$$\mathrm{N}(T) \equiv 0 \pmod{\left(3^{2b}\right)^{|\mathrm{Gal}(\mathbb{Q}(\zeta_{3^{2b}})/\mathbb{Q})|}}$$

and $\mathrm{N}(T)$ is a nonzero integer. Hence $|N(T)| \geq \left(3^{2b}\right)^{|\mathrm{Gal}(\mathbb{Q}(\zeta_{3^{2b}})/\mathbb{Q})|}$, and this implies that there is $\kappa \in \mathrm{Gal}(\mathbb{Q}(\zeta_{3^{2b}})/\mathbb{Q})$ with $|T^{\kappa}| \geq 3^{2b}$. As T^{κ} is a sum of 3^{2b} roots of unity and $|T^{\kappa}| \geq 3^{2b}$, all these root of unity must be equal. This means that $l(k) = c$ for all k for some fixed integer c. Since $T = 3^{2b}\chi(D_{00})\chi(D)^{-1} \in \mathbb{Q}(\zeta_f)$, we conclude $c = 0$ and thus $T = 3^{2b}$. Hence $\chi(D) = \chi(D_{00})$ by (6).

Now let $(r, s) \neq (0, 0)$. Recall that we have shown $l(k) = 0$ for all k. This implies $\chi\tau^k(D) = \chi(D)$ for all k. By Lemma 2.8, we have

$$3^{2b}\chi(D_{rs}) = \sum_{k=0}^{3^{2b}-1} \chi\tau^k(Dz^{-r-3^{2b-1}s}) = \chi(D) \sum_{k=0}^{3^{2b}-1} \tau^k(z^{-r-3^{2b-1}s}). \tag{14}$$

But $z^{-r-3^{2b-1}s} \neq 1$, since $(r, s) \neq (0, 0)$. Thus $\sum_{k=0}^{3^{2b}-1} \tau^k(z^{-r-3^{2b-1}s}) = 0$ and hence $\chi(D_{rs}) = 0$. $\square$

Corollary 4.4 *Let χ be a character of sophisticated type and let 2^m be the highest power of 2 dividing the order of χ. Then*

$$2^m \leq \frac{2^{a+3}}{3^b}.$$

Proof By Lemma 4.3, we have $|\chi(D_{ij})| = |\chi(D)| = u^2$ for some integers i, j. Since the kernel of χ on H has order 2^{2a+2-m}, we can write

$$\chi(D_{ij}) = \sum_{k=0}^{2^m-1} a_k \zeta_{2^m}^k$$

for some integers a_k with $0 \leq a_k \leq 2^{2a+2-m}$. Hence

$$u^2 \leq \frac{2^{4a+4-2m} 8^2}{4 \cdot 4}$$

by Result 2.6. This implies the assertion. □

5 A Necessary Condition

We use the results of the previous sections to derive a necessary condition for the existence of Hadamard difference sets with $u = 2^a 3^b$ in abelian groups with cyclic Sylow 3-subgroups.

Theorem 5.1 *Suppose that a Hadamard difference set with $u = 2^a 3^b$ exists in an abelian group which has a cyclic Sylow 3-subgroup. Then $2^a > 3^b$.*

Proof We use the notation introduced in the previous sections. Suppose that $2^a < 3^b$. Let χ be a character of sophisticated type and let 2^m be the highest power of 2 dividing the order of χ. Then

$$2^m \leq \frac{2^{a+3}}{3^b} = 8\frac{2^a}{3^b} < 8$$

by Corollary 4.4 and the assumption $2^a < 3^b$. But by Lemma 2.9 there is no sophisticated character of order < 8, as X involves ζ_8. Hence there are no characters of sophisticated type.

