

EXPLICIT FINITE p -GROUP COUNTEREXAMPLES TO THE AMIT–ASHURST CONJECTURE

SHIHAO WANG AND ZHIWEI ZHENG

ABSTRACT. For every prime p , we construct a finite p -group G of order p^{498} and nilpotency class two for which the word $w = \prod_{j=1}^{12} [x_{2j-1}, x_{2j}]$ admits a value $g \neq 1$ whose fibre has size strictly less than $|G|^{23}$. This gives counterexamples to the Amit–Ashurst conjecture for every prime. We determine the exact fibre size by reducing the word equation to matrix equations over $\mathbb{F}_p$ and counting their solutions.

1. INTRODUCTION

Let F_r denote the free group of rank $r \geq 1$ on free generators $x_1, \dots, x_r$. An *ordinary word* $w \in F_r$ induces on every group G a word map $w: G^r \rightarrow G$ via substitution. When G is finite, we denote the image of this map by $w(G) = \{w(g_1, \dots, g_r) : g_i \in G\}$, and for each $g \in G$ we write

$$N_{w,G}(g) = |\{(g_1, \dots, g_r) \in G^r : w(g_1, \dots, g_r) = g\}|, \quad P_{w,G}(g) = \frac{N_{w,G}(g)}{|G|^r},$$

for the cardinality and induced probability measure of the fibre over g , respectively.

Amit proposed the following conjecture; see [Ab06].

Amit Conjecture. *For every finite nilpotent group G and every word $w \in F_r$,*

$$N_{w,G}(1) \geq |G|^{r-1}. \quad (1)$$

Ashurst [Ash12] proposed the following strengthening, called the Amit–Ashurst conjecture [CCT23].

Amit–Ashurst Conjecture. *For every finite nilpotent group G and every word $w \in F_r$,*

$$N_{w,G}(g) \geq |G|^{r-1} \quad \text{for every } g \in w(G). \quad (2)$$

Since every finite nilpotent group is the direct product of its Sylow p -subgroups [Rob96, Theorem 5.2.4] and word evaluation commutes with direct products,

$$N_{w,A \times B}((a, b)) = N_{w,A}(a)N_{w,B}(b),$$

both conjectures (1) and (2) immediately reduce to the case of finite p -groups.

Solomon’s divisibility theorem [Sol69] gives $N_{w,G}(1) \geq |G|$ for every finite group and every two-variable word. Abért [Ab06] and Nikolov–Segal [NS07] showed that a finite group G is solvable if and only if there exists a constant $\varepsilon_G > 0$ such that $P_{w,G}(1) \geq \varepsilon_G$ for every $r \geq 1$ and every word $w \in F_r$. For arbitrary numbers of variables, Levy [Lev11, Theorem 1.1] and, independently, Iñiguez–Sangroniz [IS17] proved the original Amit conjecture for finite groups of nilpotency class two. Levy’s result also covers finite split metacyclic groups (semidirect products of two cyclic groups) [Lev11, Proposition 1.3].

For nonidentity fibres, Ashurst [Ash12, Chapter 4] established the Amit–Ashurst conjecture for dihedral 2-groups and generalized quaternion groups. Camina–Iñiguez–Thillaisundaram [CIT20, Theorems A and C] proved the Amit–Ashurst conjecture for two-variable words on finite p -groups of nilpotency class two and for products of disjoint commutators on finite p -groups with exactly two distinct irreducible complex character degrees. Camina–Cocke–Thillaisundaram [CCT23,

Theorem A] proved the full Amit–Ashurst conjecture for finite p -groups with a cyclic maximal subgroup. Kishnani–Kulshrestha [KK24] proved that

$$N_{w,G}(g) \geq \frac{|G|^{r-1}}{|G'|} \quad (g \in w(G))$$

for every finite group G of nilpotency class two, where $G' = \langle [x, y] : x, y \in G \rangle$ and $[x, y] = x^{-1}y^{-1}xy$.

For a group G , set

$$G_{(0)} = G, \quad G_{(i)} = [G_{(i-1)}, G] = \langle [x, y] : x \in G_{(i-1)}, y \in G \rangle \quad (i \geq 1).$$

A group G has nilpotency class two, written $\text{cl}(G) = 2$, if

$$G_{(1)} \neq \langle 1 \rangle \quad \text{and} \quad G_{(2)} = \langle 1 \rangle.$$

We obtain the following result.

Theorem 1.1. *For every prime p , there exists an explicitly defined finite p -group G of order $|G| = p^{498}$ and nilpotency class $\text{cl}(G) = 2$, such that for the product of twelve disjoint commutators*

$$w(x_1, \dots, x_{24}) = \prod_{j=1}^{12} [x_{2j-1}, x_{2j}] \in F_{24}, \quad (3)$$

there is an attained nonidentity value $g \in w(G) \setminus \{1\}$ whose fibre has exact cardinality

$$N_{w,G}(g) = p^{11298} \prod_{j=1}^{12} (p^{2j} - 1) \quad (4)$$

$$= |G|^{23} \prod_{j=1}^{12} (1 - p^{-2j}) < |G|^{23}. \quad (5)$$

Our construction uses the classical description of groups of nilpotency class two by bilinear maps [Bae38], with quadratic maps describing central extensions of elementary abelian 2-groups [PY07, Section 2]. We express commutators as alternating matrices and choose the relations using a nilpotent shift and an anisotropic binary quadratic form. The word equation then reduces to a symplectic matrix equation and a quadratic equation whose solutions are determined by the kernels of the shifts. Counting these solutions gives the fibre size in Theorem 1.1.

