Strong pseudo Frobenius numbers

Benjamin Sambale*

November 1, 2026

Abstract

By Sylow's theorem, the number of Sylow p-subgroups of a finite group is congruent to 1 modulo p, but not every such integer occurs. Frobenius extended the congruence to the number of subgroups of order p^a for every $a \geq 0$. Kulakoff and Hall showed that this number is congruent to 1 or $1+p$ modulo p^2 whenever p^{a+1} divides the group order. A positive integer is a Frobenius p-number if it is the number of subgroups of order p^a of some finite group for some a. There are integers congruent to 1 modulo p^2 which are not Frobenius p-numbers, and it remained open whether there are also such integers congruent to $1+p$ modulo p^2. We show that no finite group has exactly 106 subgroups of order 5^a for any $a \geq 0$.

Keywords: Frobenius' theorem, number of p-subgroups, pseudo Frobenius numbers, Sylow numbers
AMS classification: 20D20, 20D15, 20D60

1 Introduction

For a finite group G, a prime p and an integer $a \geq 0$, let $\mathcal{S}_a(G)$ be the set of subgroups of order p^a of G and $s_a(G) := |\mathcal{S}_a(G)|$. A positive integer n is a *Frobenius p-number* if $n = s_a(G)$ for some finite group G and some $a \geq 0$. By Frobenius' theorem, $s_a(G) \equiv 1 \pmod{p}$ whenever p^a divides $|G|$, and by the theorem of Kulakoff and Hall, $s_a(G)$ is congruent to 1 or $1+p$ modulo p^2 whenever p^{a+1} divides $|G|$ (see Proposition 2.1 below). Following [10], an integer n congruent to 1 or $1+p$ modulo p^2 is called a *pseudo Frobenius p-number* if it is not a Frobenius p-number. This continues the study of *pseudo Sylow p-numbers*, that is, integers $n \equiv 1 \pmod{p}$ which are not the number of Sylow p-subgroups of any finite group. By a result of M. Hall [6], such numbers exist for every odd prime p, and an elementary proof that 35 is a pseudo Sylow 17-number was given by the author [11]. In [10] it was shown that every Frobenius p-number $n \equiv 1 \pmod{p^2}$ is a Sylow p-number, and that 46 is a pseudo Frobenius 3-number. We call an integer $n \equiv 1+p \pmod{p^2}$ which is not a Frobenius p-number a *strong pseudo Frobenius p-number*. In [10] it was left open whether strong pseudo Frobenius numbers exist (see also the master's thesis of Blaas [3]).

Theorem A. *No finite group has exactly* 106 *subgroups of order* 5^a *for any* $a \geq 0$*, i. e.,* 106 *is a strong pseudo Frobenius* 5*-number.*

Corollary B. *The integer* 106 *is the smallest strong pseudo Frobenius p-number, where p runs through all primes.*

*Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany, sambale@math.uni-hannover.de

Zhang–Qu [12, Conjecture B] conjectured for p-groups P with $p > 2$ that $s_a(P)$ is congruent to 1 or $1+p+kp^2$ modulo p^3 for some $0 \le k \le 3$. Since $106 = 1+5+4\cdot 5^2 = 1+5\cdot 21$, this would imply Theorem A for 5-groups. The number 21 plays a role for arbitrary groups, since $s_1(C_5 \times H) = 1 + 5|\mathrm{Syl}_5(H)|$ for every group H with a Sylow 5-subgroup of order 5, and 21 is not a Sylow 5-number.

Compared to the previous papers [11, 10], the proof of Theorem A is more sophisticated this time. We consider a minimal counterexample G. Using the classification of primitive groups of low degree (ultimately relying on the CFSG), we show in Section 3 that G must be a 5-group. In Section 4 we prove further that G is a two-generator group of order at most 5^5, and these groups are excluded by a computer search. The computations are collected in Section 5, and the GAP code is attached to this pdf.

2 Preliminaries

Throughout, p is a prime and all groups are finite.

Proposition 2.1. *Let P be a Sylow p-subgroup of G with $|P| = p^n$ and let $0 \le a \le n$.*

(a) $s_a(G) \equiv 1 \pmod p$.

(b) If $p > 2$ and $1 \le a \le n-1$, then $s_a(G) \equiv 1 \pmod{p^2}$ if P is cyclic and $s_a(G) \equiv 1+p \pmod{p^2}$ otherwise.

