Coprime actions and characters nonvanishing on the fixed-point subgroup

Eric Hou

July 30, 2026

Abstract

Let a finite group A act coprimely on a finite group G and put $C = C_G(A)$. A classical theorem of Burnside asserts that the irreducible characters of a group vanishing nowhere are exactly the linear ones, and Navarro asked in Problem 21.100 of the 21st Kourovka Notebook whether the coprime analogue holds: is the number of A-invariant $\chi \in \mathrm{Irr}(G)$ with χ_C nowhere zero always $|C/C'|$? We answer this negatively. For A cyclic of order 21 acting on $G = B \rtimes V$, where $V = \mathbf{F}_4^2 \oplus \mathbf{F}_8$ and B is the group of Boolean functions on V, the fixed subgroup $C \cong C_2^{12}$ carries all 4096 invariant characters while only 1728 of them are nowhere zero on C.

Because C is abelian the same example refutes Problem 6.3 of Navarro's problem list, and with it the corresponding statement about the head characters of Isaacs; passing to $G \rtimes A$ refutes Problem 6.7, a conjecture Isaacs reports is supported by abundant computational evidence. The construction needs only that V have an A-stable subset of half its size. This holds for infinitely many pairs (A, V), and for none of dimension below 7, so the example is minimal over all operator groups of odd order. Exact machine verifications, independent of the proofs, accompany the paper.

1 Introduction

A classical theorem of W. Burnside asserts that a nonlinear $\chi \in \mathrm{Irr}(G)$ must vanish at some element of G: the irreducible characters of G that are nonvanishing on all of G are exactly the linear ones, so that their number is $|G/G'|$ (see [7, Theorem 3.15]).

Now let A act on G by automorphisms with $(|A|, |G|) = 1$, and let

$$C = C_G(A)$$

be the fixed-point subgroup. Write

$$\mathrm{Irr}_A(G) = \{\chi \in \mathrm{Irr}(G) : \chi^a = \chi \text{ for all } a \in A\}$$

for the set of A-invariant irreducible characters of G, and

$$N_A(G) = \{\chi \in \mathrm{Irr}_A(G) : \chi(c) \neq 0 \text{ for all } c \in C\}$$

for those whose restriction to C is nonvanishing. Taking $A = 1$ gives $C = G$ and $\mathrm{Irr}_A(G) = \mathrm{Irr}(G)$, so Burnside's theorem says $|N_1(G)| = |G/G'|$. The following problem asks whether this persists relative to a coprime operator group.

Problem 21.100 (G. Navarro [10])**.** Suppose that A and G are finite groups such that A acts coprimely on G by automorphisms. Let $C = C_G(A)$ be the fixed-point subgroup, and let C' denote its derived subgroup. Is it true that the number of A-invariant irreducible characters χ of G whose restriction χ_C is never zero is exactly $|C/C'|$? This would follow if one could show that χ_C is never zero if and only if the Glauberman–Isaacs correspondent χ^* of χ is linear.

The question is motivated by a canonical bijection $\mathrm{Irr}_A(G) \to \mathrm{Irr}(C)$, $\chi \mapsto \chi^*$, constructed by G. Glauberman [4] for solvable A and extended to arbitrary A by I. M. Isaacs [6]; see also [11, Chapter 2]. The count $|C/C'|$ asked for is thus the number of *linear* characters of C, and the proposed criterion would identify $N_A(G)$ with their preimage under the correspondence. Our principal result shows that no such identification is possible.

Theorem A. *There exist a finite group $A \cong C_{21}$ and a finite 2-group G of order 2^{135}, with A acting faithfully and coprimely on G, such that*

$$|N_A(G)| = 1728 \qquad \textit{and} \qquad |C_G(A)/C_G(A)'| = 4096.$$

In particular the equality of Problem 21.100 fails.

The group is $G = B \rtimes V$, where $V = \mathbf{F}_4^2 \oplus \mathbf{F}_8$ is an $\mathbf{F}_2$-space of dimension 7, the group B is the additive group of all Boolean functions on V, and V acts on B by translation; the generator of A acts on V as multiplication by a scalar of order 21. Section 2 sets this up in the generality we need and Section 3 explains why V has to look like this.

In this example $C \cong C_2^{12}$ is abelian, so *every* $\chi^* \in \mathrm{Irr}(C)$ is linear. The criterion in the second sentence of Problem 21.100 therefore predicts that no invariant character vanishes anywhere on C, and it fails as badly as it can. That criterion is also posed on its own by Navarro as Problem 6.3 of [12]:

Problem 6.3. Suppose that A acts coprimely on G, let $\mathrm{Irr}_A(G)$ be the set of A-invariant irreducible characters of G, let $C = C_G(A)$, and let ${}^*\colon \mathrm{Irr}_A(G) \to \mathrm{Irr}(C)$ be the Glauberman–Isaacs correspondence. Let $\chi \in \mathrm{Irr}_A(G)$. Is it true that $\chi^*(1) = 1$ if and only if χ_C is never zero?

Corollary B. *Problem 6.3 has a negative answer. For the action of Theorem A there are* 2368 *characters $\chi \in \mathrm{Irr}_A(G)$ with $\chi^*(1) = 1$ for which χ_C nevertheless has a zero.*

Navarro writes of Problem 6.3 that he does "not even know how to prove the case where G is nilpotent, and this should be territory for counterexamples" [12, p. 189]. Our G is a 2-group, so the counterexample lies in exactly that territory. Section 9 passes to $\Gamma = G \rtimes A$ and settles the Carter subgroup analogue as well, and Section 10 records precisely which of the surrounding problems of [12] the example does and does not settle.

Corollary C. *Let $\Gamma = G \rtimes A$ for the action of Theorem A. Then Γ is solvable of order $2^{135} \cdot 21$, the subgroup $K = C_G(A) \times A$ is a Carter subgroup of Γ, and exactly* 36288 *irreducible characters of Γ do not vanish on K, while $|K/K'| = 86016$. Consequently Problem 6.7 of [12] has a negative answer, and the head characters of Γ in the sense of [8] are not its Carter-nonvanishing characters.*

Nor is the failure a near miss: passing to direct powers drives the ratio to zero.

Corollary D. *For every $\varepsilon > 0$ there is a coprime action of a finite group A on a finite group G with $C = C_G(A)$ abelian and*

$$\frac{|N_A(G)|}{|C/C'|} < \varepsilon.$$

Strategy of the proof

To prove Theorem A we isolate the counterexample, which is short, in Section 4, where every step can be checked by hand. Three facts do all the work, for A of odd order acting without nonzero fixed points on V and $G = B \rtimes V$ as above.

First, $C = C_G(A) = B^A$ is elementary abelian of rank the number of A-orbits on V (Proposition 2.2); in particular $C' = 1$ and $|C/C'| = |B^A|$. Second, the little-groups method identifies $\mathrm{Irr}_A(G)$ with B^A (Proposition 2.5), so that $|\mathrm{Irr}_A(G)| = |C/C'|$ *exactly*; hence a single invariant character with a zero on C already refutes Problem 21.100. Third, if $u = \delta_0 \in B^A$ is the indicator of $0 \in V$, the associated $\chi_u \in \mathrm{Irr}_A(G)$ has degree $|V|$ and satisfies $\chi_u(c) = |V| - 2|\operatorname{supp} c|$ for $c \in B^A$ (Lemma 2.10), so χ_u vanishes as soon as V has an A-stable subset of size $|V|/2$.

Everything therefore reduces to an arithmetic question about the multiset of A-orbit sizes on V: does some sub-multiset sum to $|V|/2$? Section 3 answers it completely in small dimension. No group of prime power order admits such a V (Proposition 3.2); no group of odd order at all, of any structure, admits one of dimension less than 7 (Theorem 3.5); and the smallest admissible cyclic pair is $|A| = 21$ with $\dim V = 7$, where the orbit sizes are forced to be

$$1, 3, 3, 3, 3, 3, 7, 21, 21, 21, 21, 21 \qquad \text{and} \qquad 1 + 21 + 21 + 21 = 64 = \tfrac{1}{2}|V|$$

(Proposition 3.3). That identity is the whole example.

Sections 5–7 then refine the inequality $|N_A(G)| < 4096$ to the exact value 1728. This part is longer: we coordinatize B^A by pairs of "radial" six-bit vectors, compute the relevant correlation explicitly (Lemma 5.2), and convert vanishing into two affine conditions over $\mathbf{F}_2$ (Proposition 6.4). A reader who wants only the counterexample may stop at Section 4. Section 8 proves Corollaries B and D and records what we do not know; Section 9 proves Corollary C; Section 10 delimits the scope of the refutation among the problems of [12]; and Section 11 describes machine checks, which are independent of the proofs.

Notation

Groups are finite and characters are complex. We write C_n for the cyclic group of order n, $\mathrm{Irr}(G)$ for the irreducible characters, G' for the derived subgroup, and Ind_H^G for induction. For an A-set S we write S^A for the fixed points. Vectors over $\mathbf{F}_2$ are added coordinatewise, $\mathrm{wt}(\cdot)$ is Hamming weight, $\mathrm{supp}(\cdot)$ is support, and $\mathbf{1}$ denotes an all-ones vector whose length is clear from context.

2 A family of constructions

Throughout this section A is a finite group of odd order, and V is a finite $\mathbf{F}_2$-vector space on which A acts $\mathbf{F}_2$-linearly. We assume throughout that the action is fixed-point-free,

$$C_V(A) = 0. \tag{1}$$

Since $|A|$ is odd, $|A| = 1$ in $\mathbf{F}_2$, so $\mathbf{F}_2[A]$ is semisimple by Maschke's theorem; we use this twice below. For $a \in A$ we write $a \cdot v$ for the action on V. Let

$$B = \{f : V \to \mathbf{F}_2\}$$

be the additive group of Boolean functions on V, so $B \cong C_2^{|V|}$. For $t \in V$ let $\tau_t \in \mathrm{Aut}(B)$ be translation,

$$(\tau_t f)(x) = f(x + t),$$

and form the semidirect product

$$G = B \rtimes V, \qquad (f,t)(g,s) = (f + \tau_t g,\, t+s),$$

of order $2^{|V|} \cdot |V|$. Since $|A|$ is odd, A acts coprimely on G once we check that it acts at all:

Lemma 2.1. *For $a \in A$ the formula $a \cdot (f,t) = (f \circ a^{-1}, a \cdot t)$ defines an action of A on G by automorphisms, restricting to the given action on V. It is faithful if the action on V is.*

Proof. For $g \in B$ and $x \in V$ we have

$$\big((\tau_t g) \circ a^{-1}\big)(x) = g(a^{-1}x + t) = \big(\tau_{a\cdot t}(g \circ a^{-1})\big)(x),$$

so $(\tau_t g) \circ a^{-1} = \tau_{a\cdot t}(g \circ a^{-1})$. Hence

$$a \cdot \big((f,t)(g,s)\big) = \big((f + \tau_t g) \circ a^{-1}, a \cdot (t+s)\big) = \big(a \cdot (f,t)\big)\big(a \cdot (g,s)\big).$$

The map is bijective with inverse given by a^{-1}, and its restriction to $\{0\} \times V$ is the given action. $\square$

Proposition 2.2. *Let k be the number of A-orbits on V. Then*

$$C = C_G(A) = B^A \cong C_2^k,$$

so C is elementary abelian, $C' = 1$, and $|C/C'| = 2^k$.