2. AMBIENT LINEAR SPACES AND THE RELATION SUBSPACE

We first treat the case $p = 2$. Unless otherwise stated, all vector spaces are over $\mathbb{F}_2$, and all vectors are column vectors. Let $H = \mathbb{F}_2^{11}$ be an 11-dimensional vector space over $\mathbb{F}_2$ equipped with the ordered standard basis $e_0, e_1, \dots, e_{10}$. We define the nilpotent shift endomorphism $T: H \rightarrow H$ on basis vectors by

$$Te_i = e_{i+1} \quad (0 \leq i < 10), \quad Te_{10} = 0. \quad (6)$$

For each integer $1 \leq s \leq 6$, the s -fold iterate T^s satisfies

$$\ker T^s = \langle e_{11-s}, \dots, e_{10} \rangle, \quad \dim_{\mathbb{F}_2} \ker T^s = s. \quad (7)$$

Next, let $P = \mathbb{F}_2^{24}$ have ordered standard basis $f_1, \dots, f_{24}$, and form the 35-dimensional direct sum

$$D = P \oplus H \cong \mathbb{F}_2^{35},$$

where we order the basis of D by placing all 24 basis vectors of P before the 11 basis vectors of H .

In characteristic two, we denote by $\text{Alt}_n = \text{Alt}_n(\mathbb{F}_2)$ the $\mathbb{F}_2$ -vector space of symmetric $n \times n$ matrices with zero diagonal:

$$\text{Alt}_n = \{M \in \text{Mat}_{n \times n}(\mathbb{F}_2) : M^T = M \text{ and } M_{ii} = 0 \text{ for all } 1 \leq i \leq n\}.$$

Here $\text{Mat}_{a \times b}(\mathbb{F}_2)$ denotes the space of $a \times b$ matrices. Clearly $\dim_{\mathbb{F}_2} \text{Alt}_n = \binom{n}{2}$. The canonical bilinear assignment

$$v \wedge u \mapsto vu^T + uv^T \quad (v, u \in \mathbb{F}_2^n) \quad (8)$$

identifies the exterior square $\wedge^2 \mathbb{F}_2^n$ isomorphically with Alt_n , sending each elementary wedge $e_i \wedge e_j$ ($i < j$) to the elementary alternating matrix having 1 at entries (i, j) and (j, i) and 0 elsewhere.

For each

$$z = (z_{1,1}, z_{1,2}, \dots, z_{6,1}, z_{6,2}) \in H^{12},$$

define $C(z) \in \text{Mat}_{24 \times 11}(\mathbb{F}_2)$ by

$$C(z)_{2s-1,*} = z_{s,1}^T, \quad C(z)_{2s,*} = z_{s,2}^T, \quad (9)$$

$$C(z)_{12+2s-1,*} = (T^s(z_{s,1} + z_{s,2}))^T, \quad C(z)_{12+2s,*} = (T^s z_{s,2})^T, \quad (10)$$

for $1 \leq s \leq 6$, where $C(z)_{i,*}$ denotes the i -th row of $C(z)$. Define

$$K = \left\{ \begin{pmatrix} 0_{24 \times 24} & C(z) \\ C(z)^T & 0_{11 \times 11} \end{pmatrix} : z \in H^{12} \right\} \subseteq \text{Alt}_{35}. \quad (11)$$

Since each T^s is linear, the map

$$H^{12} \longrightarrow \text{Alt}_{35}, \quad z \longmapsto \begin{pmatrix} 0 & C(z) \\ C(z)^T & 0 \end{pmatrix}$$

is linear. By the construction of $C(z)$, this map is injective. Hence K is a linear subspace and

$$\dim_{\mathbb{F}_2} K = \dim_{\mathbb{F}_2} H^{12} = 12 \cdot 11 = 132.$$

Set $W = \text{Alt}_{35} / K$, and write $\pi : \text{Alt}_{35} \rightarrow W$, $A \mapsto A + K$, for the quotient map. Then

$$\dim_{\mathbb{F}_2} W = \binom{35}{2} - \dim_{\mathbb{F}_2} K = 595 - 132 = 463. \quad (12)$$

Remark 2.1. One can realize W explicitly as a direct sum of matrix spaces. For $R \in \text{Mat}_{24 \times 11}(\mathbb{F}_2)$, let R_+ consist of its first twelve rows and R_- of its last twelve rows. Thus

$$R = \begin{pmatrix} R_+ \\ R_- \end{pmatrix}, \quad R_+, R_- \in \text{Mat}_{12 \times 11}(\mathbb{F}_2).$$