Proof. See [7, (4.12), Lemma 4.61 and Theorem 4.6]. □

Lemma 2.2. *Let N be a normal subgroup of a p-group G with $1 < N < G$. Then the number of complements of N in G is divisible by p.*

Proof. Suppose the contrary. Since G acts on the set of complements of N by conjugation, some complement K is normal in G, and $G = N \times K$. Let H be a complement of N. For $k \in K$, the coset kN contains exactly one element of H, which we write as $k\varphi(k)$ with $\varphi(k) \in N$. Since N and K commute, $\varphi\colon K \to N$ is a homomorphism. Conversely, $\{k\varphi(k) : k \in K\}$ is a complement of N for every homomorphism $\varphi\colon K \to N$. Hence the number of complements of N is $|\mathrm{Hom}(K,N)|$. The group N acts on $\mathrm{Hom}(K,N)$ by conjugation, and the fixed points are the homomorphisms $K \to \mathrm{Z}(N)$. They form the group $\mathrm{Hom}(K,\mathrm{Z}(N))$, which is a nontrivial p-group, since $K \ne 1$ has a quotient of order p and $\mathrm{Z}(N) \ne 1$ has an element of order p. Hence $|\mathrm{Hom}(K,N)| \equiv |\mathrm{Hom}(K,\mathrm{Z}(N))| \equiv 0 \pmod p$, a contradiction. □

Lemma 2.3. *Let N be a normal subgroup of a p-group Y with $N < Y$, and let $b \ge 0$. Then the number of subgroups $Q \le Y$ of order p^b with $QN = Y$ and $N \not\le Q$ is divisible by p.*

Proof. Fix $A < N$ and let $\mathcal{Q}_A$ be the set of these subgroups Q with $Q \cap N = A$. We may assume that $\mathcal{Q}_A \ne \varnothing$. Every $Q \in \mathcal{Q}_A$ normalizes $A = Q \cap N$, so Q lies in $U := \mathrm{N}_Y(A)$ and $UN = Y$. Let $D := U \cap N = \mathrm{N}_N(A)$. Since $A < N$, the normalizer condition gives $A < D$. For $Q \in \mathcal{Q}_A$, the group Q/A is a complement of D/A in U/A. Conversely, if H/A is a complement of D/A in U/A, then $H \cap N = A$, $HN = HDN = UN = Y$ and $|H| = |A||U : D| = |Q|$. Hence, $Q \mapsto Q/A$ is a bijection between $\mathcal{Q}_A$ and the set of complements of D/A in U/A. Since $A < D$ and $(U/A)/(D/A) \cong U/D \cong Y/N \ne 1$, Lemma 2.2 yields $|\mathcal{Q}_A| \equiv 0 \pmod p$. Summing over A proves the claim. □

Lemma 2.4. *No finite group has exactly* 106 *Sylow* 5*-subgroups.*

Proof. Suppose that G is a group of minimal order with exactly 106 Sylow 5-subgroups. Let K be the kernel of the conjugation action of G on $\mathrm{Syl}_5(G)$. For $P \in \mathrm{Syl}_5(G)$ we have $PK \leq \mathrm{N}_G(P)$, so P is the only Sylow 5-subgroup of PK. Hence $P \mapsto PK/K$ is a bijection $\mathrm{Syl}_5(G) \to \mathrm{Syl}_5(G/K)$, and the minimality of G yields $K = 1$. If $\mathrm{N}_G(P) < M \leq G$, then $|\mathrm{Syl}_5(M)| = |M : \mathrm{N}_G(P)|$ is a divisor of $106 = 2 \cdot 53$ congruent to 1 modulo 5. Hence $M = G$, and G is a primitive permutation group of degree 106 whose point stabilizer $\mathrm{N}_G(P)$ has a nontrivial normal 5-subgroup. By [4, Appendix B, Table B.4], the only primitive groups of degree 106 are A_{106} and S_{106}, and their point stabilizers have no nontrivial normal 5-subgroup (see also [3, Theorem 2.13]). □

Definition 2.5. From now on, $p = 5$. A group G is *critical* if $s_a(G) = 106$ for some $a \geq 0$, and G has minimal order among all groups with this property. For a critical group G, we fix such an a and a Sylow 5-subgroup P of G, and we write $|P| = 5^n$.

Lemma 2.6. *Let G be critical. Then the following hold:*

(a) $1 \leq a \leq n-1$, P *is not cyclic and* $s_a(P) \in \{6, 31, 56, 81, 106\}$.

(b) $G = \langle \mathcal{S}_a(G) \rangle$. *In particular,* $\mathrm{O}^{5'}(G) = G$.