Note that $\chi(D) \equiv 0 \pmod{1-\zeta_3}$ for all characters χ of naive and Gauss type. For characters of Gauss type this is clear from their definition, and

for characters of naive type this follows from $3 \equiv 0 \pmod{1-\zeta_3}$. Hence, as there are no sophisticated characters, we have $\chi(D) \equiv 0 \pmod{1-\zeta_3}$ for all characters χ of G. Let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[\zeta_{3^{2b}}][H]$ be the homomorphism defined by $\rho(z) = \zeta_{3^{2b}}$ and $\rho(h) = h$ for all $h \in H$. Note that

$$\mathrm{Ker}(\rho) = \{XP : X \in \mathbb{Z}[G]\},$$

where P is the subgroup of G of order 3. Since $\chi(D) \equiv 0 \pmod{1-\zeta_3}$ for all characters χ of G, we have $\rho(D) \equiv 0 \pmod{1-\zeta_3}$ by the inversion formula. Hence there is $Y \in \mathbb{Z}[G]$ with $\rho(D) = \rho((1-w)Y)$, where w is an element of order 3 of G. This implies

$$D = (1-w)Y + ZP \tag{15}$$

for some $Z \in \mathbb{Z}[G]$. Let $\beta : G \to G/P$ be the canonical epimorphism. We have $\beta(D) \equiv 0 \pmod{3}$ by (15). But since D has coefficients $0, 1$ only, this implies $D = PZ$ for some $Z \subset G$. This is impossible by Result 2.1. □

Remark 5.2 In the proof of Theorem 5.1 we showed that there must be at least one sophisticated character. This result can be extended to all putative counterexamples to Lander's conjecture as follows. Let G be an abelian group of order v containing a difference D set of order n. Let p be a prime dividing v and n, and suppose the Sylow p-subgroup of G is cyclic. Then there is a nontrivial character χ of with $\chi(D) \not\equiv 0 \pmod{1-\zeta_p}$. This observation will be used in further publications (in preparation).

6 The Case $b = 1$

Throughout the rest of the paper, let $b = 1$. This is a particularly interesting and difficult case, as the cyclic Sylow 3-subgroup is as small as possible. As Theorem 5.1 indicates, groups with larger cyclic Sylow 3-subgroups seem to be less likely to contain Hadamard difference sets.

Lemma 6.1 *Let ϕ be a character of $H \times P$ which is trivial on P and nontrivial on H. Then exactly one of the values $\phi(D_i)$, $i = 0, 1, 2$, is nonzero.*

Proof Let τ be a character of order 3 of $H \times P$. Note that τ can be extended to a character of order 9 of G and that $3^{2b} = 9$, as we assume $b = 1$. Thus, by Lemma 4.1, there is $j \in \{0, 1, 2\}$ such that $\phi\tau(D_k) = 0$ for $k \neq j$. As $\phi\tau^2$ is equivalent to $\phi\tau$, this implies $\phi\tau^2(D_k) = 0$ for $k \neq j$. Hence

$$\phi(D_k) \equiv 0 \pmod{3 \cdot 2^a} \tag{16}$$

for $k \neq j$ by Lemma 4.2.

If $\phi(D_k) = 0$ for all $k \neq j$, then the assertion of the Lemma holds. Thus suppose $\phi(D_k) \neq 0$ for some $k \neq j$. Recall that $u = 3 \cdot 2^a$. Note that $\phi(D_k) \in \mathbb{Z}[\zeta_f]$. As $\phi(D_k) \equiv 0 \pmod{u}$ by (16), we have $\phi(D_k)^\sigma \equiv 0 \pmod{u}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$. Thus

$$\mathrm{N}(\phi(D_k)) \equiv 0 \pmod{u^{f/2}},$$

where N denotes the absolute norm of $\mathbb{Q}(\zeta_f)$. Since $\mathrm{N}(\phi(D_k))$ is a nonzero integer, it follows that $|\phi(D_k)^\sigma| \geq u$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$.

On the other hand, as D is a Hadamard difference set of order u^2, we have

$$D_0 D_0^{(-1)} + D_1 D_1^{(-1)} + D_2 D_2^{(-1)} = u^2 + (u^2 - u)(H \times P)$$

by Result 2.1. This implies

$$|\phi(D_0)^\sigma|^2 + |\phi(D_1)^\sigma|^2 + |\phi(D_2)^\sigma|^2 = u^2.$$

As $|\phi(D_k)^\sigma| \geq u$, it follows that $|\phi(D_k)^\sigma| = u$ and $\phi(D_r)^\sigma = 0$ for $r \neq k$. Hence $\phi(D_r) = 0$ for $r \neq k$, too. □

Consider any character χ of G which is nontrivial on $H \times P$. If the order of χ is divisible by 9, then χ has the building set property by Lemma 4.2. If the order of χ is not divisible by 9, then $\chi|_{H \times P}$ is trivial on P and nontrivial on H. Thus χ has the building set property by Lemma 6.1.