Define the linear operator $L : \text{Mat}_{12 \times 11}(\mathbb{F}_2) \rightarrow \text{Mat}_{12 \times 11}(\mathbb{F}_2)$ row-wise for $1 \leq s \leq 6$ by

$$L(R_+)_{2s-1,*} = (R_+_{2s-1,*} + R_+_{2s,*})(T^s)^T, \quad L(R_+)_{2s,*} = R_+_{2s,*}(T^s)^T,$$

where $R_+_{i,*}$ denotes row i of R_+ . Then $\begin{pmatrix} R_+ \\ R_- \end{pmatrix} = C(z)$ for some $z \in H^{12}$ if and only if $R_- = L(R_+)$. Consequently, the linear map

$$\text{Alt}_{35} \longrightarrow \text{Alt}_{24} \oplus \text{Mat}_{12 \times 11}(\mathbb{F}_2) \oplus \text{Alt}_{11}, \quad \begin{pmatrix} A & R \\ R^T & B \end{pmatrix} \longmapsto (A, R_- + L(R_+), B),$$

is surjective (as seen by restricting to $R_+ = 0$) and has kernel precisely equal to K , inducing an explicit coordinate isomorphism $W \cong \text{Alt}_{24} \oplus \text{Mat}_{12 \times 11}(\mathbb{F}_2) \oplus \text{Alt}_{11}$.

3. CONSTRUCTION OF THE 2-GROUP G

To construct a central extension of $D = P \oplus H \cong \mathbb{F}_2^{35}$ by W , we introduce the bilinear map $F : D \times D \rightarrow \text{Alt}_{35}$ by

$$F(v, u)_{ij} = \begin{cases} v_i u_j, & \text{if } 1 \leq i < j \leq 35, \\ v_j u_i, & \text{if } 1 \leq j < i \leq 35, \\ 0, & \text{if } i = j. \end{cases} \quad (13)$$

It is immediate from (13) that $F(v, u)$ is a symmetric matrix with zero diagonal and F is bilinear in (v, u) . Moreover, F satisfies the fundamental identity

$$F(v, u) + F(u, v) = vu^T + uv^T \in \text{Alt}_{35} \quad (v, u \in D). \quad (14)$$

Composing F with the quotient map $\pi : \text{Alt}_{35} \rightarrow W$, we set

$$f(v, u) = \pi(F(v, u)) \in W$$

and endow the Cartesian product $G = D \times W$ with the binary operation

$$(v, a)(u, b) = (v + u, a + b + f(v, u)) \quad (v, u \in D, a, b \in W). \quad (15)$$

Write $Z(G) = \{z \in G : zx = xz \text{ for every } x \in G\}$ for the center of G . The exponent $\exp(G)$ of a finite group G is the least positive integer n such that $x^n = 1$ for every $x \in G$.

Proposition 3.1. *The multiplication rule (15) makes G into a finite 2-group with the following properties:*

$$(1) |G| = 2^{498}, \text{ cl}(G) = 2 \text{ and } \exp(G) = 4.$$

$$(2) \text{ For all } (v, a), (u, b) \in G,$$

$$[(v, a), (u, b)] = (0, \pi(vu^T + uv^T)). \quad (16)$$

$$(3) G' = Z(G) = \{0\} \times W.$$

Proof. We first verify the group law, and then prove (2), (3) and (1).

Since $f: D \times D \rightarrow W$ is bilinear, we have for all $v, u, t \in D$ the 2-cocycle identity

$$f(v, u) + f(v + u, t) = f(v, u) + f(v, t) + f(u, t) = f(u, t) + f(v, u + t),$$

which guarantees that the multiplication (15) is associative. Because $f(v, 0) = f(0, v) = 0$, the element $1_G = (0, 0)$ is the two-sided identity, and every element of $\{0\} \times W$ satisfies

$$(v, a)(0, b) = (v, a + b) = (0, b)(v, a),$$

so $\{0\} \times W \leq Z(G)$. Moreover, since $2v = 0$ in D and $2a = 0$ in W , we have

$$(v, a)(v, a + f(v, v)) = (2v, 2a + 2f(v, v)) = (0, 0) = (v, a + f(v, v))(v, a),$$

establishing the inverse formula

$$(v, a)^{-1} = (v, a + f(v, v)).$$

By (12),

$$|G| = |D| \cdot |W| = 2^{35} \cdot 2^{463} = 2^{498},$$

so G is a finite 2-group.

Proof of (2). For $x = (v, a)$ and $y = (u, b)$ in G , applying (15) and the inverse formula above gives

$$\begin{aligned} x^{-1}y^{-1}x &= (v, a + f(v, v))(u, b + f(u, u))(v, a) \\ &= (u, b + f(u, u) + f(v, u) + f(u, v)), \end{aligned}$$

and multiplying on the right by $y = (u, b)$ yields, via (14),

$$[x, y] = (0, f(v, u) + f(u, v)) = (0, \pi(vu^T + uv^T)),$$

proving (16).