(c) The intersection of all members of $\mathcal{S}_a(G)$ *is trivial.*

Proof. (a) Since $s_0(G) = 1$ and $s_a(G) \neq 0$, we have $1 \leq a \leq n$. If $a = n$, then $s_a(G)$ is the number of Sylow 5-subgroups of G, which contradicts Lemma 2.4. Since $106 \equiv 1 + 5 \pmod{25}$, Proposition 2.1(b) shows that P is not cyclic. Applying Proposition 2.1(b) to P gives $s_a(P) \equiv 6 \pmod{25}$, and $s_a(P) \leq 106$ holds since $\mathcal{S}_a(P) \subseteq \mathcal{S}_a(G)$.

(b) The subgroup $H := \langle \mathcal{S}_a(G) \rangle$ satisfies $\mathcal{S}_a(H) = \mathcal{S}_a(G)$, so $H = G$. Since $\mathrm{O}^{5'}(G)$ contains all 5-subgroups, it contains H.

(c) Since $\mathcal{S}_a(G)$ is closed under conjugation, the intersection D of its members is a normal 5-subgroup of G, say of order 5^k. Every subgroup of order 5^{a-k} of G/D is of the form Q/D for a subgroup $Q \leq G$ of order 5^a containing D. Since every $Q \in \mathcal{S}_a(G)$ contains D, the map $Q \mapsto Q/D$ is a bijection $\mathcal{S}_a(G) \to \mathcal{S}_{a-k}(G/D)$. Hence $s_{a-k}(G/D) = 106$, and the minimality of G yields $D = 1$. □

Lemma 2.7. *Let X be a 5-group, $b \geq 1$ and $K \trianglelefteq H \leq X$ such that H/K has exponent 5, $|K| < 5^b$ and $|H| \geq 5^{b+3}$. Then $s_b(X) \geq 156$.*

Proof. Since $|K| \leq 5^{b-1}$ and the 5-group H/K has normal subgroups of every order dividing $|H/K|$, there exists $L \trianglelefteq H$ with $K \leq L$ and $|L| = 5^{b-1}$. Since $|H| \geq 5^{b+3}$, there exists $M \leq H$ with $L \leq M$ and $|M| = 5^{b+3}$. Then $L \trianglelefteq M$, and M/L has order 5^4 and exponent 5, since M/L is a quotient of $M/K \leq H/K$. Every nontrivial element of M/L has order 5, and each subgroup of order 5 contains exactly four of them. Hence M/L has exactly $(5^4 - 1)/4 = 156$ subgroups of order 5. Their preimages in M are 156 distinct subgroups of X of order 5^b. □

3 Arbitrary groups

In this section, G is a critical group which is not a 5-group. By Lemma 2.6(a), $s_a(P) \in \{6, 31, 56, 81, 106\}$, and $s_a(P) \neq 106$ by the minimality of G, since $P < G$. Let $\mathcal{M}_5$ be the set of positive integers which are products of prime powers congruent to 1 modulo 5.

Lemma 3.1. *Let N be a normal $5'$-subgroup of G and $Q \in \mathcal{S}_a(G)$. Then the subgroups $X \in \mathcal{S}_a(G)$ with $XN = QN$ are exactly the conjugates Q^x with $x \in N$, and their number $|N : \mathrm{C}_N(Q)|$ lies in $\mathcal{M}_5$.*

Proof. Every $X \in \mathcal{S}_a(G)$ with $XN = QN$ is a complement of N in QN. By the Schur–Zassenhaus theorem [8, Theorem 3.12], $X = Q^y$ for some $y \in QN$, and we may choose $y \in N$. Hence, the number of these subgroups is $|N : \mathrm{N}_N(Q)|$. Since $[\mathrm{N}_N(Q), Q] \leq N \cap Q = 1$, we have $\mathrm{N}_N(Q) = \mathrm{C}_N(Q)$.

Let q be a prime and let S be a Q-invariant Sylow q-subgroup of N (see [8, Theorem 3.23(a)]). By [8, Lemma 3.32], $\mathrm{C}_S(Q)$ is a Sylow q-subgroup of $\mathrm{C}_N(Q)$. Therefore, the q-part of $|N : \mathrm{C}_N(Q)|$ is $|S : \mathrm{C}_S(Q)|$. The nontrivial Q-orbits on S have length divisible by 5, so $|S| \equiv |\mathrm{C}_S(Q)| \pmod 5$. Since $|\mathrm{C}_S(Q)|$ is coprime to 5, this means $|S : \mathrm{C}_S(Q)| \equiv 1 \pmod 5$. □

