An upper bound for the nonsolvable length of a finite group in terms of its shortest law

Francesco Fumagalli1 | Felix Leinen2 | Orazio Puglisi1

1Dipartimento di Matematica e Informatica ‘U. Dini’, Università di Firenze, Firenze, Italy
2Institute of Mathematics, Johannes Gutenberg-University, Mainz, Germany

Correspondence
Felix Leinen, Institute of Mathematics, Johannes Gutenberg-University, Mainz, D-55099, Germany.
Email: Leinen@uni-mainz.de

Abstract
Every finite group $G$ has a normal series each of whose factors is either a solvable group or a direct product of non-abelian simple groups. The minimum number of nonsolvable factors, attained on all possible such series in $G$, is called the nonsolvable length $\lambda(G)$ of $G$. In the present paper, we prove a theorem about permutation representations of groups of fixed nonsolvable length. As a consequence, we show that in a finite group of nonsolvable length at least $n$, no nontrivial word of length at most $n$ (in any number of variables) can be a law. This result is then used to give a bound on $\lambda(G)$ in terms of the length of the shortest law of $G$, thus confirming a conjecture of Larsen. Moreover, we give a positive answer to a problem raised by Khukhro and Larsen concerning the non-2-solvable length of finite groups.

MSC 2020
20F22, 20B05, 20D99 (primary)

1 | INTRODUCTION

Let $F_\infty$ be the free group of countably infinite rank, with free generators $x_i$ $(i \in \mathbb{N})$. Consider a word $w = w(x_1, \ldots, x_k) \in F_\infty$. For any group $G$, the map $\phi_w : G^k \rightarrow G$, defined by $\phi_w(g_1, \ldots, g_k) = w(g_1, \ldots, g_k)$, is called the word map induced by $w$. The verbal subgroup $w(G)$ of $G$ is generated by the image of $\phi_w$. The word $w$ is said to be a law in $G$, when $w(G) = 1$.
In recent years, quite a large number of papers was devoted to questions related to word maps, leading to an impressive series of deep results. Particularly remarkable achievements were the proof of Ore’s conjecture (see [13]), that every element in a finite nonabelian simple group is a commutator, and a series of results on Waring type problems (see [10] and [11]). The interested reader should consult the survey [15] by Shalev and its extensive bibliography in order to get a clear picture of the research in this area.

Given a word \( w \) and a group \( G \), one may ask under which circumstances \( w \) is not a law in \( G \): Which properties of \( G \) ensure that \( w(G) \neq 1 \)? One of the first results in this direction is contained in [8]: Given a nontrivial word \( w \), there exist only a finite number of finite nonabelian simple groups, which admit \( w \) as a law. In other words, for every nontrivial \( w \), there exists a natural number \( N = N(w) \) such that the verbal subgroup \( w(S) \) of any finite nonabelian simple group \( S \) of order larger than \( N \) is nontrivial.

Properties of word maps in arbitrary finite groups have been investigated in [2]: In particular, for certain words \( w = w(x_1, ..., x_k) \in F_\infty \), the nonsolvable length \( \lambda(G) \) of \( G \) (see above abstract) can be bounded in terms of the sizes of the fibers of the verbal map \( \phi_w : G^k \longrightarrow G \). This provides evidence in favor of the following conjecture of Michael Larsen (see [2, Conjecture 1.6]).

**Conjecture.** There exists a function \( g : \mathbb{N} \longrightarrow \mathbb{N} \) such that \( \lambda(G) \leq g(\nu(G)) \) for every finite group \( G \). Here,

\[
\nu(G) = \min \left\{ |w| \mid w \text{ is a nontrivial reduced law in } G \right\},
\]

where \( |w| \) denotes the length of the reduced word \( w \in F_\infty \).

In the present paper, we shall confirm this conjecture in the following form.

**Theorem A.** Let \( G \) be any finite group. Then \( \lambda(G) < \nu(G) \).

Our bound on the nonsolvable length can probably be improved: At least when \( w \) is not a commutator word, we can use [6, Proposition 5.10] in order to see that the nonsolvable length \( \lambda(G) \) is bounded by \( \log_2(|w|) \). This argument uses the fact that a law of the form \( x_1^n \bar{w} \) with \( \bar{w} \in F_\infty' \) always implies the law \( x_1^n \).

This observation encourages us to set up the following conjecture.

**Conjecture.** The nonsolvable length of any finite group \( G \) can be bounded by a function in \( O(\log(\nu(G))) \).

We shall obtain Theorem A as a consequence of the following main result.

**Theorem B.** Let \( G \) be a finite group of nonsolvable length \( \lambda(G) = n \). Then, for every nontrivial word \( w = w(x_1, ..., x_k) \in F_\infty \) of length at most \( n \), there exists \( \bar{\tau} = (g_1, ..., g_k) \in G^k \) such that \( w(\bar{\tau}) = w(g_1, ..., g_k) \neq 1 \).

When proving Theorem B, one realizes immediately that a detailed knowledge of the action of the group on the components of certain nonabelian composition factors is needed. For this reason, we shall derive Theorem B from a result about permutation representations of groups of fixed nonsolvable length, which might be of interest in its own right.
In order to formulate this result, we introduce some further notation. Let \( w = y_1y_2 \cdots y_n \) (with \( y_i \in \{ x^\pm 1_1, \ldots, x^\pm 1_k \} \)) be a reduced word in \( F_\infty \). Then we shall need to consider its partial subwords, namely the words \( w_i = y_1y_2 \cdots y_i \) for \( 0 \leq i \leq n \) (where \( w_0 = 1 \)).

**Definition 1.** Let \( G \) be a finite group acting faithfully on the set \( \Omega \).

We say that \( G \) satisfies property \( \mathcal{P}_n \) in its action on \( \Omega \) (and write \( G \in \mathcal{P}_n(\Omega) \)), if for every nontrivial reduced word \( w = w(x_1, \ldots, x_k) \in F_\infty \) of length \( n \), there exist \( \omega \in \Omega \) and \( \bar{g} \in G^k \), such that the sequence \( \{ \omega w_i(\bar{g}) \}_{i=0}^n \) consists of \( n + 1 \) distinct elements in \( \Omega \).

We write \( G \in \mathcal{P}_n \) whenever \( G \in \mathcal{P}_n(\Omega) \) for every faithful \( G \)-set \( \Omega \).

Clearly, if \( G \in \mathcal{P}_n(\Omega) \) for some faithful \( G \)-set \( \Omega \), then \( w(G) \neq 1 \) for every nontrivial reduced word \( w \) of length at most \( n \). However, this property is much stronger than the nontriviality of \( w(G) \). Indeed, when \( G \in \mathcal{P}_n(\Omega) \), it is possible to find some \( \bar{g} \in G^k \) such that all the elements \( w_1(\bar{g}), w_2(\bar{g}), \ldots, w_n(\bar{g}) = w(\bar{g}) \) are nontrivial and pairwise distinct.

**Theorem B** will be a consequence of the following result.

**Theorem C.** Let \( G \) be a finite group with \( \lambda(G) = n \), and let \( \Omega \) be a faithful transitive \( G \)-set. Then, for every \( \omega \in \Omega \) and for every nontrivial reduced word \( w = w(x_1, \ldots, x_k) \in F_\infty \) of length \( n \), there exists a Sylow 2-subgroup \( P \) of \( G \) and a tuple \( \bar{g} \in p^k \) such that the points \( \omega w_0(\bar{g}), \omega w_1(\bar{g}), \ldots, \omega w_n(\bar{g}) \) are pairwise distinct. In particular, \( G \in \mathcal{P}_n \).

Theorem C says: If \( G \) has nonsolvable length \( n \), and if \( H \) is a core-free subgroup of \( G \), then for every nontrivial word \( w = w(x_1, \ldots, x_k) \) of length \( n \) there exists a \( k \)-tuple \( \bar{g} \) of elements from a Sylow 2-subgroup of \( G \) such that the cosets
\[
H, \; Hw_1(\bar{g}), \; \ldots, \; Hw_{n-1}(\bar{g}), \; Hw_n(\bar{g}) = Hw(\bar{g})
\]
are pairwise distinct.

The proof of Theorem C relies heavily on the existence of so called rarefied subgroups. In [6, Theorem 1.1], it has been proved that every finite group of nonsolvable length \( m \) contains \( m \)-rarefied subgroups. These are subgroups of the same nonsolvable length \( m \), with a very restricted structure. In particular, the nonabelian composition factors of an \( m \)-rarefied group belong to the class
\[
\mathcal{L} = \{ L_2(2^r), L_2(3^r), L_2(p^{2a}), L_3(3), \; 2B_2(2^r) \mid p, r \text{ odd primes, } a \in \mathbb{N} \}.
\]

The precise definition of \( m \)-rarefied groups will be given in Section 3.

In proving Theorem C, we shall reduce ourselves to the case of rarefied groups and then use the constraints on the structure of such groups in order to complete the proof. The proof of Theorem C depends on the classification of finite simple groups.