Proof of (3). Since the elementary wedges $vu^T + uv^T$ span Alt_{35} as v, u range over D and $\pi: \text{Alt}_{35} \rightarrow W$ is surjective, we obtain

$$G' = \{0\} \times \text{span}_{\mathbb{F}_2} \{\pi(vu^T + uv^T) : v, u \in D\} = \{0\} \times W.$$

To determine the center, write $v = p + h$ with $p \in P$ and $h \in H$. If $(v, a) \in Z(G)$, then $vu^T + uv^T \in K$ for all $u \in D$. Since every element of K has zero diagonal blocks, choosing $u \in P$ and $u \in H$ gives, respectively,

$$pu^T + up^T = 0 \quad (u \in P), \quad hu^T + uh^T = 0 \quad (u \in H).$$

Thus $p = h = 0$, and $Z(G) = \{0\} \times W$.

Proof of (1). The order of G was computed above. By (3), $G' = \{0\} \times W \subseteq Z(G)$. Since $\dim_{\mathbb{F}_2} W = 463 > 0$, we have $G' \neq \{1_G\}$, and hence $\text{cl}(G) = 2$.

For any $(v, a) \in G$, squaring via (15) gives $(v, a)^2 = (0, f(v, v)) \in \{0\} \times W$, and squaring again gives $(v, a)^4 = (0, 2f(v, v)) = (0, 0) = 1_G$. To see that $\exp(G) = 4$, take $v = f_1 + f_2 \in P$, where f_i is the standard basis vector; then $F(v, v)$ has $(1, 2)$ entry $v_1v_2 = 1$ in the upper-left block, so $F(v, v) \notin K$. Hence $(v, 0)^2 = (0, \pi F(v, v)) \neq 1_G$, confirming $\exp(G) = 4$. $\square$

4. THE ATTAINED TARGET VALUE AND THE ANISOTROPIC SHIFT LEMMA

On P , we fix the standard 24×24 nondegenerate alternating block matrix

$$J = \begin{pmatrix} 0 & I_{12} \\ I_{12} & 0 \end{pmatrix} \in \mathrm{GL}_{24}(\mathbb{F}_2),$$

where I_n is the $n \times n$ identity matrix and $\mathrm{GL}_n(\mathbb{F}_2)$ is the group of invertible $n \times n$ matrices. The matrix J satisfies $J^T = J$ and $J^2 = I_{24}$, so that $J^{-1} = J$.

We define the target matrix $A_0 \in \mathrm{Alt}_{35}$ and the corresponding central group element $g \in G' = \{0\} \times W$ by

$$A_0 = \begin{pmatrix} J & 0 \\ 0 & 0 \end{pmatrix} \in \mathrm{Alt}_{35}, \quad g = (0, \pi A_0) \in G. \quad (17)$$

Because the upper-left 24×24 block of A_0 is $J \neq 0$, whereas every matrix in K has zero upper-left 24×24 block by Remark 2.1, we have $A_0 \notin K$ and hence $g \neq 1_G$.

To verify that g is attained by the word $w = \prod_{j=1}^{12} [x_{2j-1}, x_{2j}] \in F_{24}$, evaluate w on the specific 24-tuple of basis lifts

$$x_{2j-1} = (f_j, 0), \quad x_{2j} = (f_{12+j}, 0) \quad (1 \leq j \leq 12). \quad (18)$$

By the commutator formula (16) and the centrality of G' , we have

$$w(x_1, \dots, x_{24}) = \left(0, \pi \left(\sum_{j=1}^{12} (f_j f_{12+j}^T + f_{12+j} f_j^T) \right) \right) = (0, \pi A_0) = g.$$

Thus $g \in w(G)$, confirming that the fibre $w^{-1}(g)$ is nonempty.

Before parameterizing the full fibre $w^{-1}(g)$, we study the equation $C(z)^T J C(z) = 0$ for $z \in H^{12}$, with $C(z)$ defined in (9)–(10). Under the identification (8) on $H = \mathbb{F}_2^{11}$, expanding the block product $C(z)^T J C(z) \in \mathrm{Alt}_{11}$ across the rows (9)–(10) yields

$$\begin{aligned} C(z)^T J C(z) &= \sum_{s=1}^6 \left(z_{s,1} \wedge T^s(z_{s,1} + z_{s,2}) + z_{s,2} \wedge T^s z_{s,2} \right) \\ &= \sum_{s=1}^6 Q_s(z_{s,1}, z_{s,2}), \end{aligned} \quad (19)$$

where for each $1 \leq s \leq 6$ and $a, b \in H$, the quadratic map $Q_s: H \times H \rightarrow \mathrm{Alt}_{11}$ is defined by

$$Q_s(a, b) = a \wedge T^s a + a \wedge T^s b + b \wedge T^s b. \quad (20)$$

Set $q(a, b) = a^2 + ab + b^2$ for $a, b \in \mathbb{F}_2$. It is direct to show that $q(a, b) = 0$ if and only if $(a, b) = (0, 0)$.

The following lemma is the heart of the characteristic-two counting argument: it exploits a degree grading on $\wedge^2 H$ together with the anisotropy of $q(c_1, c_2) = c_1^2 + c_1 c_2 + c_2^2$ over $\mathbb{F}_2$ to show that $C(z)^T J C(z)$ vanishes if and only if every parameter vector $z_{s,1}, z_{s,2}$ lies in the kernel of T^s .