Proposition 3.2. *We have $\mathrm{O}_{5'}(G) = 1$.*

Proof. Suppose that $N := \mathrm{O}_{5'}(G) \neq 1$ and let $\overline{G} := G/N$. For $Q \in \mathcal{S}_a(G)$ we write $\overline{Q} = QN/N$. The map $Q \mapsto \overline{Q}$ is a surjection $\mathcal{S}_a(G) \to \mathcal{S}_a(\overline{G})$. By Lemma 3.1, the preimage of $\overline{Q}$ under this map has size $t_{\overline{Q}} := |N : \mathrm{C}_N(Q)| \in \mathcal{M}_5$. Hence

$$106 = \sum_{X \in \mathcal{S}_a(\overline{G})} t_X. \tag{3.1}$$

Since $\overline{P} \cong P$, Proposition 2.1 implies $\overline{s} := s_a(\overline{G}) \equiv 6 \pmod{25}$. Moreover, $\overline{s} \leq 106$ by (3.1), and $\overline{s} \neq 106$ by the minimality of G. Hence $\overline{s} \in \{6, 31, 56, 81\}$.

Let $C := \mathrm{C}_G(N) \trianglelefteq G$. Clearly, $t_{\overline{Q}} = 1$ if and only if $Q \leq C$. If $\overline{Q} \leq \overline{C}$, then $Q \leq CN$ and $Q \leq C$, because CN/C is a $5'$-group. Therefore, the set $\mathcal{T} := \{X \in \mathcal{S}_a(\overline{G}) : t_X > 1\}$ is equal to $\mathcal{S}_a(\overline{G}) \setminus \mathcal{S}_a(\overline{C})$. Since $\overline{s} < 106$, (3.1) shows $\mathcal{T} \neq \varnothing$. The prime powers up to 106 which are congruent to 1 modulo 5 are $11, 16, 31, 41, 61, 71, 81, 101$, and the product of any two of them exceeds 106. Hence

$$\mathcal{M}_5 \cap \{1, \ldots, 106\} = \{1, 11, 16, 31, 41, 61, 71, 81, 101\}. \tag{3.2}$$

In particular, every $t \in \mathcal{M}_5 \setminus \{1\}$ with $t \leq 106$ satisfies $t \geq 11$ and $t \equiv 1 \pmod 5$. Thus (3.1) gives

$$106 - \overline{s} = \sum_{X \in \mathcal{T}} (t_X - 1) \geq 10|\mathcal{T}|. \tag{3.3}$$

By Proposition 2.1(a), $s_a(\overline{C})$ is 0 or congruent to 1 modulo 5. Hence, $|\mathcal{T}| = \overline{s}$ or $|\mathcal{T}| \equiv 0 \pmod 5$.

Suppose first that $\overline{s} \neq 6$. Then (3.3) excludes $|\mathcal{T}| = \overline{s}$, so $|\mathcal{T}| \geq 5$ and (3.3) forces $|\mathcal{T}| = 5$ and $\overline{s} \in \{31, 56\}$. Consequently, $s_a(\overline{C}) = \overline{s} - 5 \in \{26, 51\}$ is congruent to 1 modulo 25. Let $\overline{S} := \overline{P} \cap \overline{C} \in \mathrm{Syl}_5(\overline{C})$. By Proposition 2.1(b) applied to $\overline{C}$, either $\overline{S}$ is cyclic or $|\overline{S}| = 5^a$. In both cases $\overline{S}$ has exactly one subgroup X_0 of order 5^a. Since $\mathcal{S}_a(\overline{P}) \cap \mathcal{S}_a(\overline{C}) = \mathcal{S}_a(\overline{S}) = \{X_0\}$, we obtain $\mathcal{S}_a(\overline{P}) \setminus \{X_0\} \subseteq \mathcal{T}$. As $s_a(\overline{P}) \geq 6$ and $|\mathcal{T}| = 5$, it follows that $s_a(\overline{P}) = 6$ and $\mathcal{T} = \mathcal{S}_a(\overline{P}) \setminus \{X_0\}$. Since $\overline{C} \trianglelefteq \overline{G}$, the set $\mathcal{T}$ is invariant under conjugation in $\overline{G}$. For $g \in \overline{G}$ we obtain $\mathcal{T} = \mathcal{T}^g \subseteq \mathcal{S}_a(\overline{P}^g)$. Thus, every member of $\mathcal{T}$ lies in every Sylow 5-subgroup of $\overline{G}$, that is, in $\mathrm{O}_5(\overline{G})$. Now $5 \leq s_a(\mathrm{O}_5(\overline{G})) \leq s_a(\overline{P}) = 6$ and

Proposition 2.1(a) yield $\mathcal{S}_a(\mathrm{O}_5(\overline{G})) = \mathcal{S}_a(\overline{P})$. By conjugation, $\mathcal{S}_a(\overline{P}^g) = \mathcal{S}_a(\mathrm{O}_5(\overline{G}))$ for all $g \in \overline{G}$. Since every 5-subgroup lies in a Sylow 5-subgroup, this gives $\overline{s} = 6$, a contradiction.