We finally note that Theorem C partly solves a question of Evgenii Khukhro and Pavel Shumyatsky. They have shown in [9, Theorem 1.1], that the nonsolvable length of any finite group \( G \) is bounded by \( 2L_2(G) + 1 \), where \( L_2(G) \) denotes the maximum of the 2-lengths of the solvable subgroups of \( G \). This bound was improved in [6, Theorem 5.2] to \( L_2(G) \). In this context, Khukhro and Shumyatsky raised the following question [9, Problem 1.3].
Problem. For a given prime $p$ and a given proper group varity $\mathfrak{B}$, is there a bound for the non-$p$-solvable length of finite groups whose Sylow $p$-subgroups belong to $\mathfrak{B}$?

Theorem C gives an affirmative answer in the case when $p = 2$.

2 PRELIMINARIES ON GROUP ACTIONS AND WORDS

Consider any nontrivial reduced word $w = w(x_1, \ldots, x_k) \in F_\infty$ of length $n$. Let $w = y_1 \cdots y_n$ with $y_j = x_j^{\varepsilon_j}$ and $\varepsilon_j \in \{\pm 1\}$ for all $j$. As before, we let $w_0 = 1$ and

$$w_j = y_0 \cdots y_j \quad \text{and} \quad \tilde{w}_j = \begin{cases} w_j^{-1} & \text{if } \varepsilon_j = -1 \\ w_{j-1}^{-1} & \text{if } \varepsilon_j = +1 \end{cases}$$

for $1 \leq j \leq n$.

For $k$-tuples $\overline{g} = (g_1, \ldots, g_k)$ and $\overline{h} = (h_1, \ldots, h_k)$ of elements in a group $G$, we let $\overline{g} \overline{h} = (g_1 h_1, \ldots, g_k h_k)$.

The proof of the following lemma is straightforward (see [12, Lemma 2.1]).

**Lemma 1.** Let $N \vartriangleleft G$. Consider $\overline{g} \in G^k$ and $\overline{b} \in N^k$. Then, in the above notation, $w(\overline{b} \overline{g}) = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} w(\overline{g}) \in N w(\overline{g})$ with $a_j = (b_j)^{\varepsilon_j}(\overline{g})$ for all $j$.

The following situation will come up several times in the course of our analysis: A normal subgroup of a finite group $G$ is a direct product of subgroups $M_i (0 \leq i \leq m)$, which are all isomorphic to a certain group $M$ and which are permuted transitively under the conjugation with elements from $G$.

**Lemma 2.** In the above situation, let $H = N_G(M_0)$ and $\tilde{M}_0 = \prod_{i \neq 0} M_i$. Suppose, that $\mathbb{F}$ is a field and $W$ is an irreducible $\mathbb{F}H$-module satisfying $[W, M_0] \neq 0$ and $[W, \tilde{M}_0] = 0$. Then the induced $\mathbb{F}G$-module $V = \text{Ind}_H^G(W)$ is irreducible.

**Proof.** Let $T$ be a transversal to $H$ in $G$ containing 1. Then

$$V = \text{Ind}_H^G(W) = W \otimes_H \mathbb{F}G = \bigoplus_{t \in T} (W \otimes_H t)$$

and each of the subspaces $W_t = W \otimes_H t (t \in T)$ is a $G$-block. If $i \in \{0, 1, \ldots, m\}$ and $t \in T$, then $[W_t, M_i] = 0$ whenever $M_i \neq M_0, t$. The subgroup $M_0$ has trivial centralizer in $W_1$, because $W$ is an irreducible $H$-module, $M_0$ is normal in $H$ and acts nontrivially on $W$. If $U$ is a $G$-submodule of $V$ and $u \in U$ is a nontrivial element, write $u = \sum_{t \in T} u_t$, with $u_t \in W_t$ for all $t \in T$. Without loss of generality, we may assume that $u_1 \neq 0$ and pick $x \in M_0$ not centralizing $u_1$. Then $[u, x] = u_1 (x - 1)$ is still in $U$, hence $U \cap W_1 \neq 0$. Since $U \cap W_1$ is an $H$-module, it must be the whole $W_1$. Once we know that $W_1 \leq U$ we immediately deduce $U = V$. \qed

The following lemma generalizes an idea from [1].
Lemma 3. Let $G, H, W$ and $V$ be as in Lemma 2 and adopt the notation introduced in its proof. In particular, $T$ denotes a transversal to $H$ in $G$ with $1 \in T$. Suppose, that the subgroup $A_0$ of $M_0$ satisfies $[W, A_0] \neq 0$. Let

$$M^* = \prod_{t \in T} M_0^t \quad \text{and} \quad A^* = \prod_{t \in T} A_0^t.$$  

Suppose further that $w = y_1 \cdots y_n$ is a nontrivial reduced $k$-variable word of length $n$, and that there exists some $\bar{g} \in (N_G(A^*))^k$ such that the groups $M_0^{w_j(\bar{g})}$ ($0 \leq j \leq n-1$) are pairwise distinct factors of the above direct product $M^*$.

Then, for every nontrivial $z \in W$, there exist $u \in \langle zH \rangle$ and $\bar{b} \in (A^*)^k$ such that the $n+1$ elements

$$(u \otimes 1)w_j(\bar{b} \bar{g}) \quad (0 \leq j \leq n)$$

are pairwise distinct elements of $V = W \otimes_H \mathbb{C}G$. Here, the number of choices for $\bar{b}$ is at least $|A^*|^k / |A_0|$.

Proof. For convenience of notation, we let $T = \{t_0, \ldots, t_m\}$ with $t_0 = 1$ and $M_i = M_0^{t_i}$ and $A_i = A_0^{t_i}$ for all $i$. Without loss we may assume that $A_0^{w_j(\bar{g})} = A_j$ for $0 \leq j \leq n-1$. Clearly, $A_j$ acts nontrivially on the block $W_i = W \otimes t_i$ if and only if $i = j$.

Suppose first that $A_0^{w_n(\bar{g})} \neq A_j$ for $0 \leq j \leq n-1$. Then, for every $u \in W_1$, the vectors $(u \otimes 1)w_j(\bar{g})$ ($0 \leq j \leq n$) belong to pairwise different blocks and are, therefore, all distinct. In this situation, any $k$-tuple $\bar{b} \in (A^*)^k$ gives rise to a sequence $\{(u \otimes 1)w_j(\bar{b} \bar{g})\}_{j=0}^n$ with $n+1$ distinct elements. Since the number of such tuples $\bar{b}$ is $|A^*|^k$, the claim holds.

Suppose next that there exists some $\ell \in \{0, \ldots n-1\}$ such that

$$A_0^{w_n(\bar{g})} = A_0^{w_{\ell}(\bar{g})} = A_\ell.$$  

Modulo application of a suitable Nielsen transformation to the variables $x_1, \ldots, x_k$, we may assume without loss that $y_n = x_\ell$ is the last letter occurring in the word $w$. We focus our attention on the word $\mu = w_\ell^{-1}w = y_{\ell+1} \cdots y_n$ and on its partial subwords $\mu_j = w_\ell^{-1}w_{\ell+1} = y_{\ell+1} \cdots y_{\ell+j}$ for $0 \leq j \leq n-\ell$.

For every $j \in \{0, \ldots, n-\ell\}$ and every $\bar{b} \in (A^*)^k$, we define elements $f_j(\bar{b}) \in M^*$ by the equation

$$f_j(\bar{b})\mu_j(\bar{g}) = \mu_j(\bar{b} \bar{g}).$$

Each $\mu_j(\bar{g})$ is in $N_G(A^*)$ and, using Lemma 1, is readily seen that each $f_j(\bar{b})$ belongs to $A^*$. Fix any nontrivial vector $z \in W$ and consider $z \otimes t_\ell \in W_\ell = W_1 w_\ell(\bar{g})$. Choose now $b_1, \ldots, b_{k-1}$ freely in $A^*$. This choice can be done in $|A^*|^{k-1}$ different ways. The choice of $b_k$ will be described just below.