Proof. If (f,t) is fixed by every $a \in A$ then $a \cdot t = t$ for all a, so $t = 0$ by (1); thus $C_G(A) = B^A$. A function $f \in B$ satisfies $f \circ a^{-1} = f$ for all a exactly when it is constant on each A-orbit of V, and the k orbit indicators form an $\mathbf{F}_2$-basis of B^A. Being elementary abelian, C has $C' = 1$. $\square$

2.1 The irreducible characters of G

For $u, f \in B$ put

$$\langle u, f\rangle = \sum_{x \in V} u(x)f(x) \in \mathbf{F}_2, \qquad \lambda_u(f) = (-1)^{\langle u,f\rangle}.$$

The pairing is nondegenerate, so $u \mapsto \lambda_u$ is an isomorphism $B \to \mathrm{Irr}(B)$. Conjugation by $(0,t)$ sends $(f,0)$ to $(\tau_t f, 0)$, and since $\langle u, \tau_t f\rangle = \langle \tau_t u, f\rangle$ we get $\lambda_u^{(0,t)} = \lambda_{\tau_t u}$. Thus V permutes $\mathrm{Irr}(B)$ the same way it permutes B, and the stabilizer of λ_u is $B \rtimes V_u$ where

$$V_u = \{t \in V : \tau_t u = u\}.$$

Write $I_u = B \rtimes V_u$; it is normal in G, being the preimage of $V_u \le V$ under $G \to G/B \cong V$. For $\mu \in \mathrm{Irr}(V_u)$ the formula

$$\theta_{u,\mu}(f,t) = \lambda_u(f)\mu(t)$$

defines a linear character of I_u, because $\tau_t u = u$ for $t \in V_u$. Put $\chi_{u,\mu} = \mathrm{Ind}_{I_u}^G \theta_{u,\mu}$.

Proposition 2.3. *Choose one u from each V-orbit of B. Then*

$$\mathrm{Irr}(G) = \{\chi_{u,\mu} : u \text{ a chosen representative},\ \mu \in \mathrm{Irr}(V_u)\},$$

these characters are pairwise distinct, and $\chi_{u,\mu}$ has degree $[V : V_u]$.

Proof. If $g = (g_0, s) \notin I_u$ then $s \notin V_u$, so $\theta^g_{u,\mu}$ and $\theta_{u,\nu}$ restrict to the distinct characters $\lambda_{\tau_s u} \neq \lambda_u$ of B. Since $I_u \trianglelefteq G$, Mackey's formula reads

$$\langle \chi_{u,\mu}, \chi_{u,\nu} \rangle_G = \sum_{gI_u \in G/I_u} \langle \theta_{u,\mu}, \theta^g_{u,\nu} \rangle_{I_u},$$

and by the previous sentence only the identity coset contributes. It contributes 1 if $\mu = \nu$ and 0 otherwise. So each $\chi_{u,\mu}$ is irreducible, and for fixed u distinct μ give distinct characters. Representatives from different V-orbits give characters with disjoint sets of B-constituents, hence distinct characters.

For the orbit $\mathcal{O} = V \cdot u$ there are $|V_u|$ choices of μ, each of degree $[V : V_u]$, contributing

$$|V_u| \, [V : V_u]^2 = |V| \, |\mathcal{O}|$$

to the sum of squared degrees. Summing over the orbits of V on B gives $|V| \, |B| = |G|$, so the list is complete. ☐

Lemma 2.4. *Every A-stable V-orbit in B contains exactly one element of B^A.*

Proof. Let the orbit of u be A-stable, so for each $a \in A$ there is $z_a \in V$, determined modulo V_u, with $a \cdot u = \tau_{z_a} u$.

First, V_u is A-invariant. If $t \in V_u$ then $\tau_t u = u$, so by Lemma 2.1

$$\tau_{z_a} u = a \cdot u = a \cdot (\tau_t u) = \tau_{a \cdot t}(a \cdot u) = \tau_{a\cdot t + z_a} u,$$

hence $\tau_{a \cdot t} u = u$ and $a \cdot t \in V_u$. Thus V/V_u is an $\mathbf{F}_2[A]$-module, and $(V/V_u)^A = 0$: by semisimplicity V_u has an A-invariant complement X, so $V/V_u \cong X$ and $X^A \subseteq V^A = 0$.

Next, the map $a \mapsto z_a + V_u$ is a 1-cocycle: applying Lemma 2.1 twice, $\tau_{z_{ab}} u = (ab) \cdot u = a \cdot (\tau_{z_b} u) = \tau_{a \cdot z_b + z_a} u$, so $z_{ab} \equiv a \cdot z_b + z_a \pmod{V_u}$. Put

$$w = \sum_{b \in A} z_b.$$

Summing the cocycle identity over $b \in A$ and reindexing the left side gives $w \equiv a \cdot w + |A| z_a \pmod{V_u}$, and $|A| = 1$ in $\mathbf{F}_2$ because $|A|$ is odd, so

$$z_a \equiv a \cdot w + w \pmod{V_u} \qquad \text{for every } a \in A.$$

Therefore $a \cdot w + z_a \equiv w \pmod{V_u}$, and

$$a \cdot (\tau_w u) = \tau_{a \cdot w}(a \cdot u) = \tau_{a \cdot w + z_a} u = \tau_w u$$

for every a, so $\tau_w u \in B^A$. Finally, if u and $\tau_t u$ both lie in B^A then $t + V_u \in (V/V_u)^A = 0$, so $t \in V_u$ and $\tau_t u = u$. ☐

Proposition 2.5. *For $u \in B^A$ let $\widetilde{\lambda}_u(f, t) = \lambda_u(f)$ and*

$$\chi_u = \operatorname{Ind}^G_{I_u} \widetilde{\lambda}_u.$$

Then $u \mapsto \chi_u$ is a bijection from B^A onto $\operatorname{Irr}_A(G)$. In particular

$$|\operatorname{Irr}_A(G)| = |B^A| = |C/C'|.$$

Proof. By Proposition 2.3 an A-invariant irreducible character comes from an A-stable V-orbit in B, and by Lemma 2.4 that orbit has a unique representative $u \in B^A$; different orbits give different characters. So it suffices to fix $u \in B^A$ and determine which μ give invariant characters.

For such u the subgroup V_u is A-invariant, since $\tau_t u = u$ implies $\tau_{a\cdot t} u = \tau_{a\cdot t}(a \cdot u) = a \cdot (\tau_t u) = u$. The parameterization of Proposition 2.3 is A-equivariant, $\chi_{u,\mu}^a = \chi_{u,\mu^a}$, and injective, so $\chi_{u,\mu}$ is A-invariant if and only if $\mu^a = \mu$ for all a. Write $\mu(t) = (-1)^{\ell(t)}$ for an $\mathbf{F}_2$-linear functional ℓ on V_u; invariance says ℓ is A-invariant, that is, $\ell \in (V_u^*)^A$. Now $V_u^A \subseteq V^A = 0$, so by semisimplicity V_u has no trivial submodule, hence no trivial quotient, hence $(V_u^*)^A = 0$. Thus $\ell = 0$ and μ is trivial, giving $\theta_{u,\mu} = \widetilde{\lambda}_u$. The final count is Proposition 2.2. □

Remark 2.6. When A is solvable, $|\operatorname{Irr}_A(G)| = |\operatorname{Irr}(C)|$ by the Glauberman correspondence [4], and indeed C is abelian of order $|B^A|$. Proposition 2.5 recovers this independently. What matters below is the sharper statement $|\operatorname{Irr}_A(G)| = |C/C'|$: the count in Problem 21.100 is the *total* number of invariant characters here, so any single zero on C refutes it.

2.2 Character values on C

Lemma 2.7. *For $u, c \in B^A$,*

$$\chi_u(c) = \sum_{t \in V/V_u} (-1)^{\langle \tau_t u, c\rangle}, \qquad \textit{equivalently} \qquad |V_u|\,\chi_u(c) = \sum_{t\in V} (-1)^{\langle \tau_t u, c\rangle}.$$

Proof. As $I_u \trianglelefteq G$ and $c \in B \subseteq I_u$, the induced character formula gives

$$\chi_u(c) = \sum_x \widetilde{\lambda}_u\big(x^{-1}(c,0)x\big),$$

the sum over representatives x of G/I_u; take $x = (0,t)$ for $t \in V/V_u$. Conjugation gives $(0,t)^{-1}(c,0)(0,t) = (\tau_t c, 0)$, and $\langle u, \tau_t c\rangle = \langle \tau_t u, c\rangle$. The summand is constant on cosets of V_u, whence the second form. □

The next lemma is the reason the whole problem collapses to arithmetic of orbit sizes.

Lemma 2.8. *For $u, c \in B^A$ the function $t \mapsto \langle \tau_t u, c\rangle$ is constant on A-orbits of V. Consequently, if $n_1, \ldots, n_k$ are the sizes of the A-orbits on V, there are signs $\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}$ with*

$$|V_u|\,\chi_u(c) = \sum_{j=1}^{k} \varepsilon_j n_j. \tag{2}$$

Proof. The pairing is A-invariant: $\langle a \cdot f, a \cdot g\rangle = \sum_x f(a^{-1}x) g(a^{-1}x) = \langle f, g\rangle$. For $u \in B^A$, Lemma 2.1 gives $a \cdot (\tau_t u) = \tau_{a\cdot t}(a \cdot u) = \tau_{a\cdot t} u$, so

$$\langle \tau_{a\cdot t} u, c\rangle = \langle a \cdot (\tau_t u), a \cdot c\rangle = \langle \tau_t u, c\rangle.$$

Thus the exponent is constant on A-orbits, and grouping the sum of Lemma 2.7 by orbits gives (2) with ε_j the common value of $(-1)^{\langle \tau_t u, c\rangle}$ on the jth orbit. □

Corollary 2.9 (Balance condition)**.** *If some $\chi \in \operatorname{Irr}_A(G)$ vanishes at some element of C, then some sub-multiset of $\{n_1, \ldots, n_k\}$ sums to $|V|/2$.*

Proof. By (2) a zero forces $\sum_{j\in S} n_j = \sum_{j \notin S} n_j$ for $S = \{j : \varepsilon_j = -1\}$, and the two sides add to $\sum_j n_j = |V|$. □

Conversely, one distinguished character makes the balance condition sufficient.

Lemma 2.10. *Let $u = \delta_0 \in B^A$ be the indicator function of $0 \in V$. Then $V_u = 0$, so $\chi_u = \operatorname{Ind}_B^G \lambda_u \in \operatorname{Irr}_A(G)$ has degree $|V|$, and for every $c \in B^A$*

$$\chi_u(c) = |V| - 2\,|\operatorname{supp} c|.$$

Hence $\chi_u(c) = 0$ if and only if $|\operatorname{supp} c| = |V|/2$.

Proof. The set $\{0\}$ is an A-orbit, so $\delta_0 \in B^A$, and $\tau_t\delta_0 = \delta_0$ forces $t = 0$. For $c \in B^A$,

$$\langle \tau_t\delta_0, c\rangle = \sum_{x \in V} \delta_0(x+t)c(x) = c(t),$$

so Lemma 2.7 gives $\chi_u(c) = \sum_{t\in V}(-1)^{c(t)} = |V| - 2|\operatorname{supp} c|$. $\square$

Nothing so far uses any particular V, so we may already record the general counterexample. Call the pair (A, V) *balanced* if V has an A-stable subset of size $|V|/2$; by Corollary 2.9 this is equivalent to some sub-multiset of the A-orbit sizes on V summing to $|V|/2$.