In summary, we have shown the following.

Lemma 6.2 *For every character χ of G which is nontrivial on $H \times P$, there is $i \in \{0, 1, 2\}$ with $|\chi(D_i)| = u$ and $\chi(D_j) = 0$ for $j \neq i$.*

Corollary 6.3 *We have*

$$\{|D_0|, |D_1|, |D_2|\} = \{(2^{a+1}-1)u, 2^{a+1}u, 2^{a+1}u\}$$

(*viewed as an equality of multisets*).

Proof Let χ be the character of G of order 3 with $\chi(z) = \zeta_3$. Note that $\chi(D) \equiv 0 \pmod{u}$, since u is self-conjugate mod 3. Replacing D by a translate, if necessary, we can assume

$$|D_0| + \zeta_3|D_1| + \zeta_3^2|D_2| = \chi(D) = \pm u.$$

Hence, if $\chi(D) = u$, then, as multisets, $\{|D_0|, |D_1|, |D_2|\} = \{2^{a+1}(u-1), 2^{a+1}(u-1), 2^{a+1}(u-1)+u\}$. Let τ be a character of order 9 of G. Lemma 6.2 implies that $\tau(D_i) = 0$ for some $i \in \{0,1,2\}$. But this implies that $|D_i|$ is divisible by 3, a contradiction. Hence we conclude $\chi(D) = -u$ and this implies $\{|D_0|, |D_1|, |D_2|\} = \{(2^{a+1}-1)u, 2^{a+1}u, 2^{a+1}u\}$ as multisets. □

6.1 The Homomorphic Images of the D_i in $\mathbb{Z}[H]$

Recall that we assume $b = 1$ and write

$$D = D_0 + zD_1 + z^2D_2$$

with $D_i \subset H \times P$. In view of Corollary 6.3, we may assume $|D_0| = (2^{a+1}-1)u$, $|D_1| = |D_2| = 2^{a+1}u$.

Corollary 6.4 *Write $f = \exp(H)$ and $X = 1 + \zeta_8 + \zeta_8^3$. Let $i \in \{0,1,2\}$ and let χ be character of G which is nontrivial on H and trivial on K. Then there is an integer k, depending on χ, such that*

$$\zeta_f^k \chi(D_i) \in \{0, u, 2^a X^2, 2^a \bar{X}^2\}. \tag{17}$$

Furthermore, if the order of χ divides 4, there is an integer s with

$$\zeta_4^s \chi(D_i) \in \{0, u\}. \tag{18}$$

Proof Lemma 6.2 implies

$$\chi(D_i) = \zeta_f^j \chi(D) \tag{19}$$

for some integer j. Note that $\chi(D)$ cannot be of Gauss type, since χ is of order dividing f. Moreover, if the order of χ divides 4, then $\chi(D)$ cannot be of sophisticated type either. Hence (17) and (18) follow from (19) and Lemma 2.9. □

Lemma 6.5 *Let $\rho : H \times P \to H$ be the canonical epimorphism and write $\bar{D}_i = \rho(D_i)$, $i = 0, 1, 2$. Let x_i be the number of nontrivial characters χ of H with $|\chi(\bar{D}_i)| = u$ and let y_i be the number of coefficients of $\bar{D}_i$ which are divisible by 3. Then*

$$\begin{array}{rcl} 8y_0 & = & 9x_0 - 2^{2a+2} + 9 \quad \textit{and} \\ 8y_i & = & 9x_i - 2^{2a+2} \quad \textit{for } i = 1, 2. \end{array} \tag{20}$$

Furthermore,

$$\sum_{i=0}^{2} x_i = 2^{2a+2} - 1 \textit{ and } \sum_{i=0}^{2} y_i = 3 \cdot 2^{2a}. \tag{21}$$