In order to express some relations in a clearer fashion, we will interpret elements $d \in M^*$ as functions $d : \{0, \ldots, m\} \rightarrow M$ with values $d[i]$ ($0 \leq i \leq m$). Note that $W_\ell \mu(\bar{g}) = W_\ell$. We need to choose $b_k \in A^*$ in such a way that $(z \otimes t_\ell)\mu(\bar{b} \bar{g}) \neq z \otimes t_\ell$. To this end, we choose $b_k$ under the only constraint that

$$(z \otimes t_\ell)\mu(\bar{b} \bar{g}) = (z \otimes t_\ell)f_{n-\ell-1}(\bar{b})\mu_{n-\ell-1}(\bar{g})(b_k g_k) \neq z \otimes t_\ell. \quad (1)$$
Note that
\[(z \otimes t_\ell) f_{n-\ell-1}(b) \mu_{n-\ell-1}(g)(b_k g_k) = (z \otimes t_\ell) f_{n-\ell-1}(b)b^{\mu_{n-\ell-1}(g)-1}_k \mu(g)\]
\[= z(f_{n-\ell-1}(b)b^{\mu_{n-\ell-1}(g)-1}_k)[\ell] \otimes t_\ell \mu(g)\]
\[= v \otimes t_\ell,\]
where \(v = zf_{n-\ell-1}(b)[\ell](b_k g_k)\). For suitable \(r \in H\) and the elements \((u \otimes 1)w_0(b \bar{g}), \ldots, (u \otimes 1)w_n(b \bar{g})\) are all distinct for \(u = zr\). Because the element \(b_k\) could be chosen freely in all but one of its components, the possible choices for \(b_k\) are at least \(|A^*|/|A_0|\), hence the possible choices for the \(k\)-tuples \(\bar{b}\) satisfying the requirements of the Lemma are at least \(|A^*|^k/|A_0|\).

Lemma 4. Let \(G \leq \text{Sym}(\Omega)\) be a finite transitive group with a nontrivial normal subgroup \(M^* = \prod_{i=0}^m M_i\), where the subgroups \(M_i\) are permuted transitively by \(G\) under the action by conjugation. Suppose that \(\omega \in \Omega\), and let \(R\) be a subgroup of \(H = N_G(M_0)\) containing \((G_\omega \cap H)\bar{M}_0\), where \(\bar{M}_0 = \prod_{i \neq 0} M_i\).

We will also need the following fact.
If \( W \) is an irreducible constituent of \( \text{Ind}_R^H(\mathbb{C}) \), on which \( M_0 \) acts non-trivially, then \( \mathbb{C} \Omega \) has a submodule isomorphic to \( V = \text{Ind}_R^G(W) \).

**Proof.** The module \( V = \text{Ind}_R^G(W) \) is irreducible by Lemma 2. Therefore, it suffices to show that \( \text{Hom}_G(\mathbb{C} \Omega, V) \neq 0 \). Frobenius reciprocity [4, Theorem 10.8] gives

\[
\text{Hom}_G(\mathbb{C} \Omega, V) \cong \text{Hom}_G(\mathbb{C}, V) \cong C_V(G_\omega) \cong \text{Hom}_G(V, \mathbb{C}).
\]

In particular, we only need to show that \( \text{Hom}_G(V, \mathbb{C}) \neq 0 \).

The \( G \)-module \( V \) is itself an induced module. Therefore, by application of Mackey’s theorem [4, Theorem 10.13], the \( G_\omega \)-module \( V \) contains \( \text{Ind}_{H_\omega}^{G_\omega}(W) \) as a direct summand. Hence it suffices to show that \( \text{Hom}_{G_\omega}(\text{Ind}_{H_\omega}^{G_\omega}(W), \mathbb{C}) \neq 0 \).

Note that \( H_\omega \leq R \), and that the \( H \)-module \( W \) is a submodule of \( \text{Ind}_R^H(\mathbb{C}) \) by hypothesis. Together with two further applications of Frobenius reciprocity, this implies

\[
\text{Hom}_{G_\omega}(\text{Ind}_{H_\omega}^{G_\omega}(W), \mathbb{C}) \cong \text{Hom}_{H_\omega}(W, \mathbb{C}) \cong \text{Hom}_H(W, \text{Ind}_R^H(\mathbb{C})) \neq 0.
\]

\[\square\]

**Lemma 5.** Let \( G \leq \text{Sym}(\Omega) \) be a finite transitive group and \( \omega \) any point of \( \Omega \). If \( V \) is a nontrivial \( G \)-submodule of \( \mathbb{C} \Omega \) and \( \pi \) is the projection from \( \mathbb{C} \Omega \) onto \( V \), then \( (\omega)\pi \neq 0 \).

**Proof.** Write \( \mathbb{C} \Omega = V \oplus U \) with \( U \) \( G \)-invariant. If \( (\omega)\pi = 0 \), then \( \omega \in U \) and therefore \( \omega g \in U \) for every \( g \in G \). Hence, \( \Omega \subseteq U \) because \( G \) is transitive on \( \Omega \). It follows that \( U = \mathbb{C} \Omega \) and \( V = 0 \), a contradiction. \[\square\]

### 3 | \( m \)-RAREFIED GROUPS AND STRATEGY OF THE PROOF

For every finite group \( G \), we define the following characteristic subgroups.

\[
R(G) = \langle A \mid A \text{ is a normal solvable subgroup of } G \rangle.
\]

\[
S(G) = \langle B \mid B \text{ is a minimal normal nonabelian subgroup of } G \rangle.
\]

The \( RS \)-series of \( G \) is then defined recursively by

\[
\begin{align*}
R_1(G) &= R(G) \\
S_i(G)/R_i(G) &= S(G/R_i(G)), \quad \text{for } i \geq 1 \\
R_{i+1}(G)/S_i(G) &= R(G/S_i(G)), \quad \text{for } i \geq 1.
\end{align*}
\]

The series thus defined always reaches \( G \). If \( G = R_{m+1}(G) > R_m(G) \), then \( m \) is said to be the nonsolvable length of \( G \) and we write \( \lambda(G) = m \).

By [6, Theorem 1.1], every group \( G \) of nonsolvable length \( m \) has an \( m \)-rarefied subgroup, that is, a subgroup \( H \) of nonsolvable length \( m \) satisfying the following conditions.
(i) $R_i(H) = \Phi(H)$ and $R_{i+1}(H)/S_i(H) = \Phi(H/S_i(H))$ for all $i = 1, \ldots, m - 1$.

(ii) $S_i(H)/R_i(H)$ is the unique minimal normal subgroup of $H/R_i(H)$ for $1 \leq i \leq m$.

(iii) The simple components of $S_i(H)/R_i(H)$ are isomorphic to groups in the set

$$\mathcal{L} = \{L_2(2^r), L_2(3^r), L_2(p^{2a}), L_3(3), 2B_2(2^r) \mid p, r \text{ odd primes}, a \in \mathbb{N}\}$$

for $1 \leq i \leq m$.

**Lemma 6.** Let $S$ be a simple group in $\mathcal{L}$. Then $S$ contains an $\text{Aut}(S)$-invariant $S$-conjugacy class of subgroups, which are dihedral of order $2p$ for some odd prime $p$.

**Proof.** We first claim that $S$ contains a conjugacy class of (maximal) subgroups that are dihedral of order $2m$, for some odd integer $m$.

When the characteristic of $S$ is 2, choose the conjugacy class of normalizers of split-tori subgroups (diagonal subgroups) of order $q - 1$. Each of these subgroups is a dihedral group of order $2(q - 1)$ (see [7, Theorems 6.5.1 and 6.5.4]).

When $S \cong L_2(q)$, with $q = 3^r$ or $q = p^{2a}$ ($p, r$ odd primes and $a \geq 0$), then $S$ contains two conjugacy classes of maximal subgroups, which are dihedral subgroups of orders, respectively, $q - 1$ and $q + 1$. Each of these subgroups is the normalizer, respectively, of a split torus (diagonal subgroup of $S$) or of a nonsplit torus. According to the congruence class of $q$ modulo 4, take the class of subgroups having order $2m$, with $m$ odd (see [7, Theorem 6.5.1]).

When $S = L_3(3)$ the normalizers of the Sylow 13-subgroups form a conjugacy class of dihedral groups of order 26 (see [3]).

Finally, consider one of the dihedral groups $E$ in the conjugacy class just established. If $|E| = 2m$, then choose a prime $p$ dividing $m$. The group $E$ has a unique subgroup $C$ of order $p$. And if $a$ is any involution in $E$, then $D = C\langle a \rangle$ is a dihedral group of order $2p$. Since all the involutions of $E$ are conjugate in $E$, any other subgroup of $E$ of order $2p$ is conjugate to $D$. The set $\{D^g \mid g \in S\}$ is then a family of subgroups with the required properties. $\square$

Theorem C will be proved by contradiction. So assume that there exists a group $G$ with nonsolvable length $n$, such that the conclusion of Theorem C is not valid with respect to the action of $G$ on a certain faithful transitive $G$-set $\Omega$. Among all possible such counterexamples, we select a pair $(G, \Omega)$ such that $n + |G| + |\Omega|$ is minimal.

Consider an $n$-rarefied subgroup $H$ of $G$. From [6, Proposition 4.7], we obtain $\lambda(H/C_H(\Gamma)) = n$ for at least one $H$-orbit $\Gamma$ in $\Omega$. Hence, by minimal choice of $(G, \Omega)$, we have $G = H$, that is, $G$ is an $n$-rarefied group. By [6, Proposition 4.2], every proper subgroup $U$ of $G$ satisfies $\lambda(U) < n$. Hence minimality of $(G, \Omega)$ yields that every proper subgroup of $G$ has nonsolvable length strictly smaller than $n$.