Theorem 2.11. *Let A be any finite group of odd order acting fixed-point-freely on a finite $\mathbf{F}_2$-space V, and let $G = B \rtimes V$ with $B = \{f : V \to \mathbf{F}_2\}$. If (A, V) is balanced, then $C = C_G(A)$ is elementary abelian,*

$$|\operatorname{Irr}_A(G)| = |C/C'|, \qquad \text{and} \qquad |N_A(G)| < |C/C'|.$$

In particular Problem 21.100 and Problem 6.3 both have negative answers for the coprime action of A on G.

Proof. Propositions 2.2 and 2.5 give $C = B^A$ elementary abelian with $|\operatorname{Irr}_A(G)| = |B^A| = |C/C'|$. Let $S \subseteq V$ be A-stable with $|S| = |V|/2$ and let $c \in B^A$ be its indicator function. By Lemma 2.10 the character $\chi_{\delta_0} \in \operatorname{Irr}_A(G)$ satisfies $\chi_{\delta_0}(c) = 0$, so $N_A(G)$ is a proper subset of $\operatorname{Irr}_A(G)$. Since C is abelian every Glauberman–Isaacs correspondent is linear, so χ_{δ_0} has linear correspondent and a zero on C, so the criterion of Problem 6.3 fails as well. $\square$

Balanced pairs are abundant, and each one yields a counterexample.

Proposition 2.12. *If (A, V) is balanced and V' is any $\mathbf{F}_2[A]$-module with $C_{V'}(A) = 0$, then $(A, V \oplus V')$ is balanced. Consequently, for each A admitting one balanced module there are balanced pairs (A, V) with $\dim V$ arbitrarily large, and hence infinitely many groups G as in Theorem 2.11.*

Proof. Let $S \subseteq V$ be A-stable with $|S| = |V|/2$. Then $S \oplus V' \subseteq V \oplus V'$ is A-stable of size $|S|\,|V'| = |V \oplus V'|/2$. Taking V' to be a direct sum of r copies of any fixed-point-free module gives arbitrarily large $\dim V$. $\square$

3 Choosing V: the design constraint

By Corollary 2.9 and Lemma 2.10, the construction of Section 2 produces a counterexample to Problem 21.100 if and only if V has an A-stable subset of size $|V|/2$, that is, if and only if

$$\text{some sub-multiset of the } A\text{-orbit sizes on } V \text{ sums to } \tfrac{1}{2}|V|. \tag{3}$$

This section determines the smallest (A, V) satisfying (3). Two features of the problem make the search finite and elementary. First, orbit sizes are determined by the $\mathbf{F}_2[A]$-module structure of

V, so nothing of size $2^{|V|}$ is ever involved. Second, (3) is a subset-sum condition on at most $|V|$ integers.

Recall that for A cyclic of odd order m, every $\mathbf{F}_2[A]$-module is a direct sum of irreducibles, and the irreducible $\mathbf{F}_2[A]$-modules are indexed by the divisors $d \mid m$: the module attached to d has $\mathbf{F}_2$-dimension $\mathrm{ord}_d(2)$ and the generator acts on it with order d. Condition (1) says that no summand has $d = 1$, and faithfulness says the d's have least common multiple m.

Lemma 3.1. *Let $V = M_1 \oplus \cdots \oplus M_r$, where the generator acts on M_j with order $d_j > 1$ and $\dim_{\mathbf{F}_2} M_j = \mathrm{ord}_{d_j}(2)$. For $v = (v_1, \ldots, v_r) \in V$ the A-orbit of v has size $\mathrm{lcm}\{d_j : v_j \neq 0\}$, interpreted as 1 when $v = 0$.*

Proof. Identify M_j with $\mathbf{F}_{2^{\dim M_j}}$ so that a fixed generator a of A acts on it as multiplication by a field element θ_j of order d_j. Then $a^i \cdot v = v$ if and only if $\theta_j^i v_j = v_j$ for all j, that is, $d_j \mid i$ whenever $v_j \neq 0$. The stabilizer of v in $A \cong C_m$ is therefore of index $\mathrm{lcm}\{d_j : v_j \neq 0\}$. □

The first restriction needs no hypothesis on A beyond odd order, and in particular rules out the smallest operator groups outright.

Proposition 3.2. *Let A be any finite p-group of odd order acting on $V = \mathbf{F}_2^n$ with $C_V(A) = 0$. Then (A, V) is not balanced. In particular no construction of Section 2 whose operator group has prime power order gives a counterexample.*

Proof. Every A-orbit on V has size a power of p, and by $C_V(A) = 0$ the only orbit of size 1 is $\{0\}$. Counting V by orbits gives $2^n \equiv 1 \pmod{p}$, so if $d = \mathrm{ord}_p(2)$ then $d \mid n$. A sub-multiset of the orbit sizes summing to 2^{n-1} has the form

$$2^{n-1} = \alpha + (\text{a multiple of } p), \qquad \alpha \in \{0, 1\},$$

according as it uses the orbit $\{0\}$ or not. As p is odd, $p \nmid 2^{n-1}$, so $\alpha = 1$ and $2^{n-1} \equiv 1 \pmod{p}$, giving $d \mid n - 1$. With $d \mid n$ this forces $d = 1$, that is $p \mid 1$, a contradiction. □

So the operator group must have at least two prime divisors, and its module must mix at least two different element orders. The smallest possibility is the one we use.

Proposition 3.3. *Among all pairs (A, V) with A* cyclic *of odd order acting faithfully on $V = \mathbf{F}_2^n$ with $C_V(A) = 0$, condition (3) first occurs at $n = 7$, and there it occurs only for $|A| = 21$ and*

$$V \cong \mathbf{F}_4 \oplus \mathbf{F}_4 \oplus \mathbf{F}_8 = \mathbf{F}_4^2 \oplus \mathbf{F}_8,$$

with the generator acting on the summands with orders $3, 3, 7$. The A-orbit sizes on V are then

$$1,\ 3, 3, 3, 3, 3,\ 7,\ 21, 21, 21, 21, 21,$$

and the sub-multisets summing to 64 are exactly the 20 of the forms

$$1 + 21 + 21 + 21 \qquad \textit{and} \qquad 3 + 3 + 3 + 3 + 3 + 7 + 21 + 21.$$

Proof. Write $V = \bigoplus_j M_j$ as in Lemma 3.1, with element orders $d_j > 1$ and $\mathrm{lcm}_j\, d_j = m = |A|$; then $n = \sum_j \mathrm{ord}_{d_j}(2)$. Since $\mathrm{ord}_d(2) \geq 2$ for $d > 1$, we have $r \leq n/2$ summands, and each d_j divides m; so for each n there are finitely many possibilities, and the orbit sizes depend only on the multiset $\{d_j\}$.

To enumerate the candidates, note that $\mathrm{ord}_d(2) = e$ means $d \mid 2^e - 1$ but $d \nmid 2^f - 1$ for $f < e$. For $e \leq 7$ this gives

e	1	2	3	4	5	6	7
d	1	3	7	$5, 15$	31	$9, 21, 63$	127

The value $e = 1$, i.e. $d = 1$, is excluded by $C_V(A) = 0$. So each candidate corresponds to a partition of n into parts from $\{2, \ldots, 7\}$ together with a choice of d for each part, and there are finitely many for each n. Discarding those whose m is a prime power by Proposition 3.2, the complete list for $n \leq 7$ is the following, where $x^{(i)}$ means the size x repeated i times and the target is 2^{n-1}.

n	m	$\{d_j\}$	Orbit sizes	Why the target is missed
4	15	$\{15\}$	$1, 15$	parts ≤ 8 total $1 < 8$
5	21	$\{3, 7\}$	$1, 3, 7, 21$	parts ≤ 16 total $11 < 16$
6	15	$\{3, 5\}$	$1, 3, 5^{(3)}, 15^{(3)}$	sums are $\equiv 0, 1, 3, 4 \pmod 5$; $32 \equiv 2$
6	15	$\{3, 15\}$	$1, 3, 15^{(4)}$	sums are $\equiv 0, 1 \pmod 3$; $32 \equiv 2$
6	21	$\{21\}$	$1, 21^{(3)}$	sums are $0, 1, 21, 22, 42, 43, 63, 64$
6	63	$\{63\}$	$1, 63$	parts ≤ 32 total $1 < 32$
7	21	$\{3, 3, 7\}$	$1, 3^{(5)}, 7, 21^{(5)}$	$1 + 21 + 21 + 21 = 64$
7	35	$\{5, 7\}$	$1, 5^{(3)}, 7, 35^{(3)}$	at most one 35; rest total $23 < 29$
7	93	$\{3, 31\}$	$1, 3, 31, 93$	parts ≤ 64 total $35 < 64$
7	105	$\{7, 15\}$	$1, 7, 15, 105$	parts ≤ 64 total $23 < 64$

Each entry of the last column is a complete argument, of one of three kinds. Five rows are settled by a size count: a part exceeding the target cannot be used, and the parts that remain total less than the target. The row $m = 35$ is a variant: two parts 35 already exceed the target 64, so at most one is used, and the other parts total $1 + 5 + 5 + 5 + 7 = 23 < 29$. Two rows are settled by a congruence: modulo the stated modulus every part vanishes except 1, and also except 3 in the row $\{3, 5\}$, so every attainable sum lies in the listed set of residues, which omits that of the target. Each part 3 is itself divisible by 3, which is why the row $\{3, 15\}$ admits only the residues 0 and 1. The remaining row, $m = 21$ with $n = 6$, is settled by listing the eight sums $\alpha + 21\beta$ with $\alpha \in \{0, 1\}$ and $\beta \leq 3$, which omit 32.

Only the row $n = 7$, $m = 21$, $\{d_j\} = \{3, 3, 7\}$ survives, and there $V \cong \mathbf{F}_4 \oplus \mathbf{F}_4 \oplus \mathbf{F}_8$. By Lemma 3.1 the orbit sizes are lcm of the orders on the nonzero coordinates: size 1 for $v = 0$; size 3 for the 15 vectors supported on $\mathbf{F}_4 \oplus \mathbf{F}_4$, giving 5 orbits; size 7 for the 7 vectors supported on $\mathbf{F}_8$, giving 1 orbit; and size 21 for the $15 \cdot 7 = 105$ vectors with both parts nonzero, giving 5 orbits. This is the stated multiset, of total 128.

Finally we enumerate the sub-multisets summing to 64. Let κ be the number of 21's used; the remaining parts come from $\{1, 3, 3, 3, 3, 3, 7\}$ and sum to at most $1+15+7 = 23$. Thus $64 - 21\kappa \leq 23$, so $\kappa \geq 2$, and $21\kappa \leq 64$ gives $\kappa \leq 3$. If $\kappa = 3$ we need 1 more, so we take the part 1: this gives $\binom{5}{3} = 10$ sub-multisets. If $\kappa = 2$ we need 22 from $\{1, 3, 3, 3, 3, 3, 7\}$; since $22 \equiv 1 \pmod 3$ and the only parts not divisible by 3 are 1 and 7, we must use exactly one of them, and $22 - 1 = 21$ is not a sum of at most five 3's while $22 - 7 = 15$ is (all five), so the unique choice is $3 + 3 + 3 + 3 + 3 + 7$. This gives $\binom{5}{2} = 10$ sub-multisets. In total 20. $\square$

Proposition 3.3 assumes A cyclic, because its enumeration is over cyclic modules. In fact the assumption can be removed entirely: no operator group of odd order, of any structure, admits a balanced module of dimension less than 7. The key is that every simple summand of V carries a scalar subgroup whose order divides all the relevant orbit sizes.