Lemma 4.1. *For every $z \in H^{12}$, the matrix $C(z)$ defined by (9)–(10) satisfies*

$$C(z)^T J C(z) = 0 \iff z_{s,1}, z_{s,2} \in \ker T^s \text{ for every } s = 1, \dots, 6. \quad (21)$$

Consequently, the solution set in H^{12} has exact cardinality

$$|\{z \in H^{12} : C(z)^T J C(z) = 0\}| = 2^{42}. \quad (22)$$

Proof. Expand any vector $z \in H$ in the standard basis as $z = \sum_{i=0}^{10} z_i e_i$, and endow the basis elements $e_i \wedge e_j$ ($0 \leq i < j \leq 10$) of $\wedge^2 H \cong \mathrm{Alt}_{11}$ with the additive degree

$$\deg(e_i \wedge e_j) = i + j.$$

For a given parameter tuple $z = (z_{s,1}, z_{s,2})_{s=1}^6 \in H^{12}$, consider the active index set

$$S = \{s \in \{1, \dots, 6\} : (T^s z_{s,1}, T^s z_{s,2}) \neq (0, 0)\}.$$

If $S = \emptyset$, then $T^s z_{s,1} = T^s z_{s,2} = 0$ for every $1 \leq s \leq 6$, so each summand $Q_s(z_{s,1}, z_{s,2})$ in (19) vanishes identically and $C(z)^T J C(z) = 0$.

Suppose conversely that $S \neq \emptyset$. For each $s \in S$, define the leading nonvanishing coordinate index

$$a_s = \min\{i \in \{0, \dots, 10\} : ((z_{s,1})_i, (z_{s,2})_i) \neq (0, 0)\},$$

and set $c_1 = (z_{s,1})_{a_s} \in \mathbb{F}_2$ and $c_2 = (z_{s,2})_{a_s} \in \mathbb{F}_2$. Therefore, $(c_1, c_2) \neq (0, 0)$ in $\mathbb{F}_2^2$. Since $(T^s z_{s,1}, T^s z_{s,2}) \neq (0, 0)$, at least one of $z_{s,1}, z_{s,2}$ has a nonzero coordinate at an index $\leq 10 - s$, which implies that $a_s + s \leq 10$.

Expanding $Q_s(z_{s,1}, z_{s,2})$ via (20) and (6), every nonzero basis term in $Q_s(z_{s,1}, z_{s,2})$ is of the form $e_i \wedge e_{j+s}$ with $i, j \geq a_s$. Its degree therefore satisfies

$$\deg(e_i \wedge e_{j+s}) = i + j + s \geq 2a_s + s,$$

with equality $i + j + s = 2a_s + s$ holding if and only if $i = j = a_s$. At this unique minimal-degree basis element $e_{a_s} \wedge e_{a_s+s}$, the coefficient in $Q_s(z_{s,1}, z_{s,2})$ is precisely

$$c_1^2 + c_1 c_2 + c_2^2 = q(c_1, c_2) = 1 \in \mathbb{F}_2,$$

because $(c_1, c_2) \in \mathbb{F}_2^2 \setminus \{(0, 0)\}$. Thus $Q_s(z_{s,1}, z_{s,2})$ has homogeneous degree- $(2a_s + s)$ component equal to $e_{a_s} \wedge e_{a_s+s}$, and all of its other nonzero terms have strictly larger degree.

Now let $\delta = \min_{s \in S} (2a_s + s)$ be the minimum leading degree among all active indices $s \in S$. Extracting the homogeneous degree- δ component of the sum $\sum_{s=1}^6 Q_s(z_{s,1}, z_{s,2})$ in (19) gives

$$\left(\sum_{s=1}^6 Q_s(z_{s,1}, z_{s,2}) \right)_\delta = \sum_{\substack{s \in S \\ 2a_s + s = \delta}} e_{a_s} \wedge e_{a_s+s}.$$

Crucially, the basis wedges $e_{a_s} \wedge e_{a_s+s}$ appearing in this sum are pairwise distinct. We conclude that $\sum_{s=1}^6 Q_s(z_{s,1}, z_{s,2}) \neq 0$ whenever $S \neq \emptyset$. This proves (21).

Finally, since $\dim_{\mathbb{F}_2} \ker T^s = s$ for $1 \leq s \leq 6$ by (7), the number of tuples $z \in H^{12}$ satisfying $C(z)^T J C(z) = 0$ is

$$\prod_{s=1}^6 |\ker T^s|^2 = \prod_{s=1}^6 2^{2s} = 2^{2(1+2+3+4+5+6)} = 2^{42},$$

which establishes (22). $\square$

5. BIJECTIVE PARAMETERIZATION AND EXACT FIBRE ENUMERATION

We now determine the exact cardinality of the fibre $w^{-1}(g)$ in G^{24} . Let $x_i = (v_i, a_i) \in G$, with $v_i \in D$ and $a_i \in W$, for $1 \leq i \leq 24$, and arrange their D -coordinates $v_i \in \mathbb{F}_2^{35}$ as the columns of a 35×24 matrix X with the odd-indexed columns first, followed by the even-indexed columns:

$$X = (v_1 \ v_3 \ \cdots \ v_{23} \ v_2 \ v_4 \ \cdots \ v_{24}) = \begin{pmatrix} U \\ Y \end{pmatrix} \in \text{Mat}_{35 \times 24}(\mathbb{F}_2),$$