4 | PROOF OF THEOREM C: REDUCTION TO THE CASE $\Phi(G) = 1$

In this section, $(G, \Omega)$ is always a minimal counterexample to Theorem C, as above. $F = \Phi(G)$ denotes the Frattini subgroup of $G$, and $L$ denotes the last term of the derived series of $S_1(G)$. Since $G$ is $n$-rarefied, $S_1(G)/F$ is the unique minimal normal subgroup in $G/F$. In particular, $S_1(G) = FL$.

**Lemma 7.** Assume that $K$ is a normal subgroup of $G$ not containing $L$. Then $K \leq F$ and $G/K$ is $n$-rarefied.
Proof. Suppose that $K \cap L$ is not contained in $F$. Then $(K \cap L)F/F$ is a nontrivial normal subgroup of $G/F$ and therefore it contains $S_1(G)/F$, the unique minimal normal subgroup of $G/F$. Thus $S_1(G) = (K \cap L)F$ and

$$L = L \cap S_1(G) = L \cap (K \cap L)F = (L \cap F)(K \cap L).$$

Since $L$ is perfect, we get $L = L' \leq (L \cap F)'(K \cap L)$. Because $L \cap F$ is nilpotent, iteration of this argument finally yields $L = K \cap L$, that is, $L \leq K$. But this contradicts the hypothesis of the Lemma. Hence $K \cap L \leq F$, and this implies that $KF/F$ centralizes $LF/F = S_1(G)/F$. On the other hand, $S_1(G)/F$ has trivial centralizer in $G/F$ (by [6, Lemma 2.4]). It follows that $K \leq F$. Hence $G/K$ is $n$-rarefied by [6, Proposition 4.2 and Lemma 4.3].

Lemma 8. If $G_\omega < H \leq G$, for some $\omega \in \Omega$, then $L \leq H_G$. Moreover, $L$ lies in the normalizer of any block system (with respect to the action of $G$ on $\Omega$).

Proof. Let $H = \{Hg \mid g \in G\}$. The translation action of $G$ on $H$ has kernel $H_G$, and $|H| < |\Omega|$. Assume that $H_G$ does not contain $L$. Then, by Lemma 7, $G/H_G$ is $n$-rarefied. And since $|G/H_G| + |H| < |G| + |\Omega|$, the group $G/H_G$ satisfies Theorem C in its action on $H$. For each $k$-variable word $w$ of length $n$ and for every $\alpha \in H$, we can thus find a Sylow 2-subgroup $Q/H_G$ and $\bar{y} \in (Q/H_G)^k$ such that $|\{aw_i(\bar{y}) \mid 0 \leq i \leq n\}| = n + 1$. Choose $\alpha = H$. Note that $Q/H_G = PH_G/H_G$ for some Sylow 2-subgroup $P$ in $G$. Let $\bar{x} \in P^k$ be a preimage to $\bar{y}$. Since the points $aw_i(\bar{x}) (0 \leq i \leq n)$ are pairwise distinct, the products $w_i(\bar{x})w_j(\bar{x})^{-1} (0 \leq i < j \leq n)$ do not lie in $H$ and not in $G_\omega$. But then the points $aw_i(\bar{x}) (0 \leq i \leq n)$ are pairwise distinct too, showing that $G$ satisfies Theorem C, a contradiction.

Let $K$ be the normalizer in $G$ of the block system $B$. Note that $KG_\omega$ is a subgroup. Assume $K = 1$. So $G$ acts faithfully on $B$ and, since $|B| < |\Omega|$, we have that $G$ satisfies the conclusion of Theorem C in its action on $B$. It follows that $G$ satisfies the conclusion of Theorem C in its action on $\Omega$, a contradiction. Now $K \neq 1$, whence $KG_\omega > G_\omega$. We conclude that $L$ is contained in the core of $KG_\omega$, which equals $K$.

Proposition 1. The Frattini subgroup $F$ of $G$ is a $p$-group for some prime $p$, and the subgroup $A = F \cap L$ is abelian.

Proof. We only need to consider the case when $F \neq 1$. Let us show first, that the centralizer $C_F(L)$ is trivial.

To this end, assume $D = C_F(L) \neq 1$. Let $K$ denote the normalizer of the block system $B$ consisting of the $D$-orbits in $\Omega$. By Lemma 8, $L \leq K$. Consider a $D$-orbit $\Delta \in B$. By [5, Theorem 4.2A], the centralizer $C$ of $D/C_D(\Delta)$ in Sym($\Delta$) is isomorphic to a section of $D/C_D(\Delta)$, hence nilpotent. Because the actions of $D$ and $L$ on $\Delta$ commute, the group $L/C_L(\Delta)$ is isomorphic to a subgroup of $C$, hence nilpotent. On the other hand, $L$ is perfect. It follows that $L = C_L(\Delta)$. Since this happens for every orbit $\Delta$, we obtain $L = 1$. But this is impossible, because $\lambda(G) = n \geq 1$. Hence, $D = 1$. It follows immediately, that the intersection $A = L \cap F$ is nontrivial.

We will show now that $A$ is a $p$-group. To this end, assume that the order of $A$ is divisible by two different primes $p$ and $q$. Recall that $A$ is a normal subgroup in $G$, because $F$ and $L$ are normal subgroups in $G$. Moreover, $A$ is nilpotent. Let $P$ resp. $Q$ be the Sylow $p$-, respectively, the Sylow $q$-subgroup of $A$. Then $P$ and $Q$ are normal subgroups of $G$. Since the stabilizer $G_\omega$ of a point $\omega \in \Omega$
has trivial core, $P$ and $Q$ cannot be contained in $G_\omega$. Application of Lemma 8 to $QG_\omega$ in the role of $H$ yields $L \leq QG_\omega$, and Dedekind’s modular law gives $A = A \cap QG_\omega = Q(G_\omega \cap A)$. It follows that $P \leq G_\omega \cap A$, a contradiction to $P \not\leq G_\omega$.

Now $A$ is a $p$-group for some prime $p$. Assume next that $F$ is not a $p$-group. Then $F$ has a nontrivial $q$-subgroup $Q$ for some prime $q \neq p$. Again, $Q$ is normal in $G$ and $QG_\omega > G_\omega$. Therefore, $L \leq QG_\omega$ and $A = F \cap L \leq F \cap QG_\omega = Q(F \cap G_\omega)$. It follows that $A \subseteq F \cap G_\omega$, a contradiction to $A \not\subseteq G_\omega$.

It remains to show that $A$ is abelian. Consider a group $B$ which is normalized by $G_\omega$ and satisfies $F_\omega \leq B \leq F$. Lemma 8 shows that $L \leq BG_\omega$, whence

$$A = L \cap BG_\omega \cap F = L \cap (G_\omega \cap F) = L \cap BF_\omega = L \cap B \leq B.$$  

Assume that there exist two distinct minimal such groups $B_1$ and $B_2$. This would imply $A \leq B_1 \cap B_2 = F_\omega \leq G_\omega$, in contradiction to $G_\omega$ having trivial core in $G$. We conclude that for each $\omega \in \Omega$, there is a unique minimal subgroup $B(\omega)$, which is normalized by $G_\omega$ and satisfies $F_\omega \leq B(\omega) \leq F$.

Because $F$ is nilpotent, the group $K(\omega) = N_F(F_\omega)$ is strictly larger than $F_\omega$. Moreover, $K(\omega)$ is normalized by $G_\omega$. Thus, $B(\omega)$ is contained in $K(\omega)$. It follows that the subgroup $A$ of $B(\omega)$ normalizes $F_\omega$ too. Now $AF_\omega$ is a subgroup of $B(\omega)$, which is normalized by $G_\omega$. Since $A$ is not contained in $F_\omega$, we obtain $AF_\omega = B(\omega)$.

The normal subgroup $V = \bigcap_{\omega \in \Omega} B(\omega)$ of $G$ contains $A$. And so it suffices to show that $V$ is abelian. Consider a maximal subgroup $M$ of $B(\omega)$ containing $F_\omega$. Because $F_\omega$ is normalized by $G_\omega$, the $G_\omega$-core $M_0 = \bigcap_{g \in G_\omega} M^g$ of $M$ contains $F_\omega$. By minimality of $B(\omega)$, we have $M_0 = F_\omega$. Since $F$ is nilpotent, the commutator subgroup $(B(\omega))'$ of $B(\omega)$ is contained in the $G_\omega$-conjugates of $M$ and hence in $M_0 = F_\omega$. It follows that $V' \leq \bigcap_{\omega \in \Omega} (B(\omega))' \leq \bigcap_{\omega \in \Omega} F_\omega = 1$.

We shall show now that the Frattini subgroup $F$ is even trivial.

**Proposition 2.** The group $G$ has trivial Frattini subgroup.

**Proof.** Assume $F \neq 1$. In the sequel, $p$ will denote the prime dividing the order of $F$ (Proposition 1). We prove first, that $L$ splits over $A = L \cap F$ and that $S_i(G)$ splits over $F$.