Lemma 3.4. *Let $A \neq 1$ be a finite group of odd order acting faithfully and irreducibly on $V = \mathbf{F}_2^d$ with $2 \leq d \leq 7$. Then there is an odd integer $d_A \geq 3$ that divides the size of every A-orbit on $V \setminus \{0\}$, and:*

(i) *either there are a normal subgroup $Z \leq A$ and a divisor $e > 1$ of d with $\mathbf{F}_2[Z] \cong \mathbf{F}_{2^e}$, such that V is an $\mathbf{F}_{2^e}$-vector space of dimension d/e on which Z acts by scalar multiplication; in this case $d_A = |Z|$ satisfies $\operatorname{ord}_{d_A}(2) = e$, so that*

e	2	3	4	5	6	7
d_A	3	7	$5, 15$	31	$9, 21, 63$	127

(ii) *or $d = 6$ and A is a 3-group; in this case $d_A = 3$.*

Proof. By the Feit–Thompson theorem [2] A is solvable, so it has a nontrivial abelian normal subgroup; let Z be one maximal among these. By Clifford's theorem [1] V is a direct sum of k Z-isotypic components, which A permutes transitively; they have equal dimension d/k, and k divides $|A|$, so k is odd. A component of dimension 1 is impossible: on it Z would act through $\mathbf{F}_2^\times = 1$, and as the components are permuted transitively by A and Z is normal, Z would act trivially on every component, contradicting faithfulness. Hence $k \mid d$, k odd, $d/k \geq 2$, which for $d \leq 7$ leaves $k = 1$, or $k = 3$ with $d = 6$.

Suppose $k = 1$, so $V \cong W^m$ is Z-homogeneous with W a simple $\mathbf{F}_2[Z]$-module on which Z acts faithfully. Then $\mathbf{F}_2[Z]$ acts on W as a field $\mathbf{F}_{2^e}$ with $\dim_{\mathbf{F}_2} W = e$, generated by the image of Z; thus Z is cyclic of order $d_A := |Z|$ with $\operatorname{ord}_{d_A}(2) = e$, and $e > 1$ since $e = 1$ forces $Z = 1$. The homogeneous structure makes V an $\mathbf{F}_{2^e}$-space of dimension $m = d/e$ on which Z acts by scalars. A nonzero scalar $\zeta \neq 1$ fixes only 0, so every Z-orbit on $V \setminus \{0\}$ has size exactly d_A; as $Z \leq A$, every A-orbit on $V \setminus \{0\}$ is a union of such orbits and d_A divides its size. The table lists, for each $e \leq 7$, the $d_A > 1$ with $d_A \mid 2^e - 1$ and $\operatorname{ord}_{d_A}(2) = e$.

Suppose $k = 3$ and $d = 6$, so the components have dimension 2. The stabilizer of a component acts on it through an odd-order subgroup of $GL(2,2) \cong S_3$, hence through a group of order dividing 3, and the permutation action of A on the three components has odd image in S_3, again of order dividing 3. Thus A embeds in $C_3 \wr C_3$ and is a 3-group. Every A-orbit size is then a power of 3, and an orbit of size 1 outside 0 would be a nonzero fixed vector; but $C_V(A)$ is a proper submodule of the simple nontrivial module V, hence 0. So 3 divides every nonzero orbit size. □

Theorem 3.5. *Let A be any finite group of odd order acting on $V = \mathbf{F}_2^n$ with $C_V(A) = 0$ and $n \leq 6$. Then (A, V) is not balanced. Consequently $\dim V = 7$ is the least dimension in which the construction of Section 2 produces a counterexample, over all operator groups of odd order.*

Proof. By Maschke's theorem $V = \bigoplus_{i=1}^r V_i$ with each V_i simple, and no V_i is trivial since $C_V(A) = 0$; so $n_i := \dim V_i \geq 2$ and the image A_i of A on V_i satisfies the hypotheses of Lemma 3.4. Let $d_i := d_{A_i}$ be the resulting divisors.

Each A-orbit $\mathcal{O}$ on V has a well-defined support $S = \{i : v_i \neq 0\}$, since A preserves each V_i. For $i \in S$ the projection $\mathcal{O} \to A \cdot v_i$ is surjective and A-equivariant, so $|A \cdot v_i|$ divides $|\mathcal{O}|$, and Lemma 3.4 gives $d_i \mid |A \cdot v_i|$. Hence $|\mathcal{O}|$ is divisible by $D_S := \operatorname{lcm}\{d_i : i \in S\}$. Moreover the orbits of support S partition a set of $\prod_{i \in S}(2^{n_i} - 1)$ vectors. If (A, V) is balanced, there are therefore $\alpha \in \{0, 1\}$ and integers $y_S \geq 0$ with

$$2^{n-1} = \alpha + \sum_{\emptyset \neq S} y_S, \qquad D_S \mid y_S, \qquad y_S \leq \prod_{i \in S}(2^{n_i} - 1). \tag{4}$$

We check that (4) is unsolvable for every partition $(n_1, \dots, n_r)$ of $n \le 6$ into parts ≥ 2 and every choice of the d_i from Lemma 3.4. Two observations dispose of most cases. First, if 3 divides every d_i, then $2^{n-1} \equiv \alpha \pmod 3$ with $\alpha \in \{0, 1\}$, which fails whenever n is even, since then $2^{n-1} \equiv 2 \pmod 3$. As $3 \mid d_i$ for every admissible d_i except $d_i \in \{5, 7, 31, 127\}$, this kills all of $n = 2$ and, for $n \in \{4, 6\}$, every case except those involving a part with $d_i \in \{5, 7, 31\}$. Second, if 7 divides every d_i — the partitions (3), (3, 3) and (6) with $d_i = 7$ — then $2^{n-1} \equiv \alpha \pmod 7$, which fails since $2^2 \equiv 4$ and $2^5 \equiv 4 \pmod 7$.

The remaining cases are settled directly. For (4) with $d_1 = 5$: $8 \not\equiv 0, 1 \pmod 5$. For (5) with $d_1 = 31$: $16 \not\equiv 0, 1 \pmod{31}$. For (2, 3) with $(d_1, d_2) = (3, 7)$: here $y_{\{1\}} \in \{0, 3\}$, $y_{\{2\}} \in \{0, 7\}$, and $y_{\{1,2\}} \in \{0, 21\}$; since $21 > 16$ the last is 0, and $\alpha + 3 + 7 < 16$. For (2, 4) with $(d_1, d_2) = (3, 5)$: here $y_{\{1\}} \in \{0, 3\}$, $y_{\{2\}} \in 5\mathbf{Z} \cap [0, 15]$, and $y_{\{1,2\}} \in 15\mathbf{Z} \cap [0, 45]$. Taking (4) modulo the possible values: if $y_{\{1,2\}} = 30$ the remainder 2 is not of the form $\alpha + y_{\{1\}} + y_{\{2\}}$; if $y_{\{1,2\}} = 15$ the remainder 17 is not attainable, the attainable values being $\{0, 1, 3, 4\} + \{0, 5, 10, 15\} \subseteq \{0, \dots, 19\} \setminus \{2, 7, 12, 17\}$; and if $y_{\{1,2\}} = 0$ the total is at most $1 + 3 + 15 < 32$. For (2, 4) with $(d_1, d_2) = (3, 15)$: $y_{\{2\}} \in \{0, 15\}$ and $y_{\{1,2\}} \in 15\mathbf{Z} \cap [0, 45]$, so $32 - \alpha - y_{\{1\}} \in \{28, 29, 31, 32\}$ must be a multiple of 15, which it is not. This exhausts all cases; the final assertion follows because the pair of Proposition 3.3 is balanced in dimension 7, and balanced pairs give counterexamples by Theorem 2.11. □

Corollary 3.6. *Over all operator groups A of odd order: the least dimension of a balanced pair (A, V) is 7; the least order of a group G in the family of Section 2 refuting Problem 21.100 is 2^{135}; and the least order of a balanced operator group is $|A| = 15$, attained at $\dim V = 8$.*

Proof. The first claim is Theorem 3.5 together with Proposition 3.3 and Theorem 2.11, and the second follows since $|G| = 2^{2^n + n}$ is strictly increasing in $n = \dim V$. For the third, a balanced operator group has odd order that is not a prime power by Proposition 3.2, so its order is at least $3 \cdot 5 = 15$. This is attained: let the cyclic group of order 15 act on $V = \mathbf{F}_4 \oplus \mathbf{F}_4 \oplus \mathbf{F}_{16}$ with element orders 3, 3, 5 on the summands. By Lemma 3.1 the orbit sizes are 1, then $3^{(5)}$ (one orbit from each summand $\mathbf{F}_4^\times$ and three among the nine vectors meeting both), $5^{(3)}$, and $15^{(15)}$, of total 256; and

$$15 \cdot 8 + 5 + 3 = 128 = \tfrac{1}{2}|V|,$$

so the pair is balanced. This is the design at $\dim V = 8$ found in Remark 3.7. □

Remark 3.7. Proposition 3.3 was found by exactly this enumeration, which is small enough to carry out by hand and was also checked by machine. Extending the machine enumeration to all cyclic A of odd order $m \le 105$ and all faithful fixed-point-free modules with $\dim V \le 14$ returns 53 admissible designs. The smallest is the one above; the next occurs at $\dim V = 8$ with $|A| = 15$ and element orders $\{3, 3, 5\}$; and none has $|A|$ prime, in agreement with Proposition 3.2. Each admissible design yields a counterexample by the argument of Section 4, so counterexamples of this shape are plentiful, but $\dim V = 7$ is where they start.

4 The counterexample

We can now fix the example and prove the inequality. Let

$$U = \mathbf{F}_4^2, \qquad W = \mathbf{F}_8, \qquad V = U \oplus W,$$

an $\mathbf{F}_2$-space of dimension 7, so $|V| = 128$. Choose $\omega \in \mathbf{F}_4^\times$ of order 3 and $\zeta \in \mathbf{F}_8^\times$ of order 7, and let

$$T(x_1, x_2, y) = (\omega x_1, \omega x_2, \zeta y),$$

an $\mathbf{F}_2$-linear map of order 21. Let $A = \langle a \rangle \cong C_{21}$ act on V with a acting as T. Since $\omega \neq 1$ and $\zeta \neq 1$ we have $C_V(A) = C_V(T) = 0$, so (1) holds, and A acts as in Lemma 2.1 on

$$G = B \rtimes V, \qquad B = \{f : V \to \mathbf{F}_2\}, \qquad |G| = 2^{128} \cdot 2^7 = 2^{135}.$$

The action is faithful and coprime, since $|A| = 21$ is odd and T has order 21.