Proof Write $D_i = \sum_{g \in H} a_{ig} g$ with $a_{ig} \in \{0, 1, 2, 3\}$, and let $E_i = 3H - 2\bar{D}_i$. Note that $3 - 2a_{ig} = \pm 1$ if $a_{ig} = 1$ or 2; and $3 - 2a_{ig} = \pm 3$ if $a_{ig} = 0$ or 3. Hence the coefficient of of 1 in $E_i E_i^{(-1)}$ is

$$\sum_{g \in H} (3 - 2a_{ig})^2 = 9y_i + (2^{2a+2} - y_i) = 8y_i + 2^{2a+2}. \tag{22}$$

On the other hand, by Lemma 6.4, we have $\chi(\bar{D}_i) = 0$ for each nontrivial character χ of H with $|\chi(\bar{D}_i)| \neq 12$. Thus, by Result 2.2, the coefficient of of 1 in $E_i E_i^{(-1)}$ is

$$\frac{1}{2^{2a+2}}((3 \cdot 2^{2a+2} - 2|D_i|)^2 + 9 \cdot 2^{2a+2} x_i). \tag{23}$$

From (22) and (23), we get

$$8y_i + 2^{2a+2} = \frac{1}{2^{2a+2}}((3 \cdot 2^{2a+2} - 2|D_i|)^2 + 9 \cdot 2^{2a+2} x_i).$$

Since $|D_0| = (2^{a+1} - 1)u$ and $|D_1| = |D_2| = 2^{a+1}u$, we get (20).

Lemma 3.2 shows that every nontrivial character of H contributes to exactly one of the numbers x_i. Thus $\sum x_i = 2^{2a+2} - 1$. Finally, the second equation in (21) follows from the first and (20). □

6.2 The case $b = 1$ and $a = 2$

From now on, let $b = 1$ and $a = 2$. We view characters χ of H also as characters of $G = H \times K$ by setting $\chi(g) = 1$ for all $g \in K$. For $i = 0, 1, 2$, let N_i, respectively S_i, be the set of nontrivial characters of H of naive, respectively sophisticated, type. Recall that characters of H cannot be of Gauss type. Thus $\chi(D_i) = 0$ for all nontrivial characters χ of H with $\chi \notin N_i \cup S_i$. Thus Result 2.2 implies

$$64\bar{D}_i = |D_i|H + \sum_{g \in H} \left[\sum_{\chi \in S_i} \chi(D_i)\chi(g^{-1}) + \sum_{\chi \in N_i} \chi(D_i)\chi(g^{-1}) \right] g. \tag{24}$$

Note that N_i and S_i are unions of equivalence classes of characters. Furthermore, by Lemma 2.9 and Corollary 4.4, every character in S_i has order 8. Suppose there are exactly r_i inequivalent characters in S_i, say $\tau_1, \tau_2, \ldots, \tau_{r_i}$. Let Tr denote the absolute trace of $\mathbb{Q}(\zeta_8)$ and write $\bar{D}_i = \sum_{g \in H} a_g g$. Then

$$64\bar{D}_i = \sum_{g \in H} 64 a_g g = |D_i|H + \sum_{g \in H} \left[\sum_{j=1}^{r_i} \mathrm{Tr}(\tau_j(D_i g^{-1})) + \sum_{\chi \in N} \chi(D_i)\chi(g^{-1}) \right] g.$$

Recall that $|D_i| \equiv 0 \pmod 3$ for all i by Corollary 6.3. As $\chi(D_i) \equiv 0 \bmod 3$ for all $\chi \in N_i$, we conclude that

$$a_g \equiv 0 \bmod 3 \text{ if and only if } \sum_{j=1}^{r_i} \mathrm{Tr}(\tau_j(D_i g^{-1})) \equiv 0 \bmod 3. \tag{25}$$

It turns out that (25) gives enough information on the values y_i defined in Lemma 6.5 to show that no Hadamard difference sets exist in $C_9 \times C_{16} \times C_4$, $C_9 \times C_{16} \times C_2 \times C_2$, and $C_9 \times C_8 \times C_8$. The last of these groups is by far the most difficult case, since we have to deal with a larger number of equivalence classes of sophisticated characters than in the first two cases.