Let $B = \Phi(L)$, assume $B \neq 1$, and consider any $B$-orbit $\Gamma$ in $\Omega$. If $\Gamma = \Omega$ would hold, we could apply the Frattini argument to obtain $G = BG_\omega$ for every $\omega \in \Omega$. But this is clearly impossible, because $B \leq F$ and $F$ consists of nongenerators for $G$ [14, 5.2.12]. It follows that the $B$-orbits form a proper block system in the $G$-set $\Omega$. By Lemma 8, $L$ normalizes every $B$-orbit $\Gamma$. In particular, the Frattini argument yields $L = BL_\gamma$ for any point $\gamma \in \Gamma$, and this is again impossible. This contradiction shows, that $B = 1$.

Applying Proposition 1 and [14, Theorem 5.2.13], we obtain that $L$ splits over the abelian normal subgroup $A$. A complement $K$ to $A$ in $L$ is a complement to $F$ in $S_i(G)$, so that $S_i(G)$ splits over $F$ too. Because $S_i(G)/F$ is a minimal normal subgroup in $G/F$, there exists a simple group $S$ in $L$ such that $K = \prod_{i=1}^s S_i$ where each $S_i$ is a copy of $S$. In the sequel, we will distinguish the two cases when $p$ is odd and when $p = 2$, but try to treat them simultaneously.

When $p > 2$, let $R$ be any Sylow 2-subgroup of $K$. Clearly $R = \prod_{i=1}^s R_i$, where each $R_i$ is a Sylow 2-subgroup of $S_i$. When $p = 2$, Lemma 6 gives us an $\text{Aut}(S)$-invariant $S$-conjugacy class of dihedral subgroups of order $2r$ in $S$, for some odd prime $r$. Let $D_t$ denote the copy of this conjugacy class
in \( S_i \). We can now choose a subgroup \( U_i \in D_i \) for each \( i \in \{1, \ldots, \ell'\} \) and define \( U = \prod_{i=1}^{\ell'} U_i \) and \( R = \prod_{i=1}^{\ell'} R_i \) where \( R_i \) is the Sylow \( r \)-subgroup in \( U_i \).

**Next step.** Our next aim is to show that if \( R \leq G_\omega \), then \( K \leq G_\omega \).

Assume by way of contradiction that \( R \leq G_\omega \) and \( S_i \not\leq G_\omega \) for some \( i \). Without loss, \( i = 1 \). Because the simple group \( S_1 \) is generated by the conjugates of \( R_1 \) in \( S_1 \), there exists \( s_1 \in S_1 \) such that \( R_1 s_1 \not\leq G_\omega \). Let \( Q = R_1^{s_1} \) and \( Q_i = R_i^{s_1} \) for all \( i \). Clearly, \( Q_i = R_i \) when \( i \neq 1 \). Therefore, \( Q_i \leq G_\omega \) if and only if \( i \neq 1 \). When \( p = 2 \), we also let \( D = U^{s_1} \) and \( D_i = U_i^{s_1} \) for all \( i \).

In the case when \( p > 2 \), an application of the Frattini argument within the group \( G/F \) yields \( G/F = (S_1(G)/F)(Y/F) \), where \( Y/F \) denotes the normalizer of the Sylow 2-subgroup \( Q_F/F \) in \( G/F \). For every \( y \in Y \), the Sylow 2-subgroup \( Q_y \) of \( Q_F \) is conjugate to \( Q \) by a suitable element \( f \in F \), and \( yf^{-1} \in N_G(Q) \). This shows that \( G = S_1(G)X \) for \( X = N_G(Q) \).

In the case when \( p = 2 \), the \( G \)-conjugates of \( D_F/F \) are conjugate in \( S_1(G)/F \). Therefore, the Frattini argument yields \( G = S_1(G)N_G(D_F) \). Because \( Q \) is a Sylow \( r \)-subgroup of \( D_F \), it is possible to apply the Frattini argument again. It follows that \( N_G(D_F) = F_D X \), where \( X = N_G(D_F)(Q) \geq D \).

**Conclusion:** \( G = S_1(G)X \) where
\[
\begin{cases}
  X = N_G(Q) & \text{for } p > 2 \\
  X = N_G(Q) \cap N_G(D_F) & \text{for } p = 2.
\end{cases}
\]

Since \( S_1(G)/F \) is minimal normal in \( G/F \), the factorization \( G = S_1(G)X \) entails that \( X \) acts transitively on the set \( \{S_iF \mid i = 1, \ldots, \ell'\} \) by conjugation. Consider \( x \in X \) and indices \( i, j \) such that \( (S_iF)_x = S_jF \). Then \( Q_i^x \leq Q \cap S_jF \leq K \cap S_jF = S_j(K \cap F) = S_j \), whence \( Q_i^x \leq Q \cap S_j = Q_j \). This shows that \( X \) also acts transitively on the set \( \{Q_i \mid i = 1, \ldots, \ell'\} \) by conjugation. The group \( X/(X \cap S_1(G)) \) is \((n-1)\)-rarefied, because it is isomorphic to \( G/S_1(G) \). Moreover, \( X < G \), because \( Q \) is not normal in \( G \). Altogether, \( \lambda(X) = n-1 \).

Consider \( X_1 = N_X(Q_1) \) as the stabilizer of \( Q_1 \) under the conjugation action of \( X \) on \( \{Q_i \mid i = 1, \ldots, \ell'\} \). In the case when \( p > 2 \), we let \( Z = X_1 \cap X_\omega \). Clearly, \( Q_1 \not\leq Z \) because \( Q_1 \not\leq X_\omega \). In the case when \( p = 2 \), we let \( Z = (X_1 \cap X_\omega)(F \cap X) \). In order to see that \( Z \) does not contain \( Q_1 \) also in this case, we argue by contradiction: Assume \( Q_1 \leq Z \). Then
\[
\omega Q_1 \subseteq \omega Z = \omega(X_1 \cap X_\omega)(F \cap X) = \omega(F \cap X).
\]

The group \( X \cap F \) centralizes \( Q \), because \( [Q, X \cap F] \leq Q \cap F = 1 \). Therefore, \( Q_1 \) is normal in \( Z \) and \( \omega Q_1 \) is a block under the action of \( Z \) on \( \omega Z \). It follows that \( r = |\omega Q_1| \) divides \( |\omega(F \cap X)| = |(F \cap X) : (F \cap X_\omega)| \). But the latter is a power of 2, a contradiction.

We have now shown that \( Q_1 \not\leq Z \) in all cases.

However, \( Z \) contains the normal subgroup \( \tilde{Q}_1 = \prod_{i=2}^{\ell'} Q_i \) of \( X_1 \). Hence we can choose an irreducible constituent \( W \) of the \( \mathbb{C}X_1 \)-module \( \text{Ind}^{X_1}_{X_1}(\mathbb{C}) \), on which \( Q_1 \) acts nontrivially. Note that \( \tilde{Q}_1 \) acts trivially on \( W \), because it acts trivially on the whole \( \text{Ind}^{X_1}_{X_1}(\mathbb{C}) \). Since the normal subgroup \( Q_1 \) of \( X_1 \) acts nontrivially on \( W \), its fixed point space \( C_W(Q_1) \) is a proper \( X_1 \)-submodule of \( W \), whence \( C_W(Q_1) = 0 \). We choose a right transversal \( T = \{t_1, t_2, \ldots, t_r\} \) of \( X_1 \) in \( X \) such that \( t_1 = 1 \) and \( Q_1 t_i = Q_1 \) for all \( i \). Then \( V = \text{Ind}^{X_1}_{X_1}(W) = \bigoplus_{i=1}^{\ell'} (W \otimes X_1 t_i) \). We apply Lemma 2 with \( X, X_1, Q, Q_1 \) in the roles of \( G, H, M^* = \langle M_0^* \rangle, M_0 \) (respectively) and obtain, that \( V \) is an
irreducible $\mathbb{C}X$-module. The subspaces $W_i = W \otimes_{t_i} t_i$ are blocks under the action of $X$, and each factor $Q_i$ acts nontrivially only on $W_i$. Note that $C_W(Q_i) = 0$ entails $C_W(Q_i) = 0$ for all $i$.

Let $\Gamma = \omega X$ and consider the permutation module $\mathbb{C} \Gamma$. We apply Lemma 4 with $X, X_1, Z, Q, Q_1$ in the roles of $G, H, R, M^*, M_0$ (respectively). Note that the hypotheses of the lemma are satisfied, because $(G_\omega \cap X_1)\hat{Q}_1 \leq X_\omega \cap X_1 \leq Z$. It follows that $\mathbb{C} \Gamma$ contains $V$ as a direct summand.