where $U \in \text{Mat}_{24 \times 24}(\mathbb{F}_2)$ records the P -coordinates and $Y \in \text{Mat}_{11 \times 24}(\mathbb{F}_2)$ records the H -coordinates. By (16) and $(0, a)(0, b) = (0, a + b)$, we have

$$\begin{aligned} w(x_1, \dots, x_{24}) &= \prod_{j=1}^{12} [x_{2j-1}, x_{2j}] = \prod_{j=1}^{12} \left(0, \pi \left(v_{2j-1} v_{2j}^T + v_{2j} v_{2j-1}^T \right) \right) \\ &= \left(0, \pi \left(\sum_{j=1}^{12} \left(v_{2j-1} v_{2j}^T + v_{2j} v_{2j-1}^T \right) \right) \right). \end{aligned}$$

Since

$$X J X^T = \sum_{j=1}^{12} \left(v_{2j} v_{2j-1}^T + v_{2j-1} v_{2j}^T \right),$$

we obtain

$$w(x_1, \dots, x_{24}) = (0, \pi(XJX^T)). \quad (23)$$

Notice that the W -coordinates $a_1, \dots, a_{24} \in W$ do not appear in (23), so they may be chosen arbitrarily in W^{24} .

Let $\mathrm{Sp}_{2m}(2)$ denote the symplectic group of $2m \times 2m$ matrices over $\mathbb{F}_2$:

$$\mathrm{Sp}_{2m}(2) = \{U \in \mathrm{GL}_{2m}(\mathbb{F}_2) : UJ_{2m}U^T = J_{2m}\}, \quad J_{2m} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}.$$

Proposition 5.1. *The set of matrices $X = \begin{pmatrix} U \\ Y \end{pmatrix} \in \mathrm{Mat}_{35 \times 24}(\mathbb{F}_2)$ satisfying $w(x_1, \dots, x_{24}) = g$ in (17) is in explicit bijection with the Cartesian product*

$$\mathrm{Sp}_{24}(2) \times \{z \in H^{12} : C(z)^T J C(z) = 0\}$$

via the map

$$(U, z) \mapsto \begin{pmatrix} U \\ C(z)^T U^{-T} J \end{pmatrix}. \quad (24)$$

The inverse sends $\begin{pmatrix} U \\ Y \end{pmatrix}$ to (U, z) , where

$$z_{s,1} = ((UJY^T)_{2s-1,*})^T, \quad z_{s,2} = ((UJY^T)_{2s,*})^T \quad (1 \leq s \leq 6).$$

Proof. By the definitions of K in (11), $g = (0, \pi A_0)$ in (17), and $w(x_1, \dots, x_{24})$ in (23), a matrix $X = \begin{pmatrix} U \\ Y \end{pmatrix}$ satisfies $\pi(XJX^T) = \pi(A_0)$ if and only if $XJX^T - A_0 \in K$. Expanding the block product

$$XJX^T - A_0 = \begin{pmatrix} UJU^T - J & UJY^T \\ YJU^T & YJY^T \end{pmatrix}$$

and comparing with the block structure of K in (11), we see that $XJX^T - A_0 \in K$ is equivalent to the following three matrix equations

$$UJU^T = J, \quad UJY^T = C(z) \quad (z \in H^{12}), \quad YJY^T = 0. \quad (25)$$

The first equation $UJU^T = J$ implies $U \in \mathrm{Sp}_{24}(2) \leq \mathrm{GL}_{24}(\mathbb{F}_2)$. For each fixed $U \in \mathrm{Sp}_{24}(2)$ and each $z \in H^{12}$, the second equation $UJY^T = C(z)$ has the unique solution

$$Y^T = J^{-1}U^{-1}C(z) = JU^{-1}C(z) \iff Y = C(z)^T U^{-T} J, \quad (26)$$

since $J^{-1} = J = J^T$. Substituting (26) into the third equation of (25) then gives

$$\begin{aligned} YJY^T &= (C(z)^T U^{-T} J) J (JU^{-1} C(z)) \\ &= C(z)^T (U^{-T} J U^{-1}) C(z) = C(z)^T J C(z), \end{aligned}$$

where we used $J^3 = J$. Thus $YJY^T = 0$ holds if and only if $C(z)^T J C(z) = 0$. Thus the map (24) is a bijection, with inverse given by the formulas above. $\square$

For completeness, we record the classical order formula for $\mathrm{Sp}_{2m}(2)$.

Lemma 5.2. *For every integer $m \geq 1$, the symplectic group $\mathrm{Sp}_{2m}(2)$ has order*

$$|\mathrm{Sp}_{2m}(2)| = 2^{m^2} \prod_{j=1}^m (2^{2j} - 1).$$

Proof. See [Tay92, p. 70]. $\square$

We can now complete the proof of (4) and (5) in Theorem 1.1 for $p = 2$.