6.3 The Groups $C_9 \times C_{16} \times C_4$ and $C_9 \times C_{16} \times C_2 \times C_2$

Suppose that $H = C_{16} \times C_4$ or $H = C_{16} \times C_2 \times C_2$. We continue to use the notation introduced above. Recall that all sophisticated characters of H have order 8. Note that there are exactly 4 equivalence classes of characters

of order 8 of H. Hence there is $i \in \{0,1,2\}$, such that the set S_i consists of at most 1 equivalence class, i.e., $r_i \leq 1$.

Recall that $y_j \equiv 1 \pmod 9$ for $j = 0,1,2$ by Lemma 6.5 and $y_0+y_1+y_2 = 48$. If $r_i = 0$, then $y_i = 64$ by (25), which is impossible. Hence $r_i = 1$ and we can assume

$$\tau_1(D_i) = 4(-1 + 2\zeta_8 + 2\zeta_8^3) \tag{26}$$

by Lemma 2.9. Recall that τ_1 is a character of H of order 8. It is straightforward to check that (26) implies that $\mathrm{Tr}(\tau_1(D_i g^{-1}))$ takes each of the values 0 and ± 32 exactly 16 times and each of the values ± 16 exactly 8 times when g ranges over H. This implies $y_i = 16$, contradicting $y_i \equiv 1 \pmod 9$. Hence no Hadamard difference sets exist in $C_9 \times C_{16} \times C_4$ and $C_9 \times C_{16} \times C_2 \times C_2$.

6.4 The Group $C_9 \times C_8 \times C_8$

Suppose that $H = C_8 \times C_8$. Recall that $y_i \equiv 1 \bmod 9$ for $i = 0,1,2$. As $y_0+y_1+y_2 = 48$, we have $y_i \in \{1,10\}$ for at least one i. From now on, we fix such an i with $y_i \in \{1,10\}$ and write $N = N_i$, $S = S_i$, $r = r_i$ for convenience. Note that $x_i \leq 16$ by Lemma 6.5.

For each $j = 1,\ldots,r$, there exists a unique involution h_j in H with $\tau_j(h_j) = 1$. We claim that the h_j's are not all equal. Otherwise, we have $\tau_1(h) = \cdots = \tau_r(h) = \pm 1$ for every involution $h \in H$. Therefore, $\sum_{j=1}^r \mathrm{Tr}(\tau_j(D_i g^{-1})) = \pm \sum_{j=1}^r \mathrm{Tr}(\tau_j(D_i (gh)^{-1}))$ for all $g \in H$ and all involutions h in H. Thus (25) shows that $a_g \equiv 0 \bmod 3$ if and only if $a_{gh} \equiv 0 \bmod 3$, for all involutions $h \in H$. This implies $y_i \equiv 0 \pmod 4$, which contradicts $y_i \in \{1,10\}$. Thus we may assume $r \geq 2$ and $h_1 \neq h_2$.

Let g_1, g_2, g_3 denote the involutions in H.

Lemma 6.6 *Write $X_j = \{\chi \in N \cup S : \chi(g_j) = -1\}$ for $j = 1,2,3$. Then*

$$\sum_{\chi \in X_j} \chi(D_i)\chi(g^{-1}) \equiv 0 \bmod 32$$

for all $g \in G$.

Proof Note that (24) implies

$$64|a_g - a_{gg_j}| = 2\left|\sum_{\chi\in X_j}\chi(D_i)\chi(g^{-1})\right|.$$

□

Next, recall that all τ_j's are sophisticated. It is straightforward to verify the following.

Lemma 6.7 *Let $\langle x\rangle$ be a cyclic subgroup of order 8 in H.*

(i) Suppose the restriction of τ_j to $\langle x\rangle$ has order 8. Then $\mathrm{Tr}(\tau_j(D_i(gx^k)^{-1})$ takes each of the values $0, 32, -32$ exactly twice and each of the values ± 16 exactly once for $k = 0, \ldots, 7$.