Consider the image $v = \sum_{i=1}^{\ell} (v_i \otimes t_i)$ of $\omega$ under the projection of $\mathbb{C} \Gamma$ onto $V$. Then $v \neq 0$ by Lemma 5. If $b \in Q_j$ for some $j \geq 2$, then $v_b = v$ because $Q_j \leq G_\omega$. On the other hand, every $W_i$ ($i \neq j$) is fixed pointwise by $Q_j$, whence $(v_i \otimes t_i)b = v_i \otimes t_i$. Thus,

$$v = v b = \left( \sum_{i=1}^{\ell} (v_i \otimes t_i) \right) b = \left( \sum_{i \neq j} (v_i \otimes t_i) \right) + (v_j \otimes t_j)b.$$

We conclude that $v_j \otimes t_j = (v_j \otimes t_j)b$ for all $b \in Q_j$ and that $v_j \otimes t_j \in C_{W_j}(Q_j) = 0$. Hence $v \in W_1$.

Consider the block system $\mathcal{B} = \{ W_i \mid 1 \leq i \leq \ell \}$ in the $\mathbb{C}X$-module $W$. For every $x \in N_X(B)$ and every $j \in \{1, \ldots, \ell\}$, the group $Q_j$ fixes $\bigoplus_{i \neq j} W_i$ pointwise. It follows that $Q_j^x = Q_j$ for every $j$. In particular, $N_X(B)$ normalizes every component of $S_1(G)/F$, whence $N_X(B)S_1(G)/S_1(G)$ is solvable. But then, $N_X(B) \leq R_2(G)$ and $\lambda(X/N_X(B)) = \lambda(X) = n - 1$.

Let $w \in F_\infty$ be any reduced $k$-variable word of length $n$. Again, we distinguish our two cases.

**Case 1. $p > 2$.**

With respect to its action on $B$, the group $X/N_X(B)$ satisfies Theorem C. Hence there exist a Sylow 2-subgroup $P$ in $X$ and $\overline{x} \in P^k$ such that $W_1 w_1(\overline{x}) \neq W_1 w_j(\overline{x})$, for all $0 \leq i < j \leq n - 1$. An application of Lemma 3 with $X, X_1, Q, Q$ in the roles of $G, H, M^*, A^*$ (respectively) yields an element $u \in V_X$ and a $k$-tuple $b \in Q^k$ such that $u w_i(\overline{b}) \neq u w_j(\overline{b})$ for all $0 \leq i < j \leq n$. Because the 2-group $Q$ is normal in $X$, we have $Q \leq P$ and $\overline{b} \in P^k$. If $u = v g$, with $g \in X_1$, then $u$ is the projection of $\delta = \omega g$ on $V$. Hence $\overline{u} w_i(\overline{b}) \neq \overline{u} w_j(\overline{b})$, for all $0 \leq i < j \leq n$. But then, $G$ would not be a counterexample to Theorem C. This contradiction shows that $R \leq G_\omega$ implies $K \leq G_\omega$ in the case when $p$ is odd.

**Case 2. $p = 2$.**

Since $Q \leq D$ and $X = N_G(Q) \cap N_G(DF)$, we have $[D, X] \leq DF \cap N_G(Q) = DF \cap X = D(F \cap X)$. In particular, $D(F \cap X) \leq X$. Pick a Sylow 2-subgroup $J_0$ in $D$. Then $J = J_0(X \cap F)$ is a Sylow 2-subgroup in $D \cap X$, and the Frattini argument gives $X = D \cap X \cup Y$, where $Y = N_X(J)$. But $D \cap X \leq S_1(G)$, and so $G = S_1(G)X = S_1(G)Y$.

Clearly, $J_0 = \prod_{i=1}^{\ell} J_i$ for certain Sylow 2-subgroups $J_i$ of $D_i$ ($1 \leq i \leq \ell$). Moreover, $Y$ must permute the subgroups $J_i(X \cap F)$ ($1 \leq i \leq \ell$) transitively via conjugation, as well as the subgroups $S_i(F)$ ($1 \leq i \leq \ell$). Therefore, it follows as above with $J_i(X \cap F)$ in place of $Q_i$, that $Y$ acts transitively on $B$ and that $Y/N_Y(B)$ has nonsolvable length $n - 1$.

In particular, $Y/N_Y(B)$ satisfies Theorem C, and there exist a Sylow 2-subgroup $P$ of $Y$ and $\overline{x} \in P^k$ such that $W_1 w_1(\overline{x}) \neq W_1 w_j(\overline{x})$, for all $0 \leq i < j \leq n - 1$. Let $Y_1 = N_Y(J_1) = N_Y(J_1(X \cap F))$. Note that the intersection $X \cap F$ acts trivially on $V$, because it is a normal subgroup of $X$ with trivial action on $W$. Therefore, we can apply Lemma 3 with the quotients of the groups $Y, Y_1, J, J$
modulo \((X \cap F)\) in the roles of \(G, H, M^*, A^*\) (respectively). This yields an element \(u \in vY_1\) and a \(k\)-tuple \(\vec{b} \in J^k\) such that \(uw_i(b\vec{x}) \neq uw_j(b\vec{x})\) for all \(0 \leq i < j \leq n\).

Because the 2-group \(J\) is normal in \(Y\), we have \(J \leq P \in P^k\). If \(u = vg\), with \(g \in Y_1\), then \(u\) is the projection of \(\delta = \omega g\) on \(V\). Hence \(\delta w_i(b\vec{x}) \neq \delta w_j(b\vec{x})\), for all \(0 \leq i < j \leq n\). But then, \(G\) would not be a counterexample to Theorem C. This contradiction shows that \(R \leq G_\omega\) implies \(K \leq G_\omega\) in the case when \(p = 2\) too.

**Conclusion:** \(R \leq G_\omega\) implies \(K \leq G_\omega\) for all \(p\).

Since the normal subgroup \(F\) of \(G\) is not contained in \(G_\omega\), Lemma 8 gives \(S_1(G) = FL \leq FG_\omega\) and \(S_1(G) = F(S_1(G) \cap G_\omega)\) for every \(\omega \in \Omega\). Since \(R\) is a 2-group, respectively, an \(r\)-group, a conjugate of \(R\) is contained in a Sylow subgroup of \(S_1(G) \cap G_\omega\). Therefore, \(R \leq G_\alpha\) for some \(\alpha \in \Omega\), and hence \(K \leq G_\alpha\) as well.

Clearly \(R\) is normal in \(N = N_G(R)\), and so \(R \leq G_\beta\) and \(K \leq G_\beta\) for every \(\beta \in \alpha N\). In particular, \(K\) is contained in the intersection

\[
H = \bigcap_{\beta \in \alpha N} (S_1(G) \cap G_\beta).
\]

In particular, \(1 \neq K \leq H < S_1(G)\) and \(H\) is normalized by \(N\). Consider \(M = HN\).

An application of the Frattini argument to the subgroup \(R\) of \(S_1(G)\) shows that \(G = S_1(G)N\). Since \(S_1(G) = FK\) and \(K \leq M\), we have that \(G = FM\). However, \(F\) consists of nongenerators for the group \(G\). Therefore \(G = M\). But this implies \(\Omega = \alpha HN = \alpha N\) and \(1 \neq H \leq \bigcap_{\beta \in \alpha N} G_\beta = \bigcap_{\omega \in \Omega} G_\omega = 1\), a contradiction. \(\square\)

**5 PROOF OF THE MAIN THEOREMS**

We are now well-prepared to take the final steps in the proof of Theorem C.

**Theorem C.** Let \(G\) be a finite group with \(\lambda(G) = n\), and let \(\Omega\) be a faithful transitive \(G\)-set. Then, for every \(\omega \in \Omega\) and for every nontrivial reduced word \(w = w(x_1, ..., x_k) \in F_\infty\) of length \(n\), there exist a Sylow 2-subgroup \(P\) of \(G\) and a tuple \(\vec{g} \in P^k\) such that the points \(\omega w_0(\vec{g}), \omega w_1(\vec{g}), ..., \omega w_n(\vec{g})\) are pairwise distinct. In particular, \(G \in P_n\).

**Proof.** At first we shall explain why the last claim follows from the central statement in Theorem C. Consider a finite group \(G\) with nonsolvable length \(n\), and let \(\Omega\) be a faithful \(G\)-set. Then there exist finitely many \(G\)-orbits \(\Omega_1, ..., \Omega_r\) in \(\Omega\) such that \(N_1 \cap ... \cap N_r = 1\), where \(N_i\) denotes the kernel of the action of \(G\) on \(\Omega_i\). From [6, Lemma 2.5], there exists some \(k\) such that \(\lambda(G) = \lambda(G/N_k)\). Application of the first part of Theorem C to the action of \(G\) on \(\Omega_k\) now gives \(G/N_k \in P_n(\Omega_k)\), whence \(G \in P_n(\Omega)\).