Proof of Theorem 1.1 for $p = 2$. A tuple $(x_1, \dots, x_{24}) \in G^{24}$ with $x_i = (v_i, a_i) \in D \times W$ satisfies $w(x_1, \dots, x_{24}) = g$ if and only if its matrix of D -coordinates $X = \begin{pmatrix} U \\ Y \end{pmatrix}$ satisfies $\pi(XJX^T) = \pi(A_0)$, while the twenty-four coordinates $(a_1, \dots, a_{24}) \in W^{24}$ are completely unrestricted. Combining Proposition 5.1, Lemma 4.1, and Lemma 5.2 (for $m = 12$) with $|W| = 2^{463}$ from (12), we obtain

$$\begin{aligned} N_{w,G}(g) &= |W|^{24} \cdot |\{z \in H^{12} : C(z)^T J C(z) = 0\}| \cdot |\mathrm{Sp}_{24}(2)| \\ &= 2^{24 \cdot 463} \cdot 2^{42} \cdot 2^{144} \prod_{j=1}^{12} (2^{2j} - 1). \end{aligned}$$

Summing the powers of 2 in the prefactor gives

$$24 \cdot 463 + 42 + 144 = 11112 + 186 = 11298,$$

which proves (4). Since $|G|^{23} = (2^{498})^{23} = 2^{11454}$ and $\sum_{j=1}^{12} 2j = 156$, we have

$$N_{w,G}(g) = 2^{11298+156} \prod_{j=1}^{12} (1 - 2^{-2j}) = |G|^{23} \prod_{j=1}^{12} (1 - 2^{-2j}).$$

Because $0 < 1 - 2^{-2j} < 1$ for every $1 \leq j \leq 12$, the product is strictly less than 1, proving $N_{w,G}(g) < |G|^{23}$ in (5). Together with the explicit witness (18), this establishes that G and w form a counterexample to the Amit–Ashurst conjecture (2). $\square$

The proof for odd primes is similar to the case $p = 2$, with slight changes to the construction. We briefly give the details.

Proof of Theorem 1.1 for odd p . Let p be an odd prime and choose a nonsquare $d \in \mathbb{F}_p^\times$. Use $H = \mathbb{F}_p^{11}$, $P = \mathbb{F}_p^{24}$, $D = P \oplus H$, and the same shift T as in (6). In this proof, write

$$\mathrm{Alt}_n = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{F}_p) : A^T = -A, A_{ii} = 0\}, \quad J = \begin{pmatrix} 0 & I_{12} \\ -I_{12} & 0 \end{pmatrix},$$

and identify $u \wedge v$ with $uv^T - vu^T$. For $z \in H^{12}$, define $C(z)$ by

$$\begin{aligned} C(z)_{2s-1,*} &= z_{s,1}^T, & C(z)_{2s,*} &= z_{s,2}^T, \\ C(z)_{12+2s-1,*} &= (T^s z_{s,1})^T, & C(z)_{12+2s,*} &= -d(T^s z_{s,2})^T \end{aligned} \quad (1 \leq s \leq 6).$$

Set

$$K = \left\{ \begin{pmatrix} 0 & C(z) \\ -C(z)^T & 0 \end{pmatrix} : z \in H^{12} \right\}, \quad W = \mathrm{Alt}_{35} / K,$$

and let $\pi : \mathrm{Alt}_{35} \rightarrow W$ be the quotient map. As before, $\dim K = 132$ and $\dim W = 463$. Define $G_p = D \times W$ by

$$(v, a)(u, b) = \left(v + u, a + b + \frac{1}{2}\pi(vu^T - uv^T) \right),$$

where $1/2$ is the inverse of 2 in $\mathbb{F}_p$. The bilinearity of $(v, u) \mapsto \pi(vu^T - uv^T)$ implies that the multiplication is associative, and

$$(v, a)^{-1} = (-v, -a), \quad (v, a)^k = (kv, ka), \quad [(v, a), (u, b)] = (0, \pi(vu^T - uv^T)).$$

Thus $|G_p| = p^{498}$, $G'_p = \{0\} \times W \leq Z(G_p)$, $\mathrm{cl}(G_p) = 2$, and $\exp(G_p) = p$.

Expanding $C(z)^T J C(z)$ gives

$$C(z)^T J C(z) = \sum_{s=1}^6 (z_{s,1} \wedge T^s z_{s,1} - dz_{s,2} \wedge T^s z_{s,2}).$$

In the proof of Lemma 4.1, the lowest-degree coefficient is now $c_1^2 - dc_2^2$, which is nonzero whenever $(c_1, c_2) \neq (0, 0)$. The corresponding basis wedges remain pairwise distinct. Hence

$$C(z)^T J C(z) = 0 \iff z_{s,1}, z_{s,2} \in \ker T^s \quad (1 \leq s \leq 6), \quad |\{z : C(z)^T J C(z) = 0\}| = p^{42}.$$