(ii) Suppose the restriction of τ_j to $\langle x\rangle$ has order 4. Then

$$\{\mathrm{Tr}(\tau_j(D_i(gx^k)^{-1})) : k = 0, \ldots, 3\} = \{0, 16, -16\} \text{ or } \{32, -32\}.$$

We are now ready to prove that no such D_i exists. Recall that we assume $h_1 \neq h_2$ and $r \geq 2$. Let $H_1 = \mathrm{Ker}\,\tau_1$. Then $\tau_2|_{H_1}$ is of order 8. We write $H = \bigcup_{j=0}^{7} H_1h^j$ for some $h \in H$. Note that $\mathrm{Tr}(\tau_1(D_i(g^{-1}))$ remains constant when g ranges over H_1h^j. On the other hand, $\mathrm{Tr}(\tau_2(D_i(g^{-1}))$ takes each of the values $0, \pm 32$ twice and each value ± 16 once when g varies over H_1h^j. By (24), this implies that $y_i \geq 16$ if $r = 2$, contradicting $y_i \in \{1, 10\}$. Thus $r \geq 3$.

Now suppose $|\{h_1, \ldots, h_r\}| = 3$. Without loss of generality, we may assume that h_1, h_2, h_3 are distinct and $h_3 = g_3$. As $|x_i| \leq 16$, there exists at most one equivalence class of characters of order 8 in $S \cup N$ different from the equivalence classes of τ_1, τ_2, and τ_3. We may therefore assume that all characters in $S \cup N$ which are not equivalent to τ_1 or τ_2 map g_3 to 1. Thus, by Lemma 6.6, we have

$$\sum_{\chi\in X_3}\chi(D_i)\chi(g^{-1}) = \mathrm{Tr}(\tau_1(D_ig^{-1})) + \mathrm{Tr}(\tau_2(D_ig^{-1})) \equiv 0 \bmod 32 \qquad (27)$$

for all $g \in H$. This is impossible as $\mathrm{Tr}(\tau_1(D_i(g^{-1}))$ remains constant and $\mathrm{Tr}(\tau_2(D_i(g^{-1}))$ takes values $0, \pm 16, \pm 32$ when g varies over $H_1 h^j$. Thus $|\{h_1, \ldots, h_r\}| = 2$ and we may assume $h_3 = h_2$. Hence $\tau_2 \notin X_3$. We have $\tau_1 \in X_3$, since $h_1 \neq h_3$, and $\tau_3 \notin X_3$ by the definition of X_3.

Note that X_3 only contains characters of order 8. As $\mathrm{Tr}(\tau_1(D_i g^{-1}))$ takes values ± 16 for some $g \in H$, Lemma 6.6 implies that X_3 contains a character τ inequivalent to τ_1. Since $x_i \leq 16$, we conclude that $S \cup N$ consists exactly of the characters equivalent to one of τ, τ_1, τ_2 or τ_3 and that $x_i = 16$. This implies $|D_i| = 96$. Furthermore,

$$\sum_{\chi \in X_3} \chi(D_i)\chi(g^{-1}) = \mathrm{Tr}(\tau_1(D_i g^{-1})) + \mathrm{Tr}(\tau(D_i g^{-1})) \equiv 0 \bmod 32 \tag{28}$$

for all $g \in H$ by Lemma 6.6.

We first consider the case $\tau \in N$. Let $H' = \mathrm{Ker}\, \tau$. It follows from the definition of N that there exists $h \in H$ with $\mathrm{Tr}(\tau(D_i g^{-1})) = 48$ for all $g \in H'h$. By Lemma 24 and (28), we conclude that $\mathrm{Tr}(\tau_1(D_i g^{-1})) = \pm 16$ for all $g \in H'h$. However, as τ is not equivalent to τ_1, Lemma 6.7 shows that the order of τ_1 on H' is 2. Let $F = \mathrm{Ker}\, \tau_1 \neq H'$. We can write $H'h = Ff_1 \cup Ff_2$ such that

$$\mathrm{Tr}(\tau_1(D_i g^{-1})) = \begin{cases} 16 & \text{if } g \in Ff_1 \\ -16 & \text{if } g \in Ff_2. \end{cases}$$