We shall now prove the central statement of Theorem C. To this end, assume that Theorem C is wrong, and consider a minimal counterexample \((G, \Omega)\) with \(\lambda(G) = n\). Recall that minimality of the counterexample refers to the number \(n + |G| + |\Omega|\), and that \(G\) acts transitively and faithfully on \(\Omega\). Moreover, since \(G\) is a counterexample, there exist a point \(\omega \in \Omega\) and a word \(w = w(x_1, ..., x_k) \in F_\infty\) of length \(n\) such that the points \(\omega w_0(\vec{g}), ..., \omega w_n(\vec{g})\) are not pairwise dis-
tinct for any choice of a tuple \( \mathcal{G} \in D^k \) with entries from any Sylow 2-subgroup \( P \) of \( G \). The point \( \omega \) and the word \( w \) will be kept fixed throughout the proof.

By Proposition 2, the unique minimal normal subgroup \( S_j(G) \) in \( G \) is the product \( \prod_{j \in \Delta} S_j \) of copies \( S_j \) of a simple group \( S \in \mathcal{L} \). Let \( \Delta = \{1, \ldots, \ell\} \). We also write \( S^* \) instead of \( S_j(G) \) and let \( \pi_j : S^* \rightarrow S_j \) denote the canonical projection. Lemma 6 gives us an \( \text{Aut}(S) \)-invariant \( S \)-conjugacy class of dihedral subgroups of order \( 2p \) in \( S \), for some odd prime \( p \). Let \( D_j \) denote the copy of this conjugacy class in \( S_j \).

We aim to show first that \( G = S^*N_G(D^*) \) for a certain subgroup \( D^* \) of \( S^* \), which is the direct product of dihedral groups \( D_j \in D_j \) (1 \( \leq j \leq \ell \)).

**Case 1.** The subgroup \( G_\omega \cap S^* \) is not a subdirect product of the components \( S_j \).

Without loss we assume that \( (G_\omega \cap S^*)^{\pi_1} < S_1 \). Then it is possible to find \( D_1 \in D_1 \) such that the Sylow \( p \)-subgroup \( C_1 \) of \( D_1 \) is not contained in \( (G_\omega \cap S^*)^{\pi_1} \). Because \( D_1 \) is generated by its involutions, there is also a Sylow 2-subgroup \( Q_1 \leq D_1 \), which is not contained in \( (G_\omega \cap S^*)^{\pi_1} \). For every \( j \neq 1 \), we choose \( D_j \in D_1 \) arbitrarily and form \( D^* = \prod_{j \in \Delta} D_j \). The \( G \)-conjugates of \( D^* \) are precisely the \( S^* \)-conjugates of \( D^* \). Therefore, the Frattini argument yields \( G = S^*N_G(D^*) \).

**Case 2.** The subgroup \( G_\omega \cap S^* \) is a subdirect product of the components \( S_j \).

In this case, there exists a product \( U^* = \{\Delta_i \mid i = 1, \ldots, m\} \) of \( \Delta \) such that \( G_\omega \cap S^* = \prod_{i=1}^m U_i \) where each \( U_i \) is a diagonal subgroup of \( S(\Delta_i) = \prod_{j \in \Delta_i} S_j \). Here, some of the \( \Delta_i \) must contain at least two points. Without loss we may assume that \( |\Delta_1| \geq 2 \) for the set \( \Delta_1 \) containing 1. The conjugation action of \( G_\omega \) on \( G_\omega \cap S^* \) gives rise to an action of \( G_\omega \) on the set \( U^* \), and \( G_\omega \) normalizes \( \mathcal{O} = \{\Delta_i \in U^* \mid |\Delta_i| \geq 2\} \).

Assume that the action on \( \mathcal{O} \) is not transitive, and consider a \( G_\omega \)-orbit \( I \subseteq \mathcal{O} \). Because we are in case 2, it is possible to choose \( I \) such that the \( G_\omega \)-invariant subgroup \( S(I) = \prod_{\Delta_i \in I} \prod_{j \in \Delta_i} S_j \) is not contained in \( G_\omega \). From Lemma 8, the monolith \( S^* \) is contained in \( S(I)G_\omega \), and Dedekind’s identity yields \( S^* \cap S(I)G_\omega = (S^* \cap G_\omega)S(I) \). Since \( I \neq \emptyset \), there exists \( \bar{\Delta} \in \mathcal{O} \setminus I \). But now, the projection of \( S^* = (S^* \cap G_\omega)S(I) \) on \( S(\bar{\Delta}) \) is isomorphic to \( S \), a contradiction to \( |\bar{\Delta}| \geq 2 \). We conclude that all the \( \Delta_i \) of size \( \geq 2 \) are permuted transitively by \( G_\omega \). In particular, they all have the same size \( d \).

There are automorphisms \( \sigma_2, \ldots, \sigma_d \in \text{Aut}(S_1) \) such that

\[
U_1 = \{(s, s^{\sigma_2}, \ldots, s^{\sigma_d}) \mid s \in S_1\}.
\]

For each \( j \in \Delta \), we can choose a subgroup \( D_j \in D_j \), such that \( U_1 \cap (\prod_{j \in \Delta} D_j) = 1 \). We can proceed in the same fashion with every \( \Delta_i \in \mathcal{O} \). When \( S_j \leq G_\omega \), we choose \( D_i \in D_i \) freely. Let \( D^* = \prod_{i \in \Delta} D_i \). Note that \( D^* \cap G_\omega \) is the product of precisely those factors \( D_j \), for which \( S_j \leq G_\omega \). In particular, \( (D^* \cap G_\omega)^{\pi_1} = 1 \). And also in this case, the Frattini argument gives \( G = S^*N_G(D^*) \).

We proceed to work with the group \( D^* \) constructed in the two cases. For each \( j \in \Delta \), choose a Sylow 2-subgroup \( Q_j \) of \( D_j \) (in case 1, the group \( Q_1 \) has already been chosen), and let \( C_j \) be the Sylow \( p \)-subgroup of \( D_j \). As usual, we let \( C^* = \prod_{j \in \Delta} C_j \) and \( Q^* = \prod_{j \in \Delta} Q_j \). Further applications of the Frattini argument give \( G = S^*N_G(D^*) \) and \( N_G(D^*) = D^*N_G(D^*)(Q^*) \), whence \( G = S^*X \) for \( X = N_G(D^*) \cap N_G(Q^*) \).

It follows that \( X \) must act transitively via conjugation on the set \( \{D_j \mid j \in \Delta\} \). Moreover, \( X < G \) and \( G/S^* \approx X/(X \cap S^*) \) imply that \( \lambda(X) = n - 1 \). Consider the subgroup \( A = C^*X \) and note...
that $A$ contains $D^* = C^*Q^*$. We observe that any nontrivial element $c$ from $C^*$ with nontrivial constituent in some $C_j$ can be conjugated by an involution in $D_j$, whence $C_j$ is contained in the normal closure of $c$ in $A$. Together with the transitivity of the action of $X$ on the set $\{D_j \mid j \in \Delta\}$, this yields that $C^*$ is a minimal normal subgroup in $A$. Now $C_1$ is not contained in $G_\omega$. It follows that $C^*$ acts faithfully on the set $\Gamma = \omega A$. Consider the kernel $K$ of the action of $A$ on $\Gamma$. Since $K \cap C^* = 1$, the subgroup $K$ commutes with $C^*$. But then $K$ normalizes every $C_j$ and hence every $S_j$. It follows that $K = R_2(G)$ and $\lambda(A/K) = \lambda(A) = n - 1$.

If $K$ contained an involution $a$ from $D^*$, then the subgroup $[a, D^*]$ of $K$ would contain one of the $C_j$. This argument shows that $D^* \cap K = 1$. Consider $H = N_A(D_j)$ and $R = (H \cap A_\omega)\widetilde{D}_1$, where $\widetilde{D}_1 = \prod_{i \neq 1} D_i$. Assume $C_1 \leq R$. Then $C_1 \leq D^* \cap R \leq (D^* \cap G_\omega)\widetilde{D}_1$. But this implies $1 \neq C_1 \leq (D^* \cap G_\omega)^{r_1}$, a contradiction. It follows that $C_1 \ncong R$. In particular, there exists then an irreducible component $W$ in the $\mathcal{CH}$-module $\text{Ind}^H_R(C)$ on which $C_1$ acts nontrivially.

From Lemmas 2 and 4, the $\mathcal{CA}$-module $V = W \otimes_H C.A$ is (isomorphic to) a submodule of $\mathcal{C} \Gamma$. Clearly, $V = \bigoplus_{t \in T} W_1$ with $W_1 = W \otimes t$, where $T$ denotes a transversal of $H$ in $A$. Since $C^* \leq H$, the transversal can be chosen such that $1 \in T \subset X$. Note that $X$ normalizes $Q^*$. Therefore, each index $j \in \Delta$ determines a unique $t \in T$ such that $D_j = D^t_1$, and even $C_j = C^t_1$ and $Q_j = Q^t_1$. Moreover, $D_j$ acts nontrivially on $W_1$ if and only if $D_j = D^t_1$, because $\widetilde{D}_1$ acts trivially on $W$.