Put $A_0 = \begin{pmatrix} J & 0 \\ 0 & 0 \end{pmatrix}$ and $g_p = (0, \pi A_0)$. The tuple (18), interpreted over $\mathbb{F}_p$, shows that $g_p \in w(G_p) \setminus \{1\}$. Define $\mathrm{Sp}_{24}(p) = \{U \in \mathrm{GL}_{24}(\mathbb{F}_p) : UJU^T = J\}$. Since $J^T = J^{-1} = -J$ and $UJU^T = J$, the block equations give

$$UJY^T = C(z) \iff Y = C(z)^T U^{-T} J, \quad YJY^T = C(z)^T JC(z).$$

Proposition 5.1 therefore applies with $\mathrm{Sp}_{24}(p)$ in place of $\mathrm{Sp}_{24}(2)$, with the same inverse formulas. Using $|\mathrm{Sp}_{24}(p)| = p^{144} \prod_{j=1}^{12} (p^{2j} - 1)$ [Tay92, p. 70], we obtain

$$\begin{aligned} N_{w,G_p}(g_p) &= p^{24 \cdot 463 + 42 + 144} \prod_{j=1}^{12} (p^{2j} - 1) \\ &= |G_p|^{23} \prod_{j=1}^{12} (1 - p^{-2j}) < |G_p|^{23}. \end{aligned} \quad \square$$

Remark 5.3. The dimensions are chosen by balancing the powers of p in the normalized fibre size. More generally, take $k \geq 1$ pairs of parameter vectors, $\dim P = 4k$, and $\dim H = n \geq k$, with the shift $Te_i = e_{i+1}$ for $0 \leq i < n-1$ and $Te_{n-1} = 0$ on the standard basis of H . The same construction, using $T, \dots, T^k$ and the product of $2k$ disjoint commutators, gives

$$\dim D = 4k + n, \quad \dim W = \binom{4k + n}{2} - 2kn,$$

and the same count yields

$$\frac{N_{w,G}(g)}{|G|^{4k-1}} = p^{\Delta(k,n)} \prod_{j=1}^{2k} (1 - p^{-2j}), \quad \Delta(k,n) = \frac{n^2 - (4k-1)n + 2k^2 + 10k}{2}.$$

The condition $\Delta(k,n) \leq 0$ requires $8k(k-6) + 1 \geq 0$, so $k \geq 6$. For $k = 6$, it becomes $(n-11)(n-12) \leq 0$. Choosing the smaller integer solution $n = 11$ gives $\dim D = 35$, $\dim W = 463$, and $|G| = p^{498}$.

Remark 5.4. Theorem 1.1 does not give a counterexample to the original Amit conjecture (1). For every prime p , the constructed group G has nilpotency class two, so [Lev11, IS17] give

$$N_{w,G}(1_G) \geq |G|^{23}.$$

The counterexample to the Amit–Ashurst conjecture (2) occurs at the nonidentity value g .

Acknowledgements. This research was conducted in collaboration with large language model AI systems, which assisted in exploring proof strategies, refining proofs, verifying calculations, and identifying relevant literature. All contents are verified and finalized by the authors, who take full responsibility.

REFERENCES

- [Ab06] M. Abért, *On the probability of satisfying a word in a group*, J. Group Theory **9** (2006), no. 5, 685–694.
- [Ash12] C. Ashurst, *Fibres of words in finite groups, a probabilistic approach*, Ph.D. thesis, University of Bath, Bath, 2012.
- [Bae38] R. Baer, *Groups with abelian central quotient group*, Trans. Amer. Math. Soc. **44** (1938), no. 3, 357–386.
- [CCT23] R. D. Camina, W. L. Cocke, and A. Thillaisundaram, *The Amit–Ashurst conjecture for finite metacyclic p -groups*, Eur. J. Math. **9** (2023), no. 3, Paper No. 46, 13 pp.
- [CIT20] R. D. Camina, A. Iñiguez, and A. Thillaisundaram, *Word problems for finite nilpotent groups*, Arch. Math. (Basel) **115** (2020), no. 6, 599–609.
- [IS17] A. Iñiguez and J. Sangroniz, *Words and characters in finite p -groups*, J. Algebra **485** (2017), 230–246.
- [KK24] H. Kishnani and A. Kulshrestha, *Automorphic word maps and the Amit–Ashurst conjecture*, J. Group Theory **27** (2024), no. 5, 1007–1023.
- [Lev11] M. Levy, *On the probability of satisfying a word in nilpotent groups of class 2*, arXiv:1101.4286 [math.GR], 2011.
- [NS07] N. Nikolov and D. Segal, *A characterization of finite soluble groups*, Bull. Lond. Math. Soc. **39** (2007), no. 2, 209–213.

- [PY07] J. Pakianathan and E. Yalçın, *Quadratic maps and Bockstein closed group extensions*, Trans. Amer. Math. Soc. **359** (2007), no. 12, 6079–6110.
- [Rob96] D. J. S. Robinson, *A Course in the Theory of Groups*, 2nd ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.
- [Sol69] L. Solomon, *The solution of equations in groups*, Arch. Math. (Basel) **20** (1969), no. 3, 241–247.
- [Tay92] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

SHIHAO WANG, QIUZHEN COLLEGE, TSINGHUA UNIVERSITY, BEIJING, CHINA

Email address: wangshihao25@mails.tsinghua.edu.cn

ZHIWEI ZHENG, YAU MATHEMATICAL SCIENCES CENTER, TSINGHUA UNIVERSITY, BEIJING, CHINA

Email address: zhengzhiwei@mail.tsinghua.edu.cn