By Proposition 3.3 the twelve A-orbits on V have sizes $1, 3, 3, 3, 3, 3, 7, 21, 21, 21, 21, 21$. We label them once and for all, as this labeling is used throughout:

Orbit	Size	Coordinate	Description
$\{0\}$	1	x_0	the zero vector
$L_i^\times \times \{0\}$, $1 \leq i \leq 5$	3	x_i	$L_1, \ldots, L_5$ the $\mathbf{F}_4$-lines of U
$\{0\} \times W^\times$	7	y_0	
$L_i^\times \times W^\times$, $1 \leq i \leq 5$	21	y_i	

Here $L_1, \ldots, L_5$ are the five one-dimensional $\mathbf{F}_4$-subspaces of U; each $L_i^\times$ has three elements and is a single $\langle \omega \rangle$-orbit, $W^\times$ is a single $\langle \zeta \rangle$-orbit of size 7, and each $L_i^\times \times W^\times$ is a single $\langle T \rangle$-orbit of size 21 because (ω^i, ζ^i) runs through $C_3 \times C_7$ as i runs modulo 21.

Theorem 4.1. *For this action, $C = C_G(A) \cong C_2^{12}$ is abelian with*

$$|C/C'| = |\operatorname{Irr}_A(G)| = 4096,$$

and there is a $\chi \in \operatorname{Irr}_A(G)$ of degree 128 and a $c \in C$ with $\chi(c) = 0$. Consequently

$$|N_A(G)| \leq 4095 < 4096 = |C/C'|,$$

and the equality of Problem 21.100 fails.

Proof. There are twelve A-orbits on V, so Proposition 2.2 gives $C = B^A \cong C_2^{12}$, abelian, with $|C/C'| = 4096$; and Proposition 2.5 gives $|\operatorname{Irr}_A(G)| = |B^A| = 4096$.

Take $u = \delta_0$, the indicator of $0 \in V$, and let $\chi = \chi_u = \operatorname{Ind}_B^G \lambda_u$, of degree $|V| = 128$ by Lemma 2.10. Let

$$c = \text{indicator of } \{0\} \cup \left(L_1^\times \times W^\times\right) \cup \left(L_2^\times \times W^\times\right) \cup \left(L_3^\times \times W^\times\right).$$

This set is a union of A-orbits, so $c \in B^A = C$, and its size is $1 + 21 + 21 + 21 = 64$. By Lemma 2.10,

$$\chi(c) = |V| - 2|\operatorname{supp} c| = 128 - 128 = 0.$$

Since $N_A(G) \subseteq \operatorname{Irr}_A(G)$ and $\chi \in \operatorname{Irr}_A(G) \setminus N_A(G)$, we get $|N_A(G)| \leq 4095$. □

Theorem 4.1 is the whole counterexample, and every step in it can be checked by hand. The remaining sections determine $|N_A(G)|$ exactly.

5 Radial coordinates

From now on A, V, G are as in Section 4. To compute with B^A we use the labeling in the table above.

Multiplication by ω has six orbits on U, namely $\{0\}$ and $L_1^\times, \dots, L_5^\times$. Call a Boolean function on U *radial* if it is constant on these orbits, and encode such a function as

$$X = (x_0, x_1, \dots, x_5) = (x_0, x) \in \mathbf{F}_2 \oplus \mathbf{F}_2^5,$$

where x_0 is its value at 0 and x_i its value on $L_i^\times$. Write

$$\tau(X) = x_0 + \sum_{i=1}^{5} x_i,$$

which is $\sum_{z \in U} X(z)$ reduced modulo 2, since $|L_i^\times| = 3$ is odd.

Lemma 5.1 (Two slices)**.** *Every $u \in B^A$ is given by a unique pair of radial functions X, Y on U through*

$$u(z,w) = \begin{cases} X(z), & w = 0, \\ Y(z), & w \neq 0. \end{cases}$$

Proof. Invariance means $u \circ T = u$. The slice at $w = 0$ is then radial. For $w \neq 0$, the element T^7 acts as $(\omega^7, \zeta^7) = (\omega, 1)$, so it fixes w and multiplies z by ω; hence the slice at w is radial too. Finally, given $w, w' \neq 0$ choose k with $\zeta^k w = w'$; invariance gives $u(z,w) = u(\omega^k z, w')$, which equals $u(z, w')$ because the slice at w' is radial. So all nonzero slices agree. Uniqueness is clear. $\square$

Thus B^A is identified with $\mathbf{F}_2^6 \times \mathbf{F}_2^6$, and this matches the table of Section 4: X carries the coordinates $x_0, \dots, x_5$ of the orbits inside U, and Y carries $y_0, \dots, y_5$ of the orbits meeting $W^\times$. We write $u = (X, Y)$ and, for the element of C, $c = (E, F)$ with $E = (e_0, e)$ and $F = (f_0, f)$.

For radial X, E define the correlation

$$K_X(E)(s) = \sum_{z \in U} X(z+s) E(z) \in \mathbf{F}_2,$$

again a radial function of s, and $\mathbf{F}_2$-bilinear in (X, E).

Lemma 5.2 (Correlation formula)**.** *With $X = (x_0, x)$, $E = (e_0, e)$, $s_x = \sum_i x_i$, $s_e = \sum_i e_i$,*

$$K_X(E) = \big(x_0 e_0 + x \cdot e, \quad \tau(E)\, x + \tau(X)\, e + (s_x s_e + x \cdot e)\mathbf{1}\big). \tag{5}$$

Proof. At $s = 0$ we get $K_X(E)(0) = x_0 e_0 + \sum_{i=1}^5 3 x_i e_i = x_0 e_0 + x \cdot e$.

Now fix $s \in L_i^\times$ and split the sum over the six $\langle \omega \rangle$-orbits of z. The term $z = 0$ contributes $X(s)E(0) = x_i e_0$. For $z \in L_i^\times$ we have $E(z) = e_i$, and as z runs over the three elements of $L_i^\times$ the value $z + s$ is once 0 and twice in $L_i^\times$; so the contribution is $e_i(x_0 + 2x_i) = x_0 e_i$.

For $j \neq i$ and $z \in L_j^\times$ we have $E(z) = e_j$, and the three elements of $s + L_j^\times$ lie one on each of the three lines other than L_i and L_j. Indeed none of them is 0 or lies on L_i or L_j, since $s \notin L_j$ and $z \notin L_i$; and if $s + z$ and $s + z'$ lay on a common line L_k then $z + z' \in L_j^\times \cap L_k = 0$, a contradiction. Hence $L_j^\times$ contributes $e_j \sum_{k \neq i,j} x_k$, and altogether

$$K_X(E)_i = x_i e_0 + x_0 e_i + \sum_{j \neq i} e_j \sum_{k \neq i,j} x_k.$$

Since $\sum_{k \neq i,j} x_k = s_x + x_i + x_j$, the last sum equals

$$(s_x + x_i)(s_e + e_i) + \big(x \cdot e + x_i e_i\big) = s_x s_e + s_x e_i + x_i s_e + x \cdot e,$$

using $2x_ie_i = 0$. Therefore

$$K_X(E)_i = x_i(e_0 + s_e) + e_i(x_0 + s_x) + (s_x s_e + x \cdot e) = \tau(E)x_i + \tau(X)e_i + (s_x s_e + x \cdot e),$$

which is the ith coordinate in (5). □

Now let $u = (X, Y)$ and $c = (E, F)$, and for $t = (s, v) \in U \oplus W$ put $h_{u,c}(t) = \langle \tau_t u, c\rangle$. By Lemma 2.8 this depends only on the A-orbit of t, so two radial functions of s determine it. Write $H_0(s) = h_{u,c}(s, 0)$ and $H_1(s) = h_{u,c}(s, v)$ for any $v \neq 0$; then

$$H_0 = K_X(E) + K_Y(F), \tag{6}$$
$$H_1 = K_Y(E) + K_X(F). \tag{7}$$

Indeed, summing $u(z + s, w + v)c(z, w)$ over (z, w) and splitting on w: for $v = 0$ the slice $w = 0$ gives $K_X(E)$ and the seven slices $w \neq 0$ give $7K_Y(F) = K_Y(F)$ in $\mathbf{F}_2$; for $v \neq 0$ the slices $w = 0$ and $w = v$ give $K_Y(E)$ and $K_X(F)$, while the remaining six slices give $6K_Y(F) = 0$. In particular H_1 does not depend on the choice of $v \neq 0$.

Set $P = X + Y$ and $Q = E + F$. Bilinearity of K gives

$$H_0 + H_1 = K_P(Q), \tag{8}$$
$$H_0 = K_P(E) + K_Y(Q). \tag{9}$$

Finally, for radial $H = (h_0, h_1, \ldots, h_5)$ put

$$S(H) = (-1)^{h_0} + 3\sum_{i=1}^{5}(-1)^{h_i} = \sum_{s\in U}(-1)^{H(s)},$$

so that Lemma 2.7 becomes

$$|V_u|\,\chi_u(c) = S(H_0) + 7S(H_1). \tag{10}$$

6 The exact zero criterion

Let

$$\delta = (1, 0, 0, 0, 0, 0), \qquad J = (1, 1, 1, 1, 1, 1),$$

and for $R \subseteq \{1, \ldots, 5\}$ let $\rho_R = (0, \mathbf{1}_R)$ with $\mathbf{1}_R$ the indicator vector of R.

Lemma 6.1 (Zero patterns)**.** *Expression* (10) *vanishes if and only if*

$$(H_0, H_1) = (\delta + \varepsilon J,\ \rho_R + \varepsilon J) \tag{11}$$

for some $\varepsilon \in \mathbf{F}_2$ and some three-element subset $R \subseteq \{1, \ldots, 5\}$. There are exactly twenty such patterns, and they correspond bijectively to the twenty A-stable subsets of V of size 64 *found in Proposition 3.3.*

Proof. By Lemma 2.8, $h_{u,c}$ is the indicator function of an A-stable subset $S \subseteq V$, and $|V_u|\chi_u(c) = |V| - 2|S|$. So the expression vanishes precisely when $|S| = 64$, and Proposition 3.3 lists the twenty possibilities: either S is $\{0\}$ together with three of the five orbits $L_i^\times \times W^\times$, or S consists of all five orbits $L_i^\times \times \{0\}$, the orbit $\{0\} \times W^\times$, and two of the orbits $L_i^\times \times W^\times$.

Translate these into the coordinates of Lemma 5.1: the first family has $H_0 = \delta$ (the value 1 at $z = 0$ and 0 on each $L_i^\times$ in the slice $w = 0$) and $H_1 = \rho_R$ with $|R| = 3$; the second family has $H_0 = (0, \mathbf{1}) = \delta + J$ and $H_1 = (1, \mathbf{1}_{R^c}) = \rho_R + J$ with $|R^c| = 2$, i.e. $|R| = 3$. These are exactly the patterns (11) with $\varepsilon = 0$ and $\varepsilon = 1$, and there are $2\binom{5}{3} = 20$ of them. □

Remark 6.2. Lemma 6.1 can also be proved by direct sign arithmetic: writing $S(H_0) = a + 3\sum b_i$ and $S(H_1) = d+3\sum e_i$ with $a, b_i, d, e_i \in \{\pm 1\}$, vanishing reads $a+3\sum b_i+7d+21\sum e_i = 0$. Since $\sum e_i$ is odd and $|a + 3\sum b_i + 7d| \leq 23$, one gets $\sum e_i = \pm 1$; the case $\sum e_i = -1$ forces $a = -1$, all $b_i = 1$, $d = 1$ and exactly three $e_i = -1$, and the case $\sum e_i = 1$ is the simultaneous sign reversal. We prefer the orbit-counting proof because it shows what the twenty patterns are.