Recall that

$$96 + \mathrm{Tr}(\tau(D_i g^{-1})) + \sum_{j=1}^{3} \mathrm{Tr}(\tau_j(D_i g^{-1})) \equiv 0 \bmod 64$$

by (24). We therefore have

$$\mathrm{Tr}(\tau_2(D_i g^{-1})) + \mathrm{Tr}(\tau_3(D_i g^{-1})) \equiv \begin{cases} 32 \mod 64 & \text{if } g \in Ff_1, \\ 0 \mod 64 & \text{if } g \in Ff_2. \end{cases} \tag{29}$$

As both τ_2, τ_3 are of order 8 on H', it is easy to see that for $j = 1, 2$, we have

$$\begin{aligned} &\{\{\mathrm{Tr}(\tau_j(D_i g^{-1})) : g \in Ff_1\}, \{\mathrm{Tr}(\tau_j(D_i g^{-1})) : g \in Ff_2\}\} \\ &= \{\{0, 16, -16\}, \{32, -32\}\}. \end{aligned}$$

Observe that

$$\sum_{\chi \in X_1} \chi(D_i)\chi(g^{-1}) = \mathrm{Tr}(\tau_2(D_i g^{-1})) + \mathrm{Tr}(\tau_3(D_i g^{-1})) \equiv 0 \bmod 32$$

by Lemma 6.6. This forces

$$\{\mathrm{Tr}(\tau_2(D_i g^{-1})) : g \in F f_k\} = \{\mathrm{Tr}(\tau_3(D_i g^{-1})) : g \in F f_k\}.$$

for $k = 1, 2$. By (29), it follows that $\{\mathrm{Tr}(\tau_2(D_i g^{-1})) : g \in F f_1\} \neq \{32, -32\}$. But hence both $\mathrm{Tr}(\tau_2(D_i g^{-1}))$ and $\mathrm{Tr}(\tau_3(D_i g^{-1}))$ take the value 0 twice and the values $16, -16$ once, when g ranges over $F f_1$. But this contradicts (29).

Finally, we deal with the case $\tau \in S$ with a similar argument. We just need to take h such that $\mathrm{Tr}(\tau(D_i g^{-1})) = 16$ for all $g \in H'h$. Hence no Hadamard difference set exists in $C_9 \times C_8 \times C_8$. □

Together with previously known results (see [4]), our results imply that there is no Hadamard difference set in any group $C_9 \times H$, where H is an abelian 2-group of order at most 64. We believe the following problem deserves further study.

Question 6.8 *Does there exist a Hadamard difference set in any group $C_9 \times H$, where H is an abelian group of order 2^{2a}, $a \geq 4$?*

Acknowledgement The fourth author would like to acknowledge discussions with James Davis and Jonathan Jedwab. Attempts to construct a $C_8 \times C_8 \times C_9$ difference set began when the fourth author was visiting Davis at the University of Richmond in 2005. At that time, Davis, Jedwab, and Smith worked very hard to construct a difference set in this group and they still hold out hope for a counterexample to Lander's conjecture in families of the form $C_{2^k} \times C_{2^k} \times C_9$. The many suggestions of Davis and Jedwab and the hospitality of the University of Richmond are all gratefully acknowledged.

We are grateful to the referees for their careful reading of the paper and suggestions, which substantially improved the exposition of the paper.

References

[1] L. D. Baumert: *Cyclic Difference Sets.* Springer Lecture Notes **182**, Springer 1971.

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

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

[4] J. A. Davis, J. Jedwab: A survey of Hadamard difference sets. *K. T. Arasu (Ed.), Groups, Difference Sets and the Monster.* De Gruyter 1996, 145–156.

[5] J. A. Davis, J. Jedwab: A unifying construction of difference sets. *J. Combin. Theory Ser. A* **80** (1997), 13–78.

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

[7] E. S. Lander: *Symmetric Designs: An Algebraic Approach.* London Math. Soc. Lect. Notes **75**, Cambridge University Press 1983.

[8] 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.

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

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

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