Let $v = \sum_{t \in T} u_t \otimes t$ denote the projection of a point $\tau \in \Gamma$ on $V$. Then $v \neq 0$ by Lemma 5, and we may choose $\tau$ in such a way that $u_1 \neq 0$. Consider any reduced $k$-variable word $w \in F_\infty$ of length $n$. The group $G$ permutes the set $\{S_j \mid j \in \Delta\}$ of components of $S^*$. Because $G$ is a minimal counterexample, there exist a Sylow 2-subgroup $P_0$ of $X$ and a $k$-tuple $\overline{g} \in P^k_2$ such that the components $S_1^{w_0(\overline{g})}, S_1^{w_1(\overline{g})}, \ldots, S_1^{w_{n-1}(\overline{g})}$ are pairwise distinct. In particular, the subgroups $D_1^{w_0(\overline{g})}, D_1^{w_1(\overline{g})}, \ldots, D_1^{w_{n-1}(\overline{g})}$ are pairwise distinct as well.

Clearly, $W = \langle u_1, H \rangle$. And since $D_1 = \langle Q^t_1 \rangle$ acts nontrivially on $W$, the group $Q_1$ acts nontrivially on $W$ too. We can therefore apply Lemma 3 with $A, H, D_1, Q_1$ in place of $G, H, M_0, A_0$ (respectively). It follows that there are a $k$-tuple $\overline{h} \in Q^*P_0^k$ and a vector $u_1 = u_1, h \in u_1, H$, such that the elements $(u_1 \otimes 1)u_1(\overline{g} h)$ are pairwise distinct for $0 \leq j \leq n$. Here, $\overline{g} h \in (Q^*P_0)^k$ and $Q^*P_0$ is contained in a Sylow 2-subgroup $P$ of $G$.

The projection $u = uh = \sum_{t \in T} u_t \otimes t \cdot \tau h$ on $V$ has nontrivial component $u_1 \otimes 1$ along $W_1$. We now refine our choice of $T$ by asking that $T$ contains a transversal of $Z = H \cap P$ in $P$. Consider the elements $x_{ij} = u_i(\overline{h} g)u_j(\overline{g} h)^{-1}$ for $0 \leq i < j \leq n$. Let $x$ be one of the elements $x_{ij} \in P$. Then $u_1 \otimes 1 \neq (u_1 \otimes 1)x = u_1z \otimes t$, where $z = xt$ for unique $z \in Z$ and $t \in T \cap P$. Since $Z$ is a 2-group, $|u_1z| \leq 2$.

Assume $u_1C_1 \subseteq u_1Z$. The set $u_1C_1$ is a block for the action of $H$ on $u_1H$ and therefore it is also a block for the action of $Z$ on $u_1Z = u_1Z$. In particular, also $|C_1 : \text{Stab}_{C_1}(u_1)| = |u_1C_1|$ is a power of 2. On the other hand, the $p$-group $C_1$ is a normal subgroup of $H$, which acts nontrivially on $W$, so that it must in fact act fixed-point-freely on $W$, with orbits of size $p$. This contradiction shows that $u_1C_1 \ncong u_1Z$.

For each $t \in T \setminus \{1\}$, we choose an element $s_t \in C_1$ such that $u_1s_t \ncong u_1Z$. And we let $s_1 = 1$. Consider $s^* = \prod_{t \in T} s_t^t \in \prod_{t \in T} C_1^t = C^*$ and the point $\alpha = \tau hs^* \in \Gamma$. The projection of $\alpha$ on $V$ is

$$\bar{v} = us^* = u_1 \otimes 1 + \sum_{1 \neq t \in T} u_t s_t \otimes t.$$  

We claim that $\bar{v} x_{ij} \neq \bar{v}$ for $1 \leq i < j \leq n$. 


To this end, we only need to show that for every choice of $i < j$ there exists some $t \in T$ such that the $W_t$-components of $\bar{v}x_{ij}$ and $\bar{v}$ are different. In the case when $x_{ij}$ normalizes $W_1$, the $W_1$-component of $\bar{v}x_{ij}$ is $(u_1 \otimes 1)x_{ij} \neq u_1 \otimes 1$. In the case when $W_1x_{ij} = W_t \neq W_1$, the $W_t$-component of $\bar{v}x_{ij}$ has the form $y \otimes t$ for some $t \in u_1Z$, while the $W_t$-component of $\bar{v}$ is $(u_t \otimes t) \otimes t \neq y \otimes t$.

We have shown now that $\alpha x_{ij} \neq \alpha$, respectively, $\alpha w_i(\bar{b}g\bar{a}) \neq \alpha w_j(\bar{b}g\bar{a})$ for all $0 \leq i < j \leq n$. Recall that $\Gamma = \omega A$, so that $\omega = \alpha a$ for some $a \in A$. Now $\omega w_i((\bar{b}g\bar{a})^a) = \alpha w_i(\bar{b}g)a$ for all $i$, and so it follows that the points $\omega w_i((\bar{b}g\bar{a})^a)$ are pairwise distinct for $0 \leq i \leq n$. However, also the entries of the tuple $(\bar{b}g\bar{a})^a$ lie in a common Sylow 2-subgroup of $G$. This contradicts the choice of $\omega$ and $w$ at the very beginning of the proof. □

Proof of Theorem B. Consider any faithful transitive $G$-set $\Omega$. By Theorem C, the group $G$ satisfies $P_n$ on $\Omega$. Thus we can find $\omega \in \Omega$ and $\bar{g} \in G^k$ such that $\omega w(\bar{g}) = \omega w_n(\bar{g}) \neq \omega$. This implies immediately that $w(\bar{g}) \neq 1$. □

Proof of Theorem A. Consider a nontrivial $k$-variable reduced word $w \in F_\infty$ of length $n = \lambda(G)$. Theorem B provides a $k$-tuple $\bar{g} \in H^k$ such that $w(\bar{g}) \neq 1$. Therefore, $w$ is not a law in $G$. This shows that $\lambda(G) < \nu(G)$. □

JOURNAL INFORMATION
The Proceedings of the London Mathematical Society is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES
1. M. Bhattacharjee, The ubiquity of free subgroups in certain inverse limits of groups, J. Algebra 172 (1995), no. 1, 134–146.
2. A. Bors and A. Shalev, Words, permutations, and the nonsolvable length of a finite group, J. Comb. Algebra 5 (2021), no. 2, 93–122.
3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, Atlas of finite groups, Oxford University Press, Eynsham, 1985. (Maximal subgroups and ordinary characters for simple groups, with computational assistance from J. G. Thackray.)
4. C. W. Curtis and I. Reiner, Methods of representation theory, vol. I, Wiley Classics Library. John Wiley & Sons, Inc., New York, N.Y., 1990. (With applications to finite groups and orders; Reprint of the 1981 original; A Wiley-Interscience Publication.)
5. J. D. Dixon and B. Mortimer, Permutation groups, Grad. Texts Math., vol. 163, Springer, New York, N.Y., 1996.
6. F. Fumagalli, F. Leinen, and O. Puglisi, A reduction theorem for nonsolvable finite groups, Israel J. Math. 232 (2019), no. 1, 231–260.
7. D. Gorenstein, R. Lyons, and R. Solomon, The classification of the finite simple groups. Number 3. Part I, Chapter A, Math. Surv. Monographs., vol. 40, Amer. Math. Soc., Providence, R.I., 1998. Almost simple $K$-groups.
8. G. A. Jones, Varieties and simple groups, J. Austral. Math. Soc. 17 (1974), 163–173. (Collection of articles dedicated to the memory of Hanna Neumann, VI.)
9. E. I. Khukhro and P. Shumyatsky, Nonsoluble and non-p-soluble length of finite groups, Israel J. Math. 207 (2015), no. 2, 507–525.
10. M. Larsen and A. Shalev, Word maps and Waring type problems, J. Amer. Math. Soc. 22 (2009), no. 2, 437–466.
11. M. Larsen, A. Shalev, and P. H. Tiep, The Waring problem for finite simple groups, Ann. of Math. (2) 174 (2011), no. 3, 1885–1950.
12. F. Leinen and O. Puglisi, *Free subgroups of inverse limits of iterated wreath products of non-abelian finite simple groups in primitive actions*, J. Group Theory 20 (2017), no. 4, 749–761.

13. M. W. Liebeck, E. A. O’Brien, A. Shalev, and P. H. Tiep, *The Ore conjecture*, J. Eur. Math. Soc. (JEMS) 12 (2010), no. 4, 939–1008.

14. D. J. S. Robinson, *A course in the theory of groups*, 2nd edn, Grad. Texts Math., vol. 80, Springer, New York, N.Y., 1996.

15. A. Shalev, *Some results and problems in the theory of word maps*, in, Erdős centennial, Bolyai Soc. Math. Stud., vol. 25, János Bolyai Math. Soc., Budapest, 2013, pp. 611–649.