By (8) a zero therefore requires

$$K_P(Q) = H_0 + H_1 = \delta + \rho_R \tag{12}$$

for some three-element R. Write $P = (p_0, p)$ with $p \in \mathbf{F}_2^5$.

Lemma 6.3. *If $\tau(P) = 1$ then K_P is invertible on the six-dimensional space of radial functions on U.*

Proof. Identify functions on $U \cong C_2^4$ with the group algebra $\mathbf{F}_2[U]$. Every element of U is an involution, so the coefficient of s in a product equals $\sum_z X(z + s)E(z) = K_X(E)(s)$; that is, K_P is multiplication by P. Choosing a basis $g_1, \ldots, g_4$ of U and setting $z_i = g_i + 1$ gives

$$\mathbf{F}_2[U] \cong \mathbf{F}_2[z_1, z_2, z_3, z_4]/(z_1^2, z_2^2, z_3^2, z_4^2),$$

so the augmentation ideal is nilpotent and every element of augmentation 1 is a unit. The augmentation of a radial P is $p_0+3\sum_i p_i = \tau(P)$, so P is a unit. Multiplication by ω is a ring automorphism of $\mathbf{F}_2[U]$ fixing P, hence fixing P^{-1}; so P^{-1} is radial and K_P restricts to an invertible map of the radial subspace. $\square$

Proposition 6.4 (Complete zero criterion)**.** *Let $u = (X, Y) \in B^A$, put $P = X + Y = (p_0, p)$ and $Y = (y_0, y)$, and when $\tau(P) = 0$ set*

$$r = p + p_0\mathbf{1}.$$

Then χ_u vanishes at some element of C if and only if one of the following holds:

(i) $\tau(P) = 1$*;*

(ii) $\tau(P) = 0$*,* $\mathrm{wt}(r) = 2$*,* $\tau(Y) = 1$*, and* $r \cdot y = 1 + p_0$*.*

Proof. Suppose $\tau(P) = 1$. Using Lemma 6.3, pick any three-element R and set

$$Q = K_P^{-1}(\delta + \rho_R), \qquad E = K_P^{-1}\big(\delta + K_Y(Q)\big), \qquad F = E + Q.$$

Then (9) gives $H_0 = \delta$ and (8) gives $H_1 = \rho_R$, so χ_u vanishes at $c = (E, F)$ by Lemma 6.1.

Assume now $\tau(P) = 0$, so $\sum_i p_i = p_0$. For $Q = (q_0, q)$, formula (5) simplifies to

$$K_P(Q) = \alpha J + \beta\,(0, r), \qquad \alpha = p_0q_0 + p \cdot q, \quad \beta = \tau(Q), \tag{13}$$

since the first coordinate is α and the line part is $\beta p + (p_0 \sum_i q_i + p \cdot q)\mathbf{1} = \alpha\mathbf{1} + \beta r$. Moreover

$$\alpha + p_0\beta = r \cdot q. \tag{14}$$

If $r \neq 0$, every pair (α, β) is realized: choose q with $r \cdot q = \alpha + p_0\beta$ and then $q_0 = \beta + \sum_i q_i$.

The target (12) has first coordinate 1 and line part of weight 3. By (13), an element of the image with first coordinate 1 has line part $\mathbf{1}$ or $\mathbf{1} + r$, of weight 5 or $5 - \mathrm{wt}(r)$. Now $\mathrm{wt}(r)$ is even: if $p_0 = 0$ then $r = p$ has $\sum_i p_i = 0$, and if $p_0 = 1$ then $\mathrm{wt}(r) = 5 - \mathrm{wt}(p)$ with $\mathrm{wt}(p)$ odd. So the target is attained exactly when $\mathrm{wt}(r) = 2$, in which case R is the complement of $\mathrm{supp}(r)$ and (12) becomes

$$\tau(Q) = 1, \qquad r \cdot q = 1 + p_0. \tag{15}$$

It remains to decide when E can be chosen in (9). Since J lies in the image of K_P, the value of ε in (11) is immaterial, and solvability amounts to

$$\delta + K_Y(Q) \in \langle J, (0, r)\rangle. \tag{16}$$

Put $t = \tau(Y)$ and $\sigma = \sum_i q_i$, so $q_0 = 1 + \sigma$ by (15). Substituting (5) into (16) and subtracting the multiple of J prescribed by the first coordinate turns it into

$$y + tq + (1 + y_0 + t\sigma)\mathbf{1} \in \{0, r\}. \tag{17}$$

If $t = 0$ then $\sum_i y_i = y_0$, so the coordinate sum of the left side of (17) is $\sum_i y_i + 5(1 + y_0) = 1$, which is odd, whereas 0 and r have even coordinate sum. So $t = 0$ is impossible and $\tau(Y) = 1$. Taking the inner product of (17) with r and using $r \cdot \mathbf{1} = \mathrm{wt}(r) = 0$ and $r \cdot r = \mathrm{wt}(r) = 0$ in $\mathbf{F}_2$, we get $r \cdot y = r \cdot q$, which with (15) gives $r \cdot y = 1 + p_0$.

Conversely, assume $\tau(Y) = 1$ and $r \cdot y = 1 + p_0$, and set

$$q = y + (1 + y_0)\mathbf{1}, \qquad q_0 = 1.$$

From $\sum_i y_i = 1 + y_0$ we get $\sigma = \sum_i q_i = 0$, hence $\tau(Q) = 1$; and $r \cdot q = r \cdot y = 1 + p_0$ because $r \cdot \mathbf{1} = 0$. So (15) holds, and the left side of (17) is $y + y + (1 + y_0)\mathbf{1} + (1 + y_0)\mathbf{1} = 0$. Hence a suitable E exists and χ_u has a zero on C. $\square$

7 The exact count

Theorem 7.1. *For the action of Section 4,*

$$|N_A(G)| = 1728 \qquad \textit{and} \qquad |C_G(A)/C_G(A)'| = 4096.$$

Proof. The second equality is Theorem 4.1. For the first, count the $u = (X, Y)$ failing both conditions of Proposition 6.4. The substitution $(X, Y) \mapsto (P, Y)$ with $P = X + Y$ is a bijection of $\mathbf{F}_2^6 \times \mathbf{F}_2^6$, so we may count pairs (P, Y).

Since τ is a nonzero linear functional on $\mathbf{F}_2^6$, there are 32 choices of P with $\tau(P) = 1$; for these, all 64 choices of Y give a character with a zero, contributing nothing.

Let $\tau(P) = 0$, the other 32 choices. The map $(p_0, p) \mapsto (p_0, r)$ with $r = p + p_0\mathbf{1}$ is a bijection from these onto the pairs with $p_0 \in \mathbf{F}_2$ and $r \in \mathbf{F}_2^5$ of even weight, of which there are $2 \cdot 1 = 2$ with $\mathrm{wt}(r) = 0$, $2\binom{5}{2} = 20$ with $\mathrm{wt}(r) = 2$, and $2\binom{5}{4} = 10$ with $\mathrm{wt}(r) = 4$; note $2 + 20 + 10 = 32$.

If $\mathrm{wt}(r) \in \{0, 4\}$, condition (ii) fails for every Y, so all 64 choices of Y are zero-free. If $\mathrm{wt}(r) = 2$, vanishing is equivalent to the two affine conditions

$$\tau(Y) = 1, \qquad r \cdot y = 1 + p_0.$$

The functionals $Y \mapsto \tau(Y)$ and $Y \mapsto r \cdot y$ on $\mathbf{F}_2^6$ are linearly independent, since the first has a nonzero y_0 coefficient, the second has none, and $r \neq 0$. So exactly $2^{6-2} = 16$ of the 64 choices of Y give a zero and 48 are zero-free. Altogether

$$|N_A(G)| = \underbrace{2 \cdot 64}_{\mathrm{wt}(r)=0} + \underbrace{10 \cdot 64}_{\mathrm{wt}(r)=4} + \underbrace{20 \cdot 48}_{\mathrm{wt}(r)=2} = 128 + 640 + 960 = 1728.$$

$\square$

This proves Theorem A. Note $1728 = 12^3$ and $4096 = 16^3$, so the ratio is $(3/4)^3 = 27/64$.

8 Consequences and questions

Proof of Corollary B. By Theorem 4.1, $C \cong C_2^{12}$ is abelian, so every irreducible character of C is linear; in particular χ^* is linear for all $\chi \in \mathrm{Irr}_A(G)$. By Theorem 7.1 exactly $4096 - 1728 = 2368$ of these χ have a zero on C. $\square$

So the proposed criterion of Problem 21.100 fails in the direction "χ^* linear $\Rightarrow \chi_C$ nonvanishing". The converse direction is vacuous here. What the example shows is that the property "χ_C is nonvanishing" is not a function of χ^* alone.

Proof of Corollary D. Let A, G, C be as in Theorem A and let A act diagonally on G^n, so that $C_{G^n}(A) = C^n$ is abelian of order 4096^n. Every irreducible character of G^n is $\chi_1 \otimes \cdots \otimes \chi_n$ with $\chi_i \in \mathrm{Irr}(G)$, uniquely, and this is A-invariant if and only if each χ_i is; moreover its value at $(c_1, \ldots, c_n) \in C^n$ is $\prod_i \chi_i(c_i)$, which is nonzero for all such tuples if and only if each χ_i lies in $N_A(G)$. Hence

$$\frac{|N_A(G^n)|}{|C^n/(C^n)'|} = \left(\frac{1728}{4096}\right)^n = \left(\frac{27}{64}\right)^n \xrightarrow[n\to\infty]{} 0,$$

and $|A| = 21$ remains coprime to $|G^n| = 2^{135n}$. $\square$

Head characters

The same question is raised, and the same correspondence studied, by Isaacs [8]. For G solvable and A acting coprimely, Isaacs calls $\chi \in \mathrm{Irr}_A(G)$ an *A-head character* if χ is the head character of some strong A-pair series, a condition formulated purely in terms of A-composition series of G, and proves in [8, Theorem 7.1] that the A-head characters of G are exactly the $\chi \in \mathrm{Irr}_A(G)$ whose Glauberman–Isaacs correspondent is linear. He closes [8, §7] by recording Navarro's question in the form of Problem 6.3. Combining his theorem with the exact count of Section 7 answers it in his own terms.

Corollary 8.1. *Let A, G, C be as in Theorem A. Then G is solvable, all* 4096 *characters in* $\mathrm{Irr}_A(G)$ *are A-head characters of G, and exactly* 1728 *of them are nonvanishing on C. In particular the A-head characters of G are not the A-invariant irreducible characters that are nonvanishing on C.*

Proof. G is a 2-group, hence solvable, and $|A| = 21$ is coprime to $|G|$, so [8, Theorem 7.1] applies. By Theorem 4.1, C is abelian, so $\chi^*(1) = 1$ for every $\chi \in \mathrm{Irr}_A(G)$, and all 4096 of them are A-head characters. The exact count of Section 7 gives $|N_A(G)| = 1728$. $\square$

Several natural questions remain.

Minimality. Our G has order 2^{135}. Within the family of Section 2, Theorem 3.5 and Corollary 3.6 show that this is the least attainable order over *all* operator groups of odd order, that $\dim V = 7$ is the least attainable dimension, and that $|A| = 15$ is the least attainable operator order (at $\dim V = 8$). We do not know the smallest counterexample to Problem 21.100 overall: the family consists of very particular groups, and nothing here excludes smaller counterexamples of a different shape.

Inequality. Is $|N_A(G)| \leq |C/C'|$ always true? It holds in our examples, and holds trivially whenever C is abelian, since then $|C/C'| = |\mathrm{Irr}(C)| = |\mathrm{Irr}_A(G)| \geq |N_A(G)|$. We know of no general argument.

Repair. Is there a characterization of $N_A(G)$ in terms of the Glauberman–Isaacs correspondence at all? Our example rules out the linearity criterion, but leaves open whether some other invariant of χ^* detects nonvanishing on C.

Nonabelian C. The fixed subgroup in Theorem A is elementary abelian, but this is not essential.

Proposition 8.2. *Let A, G, C be as in Theorem A, let Q be any nonabelian 2-group, and let A act trivially on Q. Then A acts coprimely on $G \times Q$ with nonabelian fixed subgroup $C_{G\times Q}(A) = C \times Q$, and*

$$|N_A(G \times Q)| = 1728\,|Q/Q'| < 4096\,|Q/Q'| = |(C \times Q)/(C \times Q)'|.$$

Problem 21.100 and Problem 6.3 therefore fail with C nonabelian.

Proof. Coprimality is clear since $|G \times Q|$ is a power of 2, and $C_{G\times Q}(A) = C \times Q$ because A is trivial on Q. Every irreducible character of $G \times Q$ is $\chi_1 \otimes \chi_2$ uniquely, and it is A-invariant exactly when χ_1 is. Its value at (c, q) is $\chi_1(c)\chi_2(q)$, so it is nonvanishing on $C \times Q$ exactly when $\chi_1 \in N_A(G)$ and χ_2 is nonvanishing on Q; by Burnside's theorem the latter says χ_2 is linear. Hence $|N_A(G \times Q)| = |N_A(G)|\,|Q/Q'| = 1728|Q/Q'|$, while $(C \times Q)' = Q'$ as C is abelian, so $|(C \times Q)/(C \times Q)'| = |C|\,|Q/Q'| = 4096|Q/Q'|$. For Problem 6.3, the Glauberman–Isaacs correspondence is a bijection $\mathrm{Irr}_A(G\times Q) \to \mathrm{Irr}(C\times Q)$, so the characters with linear correspondent number $|(C \times Q)/(C \times Q)'| = 4096|Q/Q'|$, which differs from $1728|Q/Q'|$. ☐

This still refutes Problem 6.3 in the direction "χ^* linear $\Rightarrow$ χ_C nonvanishing". The opposite direction, which for $A = 1$ is exactly Burnside's theorem, is untouched by our examples, and we do not know whether it can fail.

9 The Carter subgroup analogue

Problem 6.7 of [12] asks whether the number of irreducible characters of a solvable group Γ that do not vanish on a Carter subgroup K is $|K/K'|$. By Theorem A of [8] the head characters of Γ number exactly $|K/K'|$, so the question is equivalently whether the head characters of Γ are exactly the Carter-nonvanishing ones; Isaacs raises it in [8, §6], attributes the affirmative guess to Navarro, reports "abundant computational evidence" for it, and proves it when K is a maximal subgroup [8, Theorem 6.1].

The subgroup C of Theorem 4.1 is not a Carter subgroup of G: it lies in the abelian group B, so $B \le C_G(C) \le N_G(C)$ while $|B| = 2^{128}$ and $|C| = 2^{12}$. Passing to $\Gamma = G \rtimes A$ repairs this.

Proposition 9.1. *Let A, G, C be as in Theorem A and put $\Gamma = G \rtimes A$, a solvable group of order $2^{135} \cdot 21$. Then $K = C \times A$ is a Carter subgroup of Γ, abelian of order $4096 \cdot 21 = 86016$.*

Proof. A centralizes C, and $|C|$ is a power of 2 while $|A| = 21$ is odd, so $K = C \times A$ is abelian, in particular nilpotent. Its Hall $2'$-subgroup A is characteristic in K, so $N_\Gamma(K) \le N_\Gamma(A)$. If $g \in G$ normalizes A then $gag^{-1}a^{-1} \in A \cap G = 1$ for every $a \in A$, so $g \in C_G(A) = C$; hence $N_\Gamma(A) = C_G(A)A = K$, and K is self-normalizing. ☐

We now compute the characters of Γ that are nonvanishing on K. Write $\Gamma = B \rtimes (V \rtimes A)$ and, for $a \in A$ acting on V as T^k, put

$$S_k = \{t \in V : (T^k + 1)t \in V_u\},$$

a T-invariant subgroup of V containing V_u.

Lemma 9.2. *Let $u \in B^A$ and $\theta = \chi_u$. Then θ extends to Γ, the irreducible characters of Γ lying over θ are the 21 characters $\chi_{u,\psi}$ with $\psi \in \mathrm{Irr}(A)$, and for $c \in C$ and $a \in A$ acting as T^k,*

$$\chi_{u,\psi}(ca) = \psi(a) \sum_{t \in S_k/V_u} (-1)^{\langle \tau_t u, c\rangle}.$$

In particular whether $\chi_{u,\psi}$ vanishes at ca does not depend on ψ.

Proof. Let $W = V \rtimes A$, so $\Gamma = B \rtimes W$. As $u \in B^A$ and V_u is T-invariant, the stabilizer of λ_u in W is $W_u = V_u \rtimes A$. For $\psi \in \mathrm{Irr}(A)$ set $\eta_\psi(f,(s,a')) = \lambda_u(f)\psi(a')$ on $B \rtimes W_u$; this is a linear character, because for $s \in V_u$ and a' acting as T^j,

$$\langle u, \tau_s(g \circ T^{-j})\rangle = \langle \tau_s u, g \circ T^{-j}\rangle = \langle u \circ T^j, g\rangle = \langle u, g\rangle.$$

Since $B \rtimes W_u$ is the inertia group of λ_u in Γ, the induced characters $\chi_{u,\psi} = \mathrm{Ind}_{B \rtimes W_u}^{\Gamma} \eta_\psi$ are irreducible and distinct, and they lie over θ; there are 21 of them. Since Γ/G is cyclic, θ extends to Γ [7, Corollary 11.22], so by Gallagher's theorem [7, Corollary 6.17] there are exactly 21 irreducible characters over θ, and these are all of them.

Take $x_t = (0,(t,1))$ for $t \in V/V_u$ as a transversal of $\Gamma/(B \rtimes W_u)$. A direct computation gives

$$x_t^{-1}(c,(0,a))x_t = \big(\tau_t c, ((1+T^k)t, a)\big),$$

which lies in $B \rtimes W_u$ exactly when $(1+T^k)t \in V_u$, that is, when $t \in S_k$. For such t the value of η_ψ is $\lambda_u(\tau_t c)\psi(a) = (-1)^{\langle \tau_t u, c\rangle}\psi(a)$, and the induced-character formula gives the stated sum. ☐

Lemma 9.3. *Let $u \in B^A$ and let $k \not\equiv 0 \pmod{21}$. Then $\sum_{t \in S_k/V_u}(-1)^{\langle \tau_t u, c\rangle} \neq 0$ for every $c \in B^A$, provided $\chi_u \in N_A(G)$.*

Proof. Because S_k is T-invariant and $t \mapsto \langle \tau_t u, c\rangle$ is constant on A-orbits by Lemma 2.8, the sum is a signed sum of the sizes of the A-orbits contained in S_k. Let $d = \gcd(k, 21)$.

If $d = 1$ then $\langle T^k\rangle = \langle T\rangle$, so T^k has no nonzero fixed point on V/V_u by the argument in Lemma 2.4; hence $T^k + 1$ is invertible there and $S_k = V_u$. As $\tau_t u = u$ for $t \in V_u$, the sum is $(-1)^{\langle u,c\rangle} \neq 0$.

If $d = 3$ then $3 \mid k$ and $7 \nmid k$, so T^k acts trivially on U and as multiplication by $\zeta^k \neq 1$ on W. Thus $T^k + 1$ vanishes on U and acts on W as the nonzero $\mathbf{F}_8$-scalar $\zeta^k + 1$. Now $V_u \cap W$ is a ζ-invariant $\mathbf{F}_2$-subspace of $W \cong \mathbf{F}_8$, hence an $\mathbf{F}_8$-subspace, so it is 0 or W; either is preserved by the scalar, and $S_k = U \oplus (V_u \cap W)$. If $V_u \cap W = W$ then $S_k = V$ and the sum is $\chi_u(c) \neq 0$ because $\chi_u \in N_A(G)$. If it is 0 then $S_k = U$, whose A-orbits have sizes $1, 3, 3, 3, 3, 3$; a signed sum $\pm 1 + 3(\pm 1 \pm 1 \pm 1 \pm 1 \pm 1)$ has odd inner sum, so it lies in $\{\pm 1\} + \{\pm 3, \pm 9, \pm 15\}$ and is never 0.

If $d = 7$ then $7 \mid k$ and $3 \nmid k$, so $T^k + 1$ acts on U as the nonzero $\mathbf{F}_4$-scalar $\omega^k + 1$ and vanishes on W. Here $V_u \cap U$ is an ω-invariant $\mathbf{F}_2$-subspace of $U \cong \mathbf{F}_4^2$, hence an $\mathbf{F}_4$-subspace — 0, a line L, or U — and each is preserved by the scalar, giving $S_k = (V_u \cap U) \oplus W$. If $V_u \cap U = U$ then $S_k = V$ and the sum is $\chi_u(c) \neq 0$ as before. If it is 0 then $S_k = W$, with orbit sizes $1, 7$, and $\pm 1 \pm 7 \neq 0$. If it is a line L then $S_k = L \oplus W$, with orbit sizes $1, 3, 7, 21$ summing to 32; no sub-multiset of $\{1, 3, 7, 21\}$ sums to 16, so no signed sum vanishes. ☐

Theorem 9.4. *Let $\Gamma = G \rtimes A$ and $K = C \times A$ be as in Proposition 9.1. The number of $\chi \in \mathrm{Irr}(\Gamma)$ that do not vanish at any element of K is*

$$21\,|N_A(G)| = 21 \cdot 1728 = 36288,$$

whereas $|K/K'| = 86016$. Hence Problem 6.7 of [12] has a negative answer.

Proof. Let $\chi \in \mathrm{Irr}(\Gamma)$ lie over $\theta \in \mathrm{Irr}(G)$ and suppose χ does not vanish on K. Since $\Gamma/G \cong A$ is abelian, the inertia group Γ_θ is normal in Γ and equals $G\,A_\theta$, where $A_\theta = \Gamma_\theta \cap A$. If θ is not A-invariant then $A_\theta < A$, and $\chi = \mathrm{Ind}_{\Gamma_\theta}^{\Gamma}\psi$ vanishes off Γ_θ; choosing $a \in A \setminus A_\theta \subseteq K$ gives $\chi(a) = 0$, a contradiction. So $\theta \in \mathrm{Irr}_A(G)$, and $\theta = \chi_u$ for a unique $u \in B^A$ by Proposition 2.5.

By Lemma 9.2, $\chi = \chi_{u,\psi}$ for some $\psi \in \mathrm{Irr}(A)$, and taking $k = 0$ there gives $S_0 = V$ and $\chi(c) = \theta(c)$ for $c \in C$. Hence $\theta \in N_A(G)$. Conversely, if $\theta = \chi_u \in N_A(G)$ then all 21 characters $\chi_{u,\psi}$ are nonvanishing on K: the case $k = 0$ is the definition of $N_A(G)$, and the cases $k \not\equiv 0$ are Lemma 9.3. So the characters of Γ nonvanishing on K are exactly the $21|N_A(G)| = 36288$ characters $\chi_{u,\psi}$ with $\chi_u \in N_A(G)$, by Theorem 7.1. Finally K is abelian, so $|K/K'| = |K| = 86016 > 36288$. □

Corollary 9.5. *The head characters of* Γ *are not the Carter-nonvanishing irreducible characters of* Γ*. This answers the question of [8, §6] negatively.*

Proof. By [8, Theorem A] the set of head characters of Γ is in bijection with $\mathrm{Lin}(K)$, so it has $|K/K'| = 86016$ elements, while Theorem 9.4 gives 36288 Carter-nonvanishing characters. □

Remark 9.6. The ratio is again $36288/86016 = 27/64$, and by Corollary D the same construction applied to G^n makes it $(27/64)^n$. Since $|\Gamma| = 2^{135} \cdot 21$, the computer searches reported in [8, §6] could not have found it.

As with Theorem 2.11, the counterexample does not depend on the particular V: only the exact value 36288 does.

Theorem 9.7. *Let* A*,* V*,* G *be as in Theorem 2.11 with* (A, V) *balanced, and assume in addition that* A *is abelian. Put* $\Gamma = G \rtimes A$ *and* $K = C \times A$*. Then* Γ *is solvable,* K *is an abelian Carter subgroup of* Γ*, and the number of* $\chi \in \mathrm{Irr}(\Gamma)$ *that do not vanish on* K *is at most*

$$|A|\,|N_A(G)| < |A|\,|C| = |K/K'|.$$

Hence Problem 6.7 has a negative answer for Γ*, and the head characters of* Γ *are not its Carter-nonvanishing characters.*

Proof. G is a 2-group and A is abelian, so Γ is solvable, and the proof of Proposition 9.1 applies verbatim: $K = C \times A$ is abelian, hence nilpotent, and self-normalizing, so it is a Carter subgroup, of order $|C|\,|A|$.

Let $\chi \in \mathrm{Irr}(\Gamma)$ be nonvanishing on K and lie over $\theta \in \mathrm{Irr}(G)$. Since $\Gamma/G \cong A$ is abelian, the inertia group $\Gamma_\theta \geq G$ is normal in Γ, and if θ were not A-invariant, then χ, being induced from Γ_θ, would vanish at any $a \in A \setminus A_\theta \subseteq K$, where $A_\theta = \Gamma_\theta \cap A$. So $\theta \in \mathrm{Irr}_A(G)$. As $(|A|, |G|) = 1$ and Γ splits over G, the character θ extends to some $\hat{\theta}$, and by Gallagher's theorem the characters of Γ over θ are the $|A|$ characters $\hat{\theta}\beta$ with $\beta \in \mathrm{Irr}(A)$; all β are linear because A is abelian. For $c \in C \leq G$ we have $\beta(c) = 1$, so χ and θ agree on C, and nonvanishing of χ on C forces $\theta \in N_A(G)$. There are therefore at most $|A|\,|N_A(G)|$ such characters χ. Theorem 2.11 gives $|N_A(G)| < |C|$, and K is abelian, so $|K/K'| = |K| = |C|\,|A|$. The last sentence follows from [8, Theorem A] as in Corollary 9.5. □

Remark 9.8. Combining Theorem 9.7 with Proposition 2.12, there are infinitely many solvable groups Γ for which the number of Carter-nonvanishing irreducible characters is strictly smaller than $|K/K'|$. The smallest we obtain is the one of Theorem 9.4, of order $2^{135} \cdot 21$.

10 Scope: the surrounding problems

Problem 6.3 sits inside a group of related problems in [12], and Navarro raises it there as an instance of a general principle: for a distinguished subgroup $H \leq G$ and a natural bijection * from a canonical subset of $\mathrm{Irr}(G)$ onto one of $\mathrm{Irr}(H)$, one expects χ^* to be linear exactly when χ_H is never zero [12, p. 189]. Corollary B refutes that principle for the Glauberman–Isaacs correspondence. Its reach is limited, and we record the limits.

The hypothesis that A be a p-group cannot be dropped. Both Navarro [12, p. 189] and Isaacs [8, §7] observe that an argument with roots of unity proves one direction of Problem 6.3 when A is a p-group: if A is a p-group and $\chi^*(1) = 1$, then χ_C is never zero. In our example $|A| = 21$ is divisible by two primes, and $\chi^*(1) = 1$ holds for all 4096 invariant characters while 2368 of them vanish somewhere on C. So that observation becomes false the moment A is allowed two prime divisors, and the restriction to p-groups in it is essential rather than an artifact of the proof.

Three neighboring statements are untouched, for reasons worth stating briefly. Problem 6.1 asks whether a $\chi \in \mathrm{Irr}(\Gamma)$ nonvanishing on $N_\Gamma(P)$, for $P \in \mathrm{Syl}_p(\Gamma)$, must have degree prime to p; for the Γ of Section 9 it holds at every p, since at $p = 2$ we have $N_\Gamma(G) = \Gamma$ and Burnside applies, while at $p \in \{3, 7\}$ the argument of Theorem 9.4 forces χ to lie over an A-invariant θ, whence $\chi(1) = \theta(1)$ is a power of 2. Problem 6.5 and Theorem 6.6 of [12] take as hypothesis only the p-group case of Problem 6.3, which our example does not touch, so both remain open — and by the previous paragraph that case is now the only one available to them. Finally the problems of [12, §5], on elements where the characters of degree prime to p do not vanish, are vacuous or trivial for a 2-group: at $p = 2$ the odd-degree characters are the linear ones and every element is a 2-element, and at odd p we have $\mathbf{O}_{p'}(G) = G$.

What the example does establish, beyond the two counts of Theorem A, is that nonvanishing on C is not determined by χ^*, and that any repair of Problem 6.3 must either restrict the operator group — to a p-group, say — or use more of χ than its correspondent. The p-group case is the one that survives, and it is the natural remaining question: by the argument of [8, §7] one of its two directions is a theorem, so a counterexample there would have to refute the other, and by Proposition 3.2 it would have to be built differently from ours.

11 Verification

The proofs above are self-contained; the computations described here are independent checks and are used nowhere in them. All of them are exact, in integer and $\mathbf{F}_2$ arithmetic with no floating point, and all are available in [5].

Three programs compute $|N_A(G)|$ by different routes — a 128-point integer Walsh transform, a direct computation in $\mathbf{F}_4^2 \oplus \mathbf{F}_8$ from the radial correlation table, and a binary linear-algebra test built on the twenty zero patterns of Lemma 6.1 — and all three return 1728. A fourth evaluates the characters of Γ on K by Lemma 9.2 and returns the 36288 of Theorem 9.4. Further scripts reproduce the design enumeration of Section 3 and check Theorem 3.5 twice over: once through the support-sum criterion on which its proof rests, and once through an independent enumeration of the odd-order subgroups of the relevant groups $\Gamma L(m, 2^e)$, which confirms its conclusion in dimension at most 5. An accompanying test suite checks the orbit sizes, the correlation identity (5), the twenty zero patterns, and the vanishing of Theorem 4.1.

Since $|G| = 2^{135}$, the group cannot be constructed in a computer algebra system, and nothing above requires it: every computation runs on V, with 128 points and 12 orbits, on B^A, with 4096 elements, or on multisets of divisors and small matrix groups over $\mathbf{F}_2$.

A further script in [5] checks the ingredients in GAP [3], using that system's own character theory rather than any formula proved here. It confirms the arithmetic of Section 3 at $\dim V = 7$, and then, in the same family $G = C_2 \wr V$ at $\dim V = 2$ and 3, the structural statements of Section 2: that $C_G(A) = B^A$ is elementary abelian of the predicted rank, that $|\mathrm{Irr}_A(G)| = |C/C'|$, and that $\chi_{\delta_0}(c) = |V| - 2|\mathrm{supp}\, c|$ at every A-stable c, which is Lemma 2.10, the identity producing the zero.

It also confirms that $K = C \times A$ is a Carter subgroup of Γ, as Proposition 9.1 asserts. We single out two further runs. Dropping $C_V(A) = 0$ admits a balanced V of dimension 3, where GAP displays vanishing invariant characters outright: there $|G| = 2048$, C is nonabelian of order 32, and $|\operatorname{Irr}_A(G)| = |\operatorname{Irr}(C)| = 14$ while $|C/C'| = 8 = |N_A(G)|$, so Problem 21.100 survives because the slack between $|C/C'|$ and $|\operatorname{Irr}(C)|$ absorbs the zeros. Removing that slack is exactly what the fixed-point-free hypothesis does. And a search over all 968 coprime cyclic actions on all groups of order at most 63 finds no counterexample to Problem 21.100 anywhere, which places the size of ours in context.

Acknowledgments

The author thanks Abhinav Namboori for helpful discussions and comments on the exposition.

The author used OpenAI's ChatGPT (GPT-5.6 Thinking) during the preparation of this manuscript for mathematical exploration, checking intermediate arguments and edge cases, generating exact verification code, and editorial revision. The author reviewed the resulting arguments and takes responsibility for the contents of the paper.

References

[1] A. H. Clifford, *Representations induced in an invariant subgroup*, Ann. of Math. (2) **38** (1937), 533–550.

[2] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.14.0, 2024, `https://www.gap-system.org`.

[4] G. Glauberman, *Correspondences of characters for relatively prime operator groups*, Canad. J. Math. **20** (1968), 1465–1488.

[5] E. Hou, *Coprime actions and characters nonvanishing on the fixed-point subgroup: manuscript and verification code*, Zenodo, 2026, `https://doi.org/10.5281/zenodo.21709999`.

[6] I. M. Isaacs, *Characters of solvable and symplectic groups*, Amer. J. Math. **95** (1973), 594–635.

[7] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[8] I. M. Isaacs, *Carter subgroups, characters and composition series*, Trans. Amer. Math. Soc. Ser. B **9** (2022), 470–498.

[9] I. M. Isaacs, G. Navarro and T. R. Wolf, *Finite group elements where no irreducible character vanishes*, J. Algebra **222** (1999), no. 2, 413–423.

[10] E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved Problems in Group Theory: The Kourovka Notebook*, No. 21, Sobolev Institute of Mathematics, Novosibirsk, 2026, Problem 21.100, p. 178; arXiv:1401.0300v45.

[11] G. Navarro, *Character Theory and the McKay Conjecture*, Cambridge Studies in Advanced Mathematics 175, Cambridge University Press, Cambridge, 2018.

[12] G. Navarro, *Problems on characters: solvable groups*, Publ. Mat. **67** (2023), 173–198, Problem 6.3, p. 189.