Hence $\overline{s} = 6 = s_a(\overline{P})$. As before, $\mathcal{S}_a(\overline{G}) = \mathcal{S}_a(\overline{P}) = \mathcal{S}_a(\mathrm{O}_5(\overline{G}))$. The preimage of $\mathrm{O}_5(\overline{G})$ contains every element of $\mathcal{S}_a(G)$, and Lemma 2.6(b) implies that $\overline{G}$ is a 5-group. Thus $G = N \rtimes P$, $s_a(P) = 6$, and we can identify $\mathcal{S}_a(\overline{G})$ with $\mathcal{S}_a(P)$, so that $t_X = |N : \mathrm{C}_N(X)|$ for $X \in \mathcal{S}_a(P)$. Moreover $t_{X^g} = t_X$ for $g \in P$. Since P acts on $\mathcal{S}_a(P)$ by conjugation, the number of members of $\mathcal{S}_a(P)$ which are normal in P is 1 or 6.

Suppose that exactly one $X_0 \in \mathcal{S}_a(P)$ is normal in P. Then the other five subgroups $X_1, \ldots, X_5$ are conjugate in P, and (3.1) becomes $106 = t_{X_0} + 5t$ with $t := t_{X_1} \in \mathcal{M}_5$. By (3.2), $t \in \{1, 11, 16\}$ and $t_{X_0} \in \{101, 51, 26\}$. Since $51, 26 \notin \mathcal{M}_5$, we have $t = 1$, that is, $X_1, \ldots, X_5$ are contained in $K := \mathrm{C}_P(N) \trianglelefteq P$. Then $s_a(K) \geq 5$ and Proposition 2.1(a) gives $X_0 \leq K$. Hence $t_{X_0} = |N : \mathrm{C}_N(X_0)| = 1$, a contradiction.

Therefore, all six members of $\mathcal{S}_a(P)$ are normal in P. Let q be a prime divisor of $|N|$ and let S_q be a P-invariant Sylow q-subgroup of N (see [8, Theorem 3.23(a)]). For $X \in \mathcal{S}_a(P)$, the group S_q is X-invariant, so $\mathrm{C}_{S_q}(X)$ is a Sylow q-subgroup of $\mathrm{C}_N(X)$ by [8, Lemma 3.32], and the q-part of t_X is $|S_q : \mathrm{C}_{S_q}(X)|$.

Choose a series $1 = U_0 < U_1 < \ldots < U_k = S_q$ of P-invariant normal subgroups of S_q which cannot be refined. Each factor $V_i := U_i/U_{i-1}$ is a chief factor of S_qP, hence an elementary abelian q-group on which S_q acts trivially, and V_i is an irreducible $\mathbb{F}_qP$-module. By [8, Corollary 3.28], $|U_i : \mathrm{C}_{U_i}(X)| = |V_i : \mathrm{C}_{V_i}(X)| \cdot |U_{i-1} : \mathrm{C}_{U_{i-1}}(X)|$, so

$$|S_q : \mathrm{C}_{S_q}(X)| = \prod_{i=1}^{k} |V_i : \mathrm{C}_{V_i}(X)|.$$

Since $X \trianglelefteq P$, $\mathrm{C}_{V_i}(X)$ is a submodule of V_i, so $\mathrm{C}_{V_i}(X) \in \{0, V_i\}$. Let $\mathcal{V}$ be the family of all these factors for all prime divisors q of $|N|$. For $V \in \mathcal{V}$ let $A_V := \{X \in \mathcal{S}_a(P) : X \not\leq \mathrm{C}_P(V)\}$. We have shown that

$$t_X = \prod_{\substack{V \in \mathcal{V} \\ X \in A_V}} |V| \qquad (X \in \mathcal{S}_a(P)).$$

If $A_V \neq \varnothing$, then some $X \in \mathcal{S}_a(P)$ acts fixed point freely on $V \setminus \{0\}$ and $|V| \equiv 1 \pmod 5$. By Proposition 2.1(a), $s_a(\mathrm{C}_P(V)) \in \{0, 1, 6\}$ and therefore $|A_V| \in \{6, 5, 0\}$. Let c be the product of the $|V|$ with $|A_V| = 6$, and for $X \in \mathcal{S}_a(P)$ let m_X be the product of the $|V|$ with $A_V = \mathcal{S}_a(P) \setminus \{X\}$. Then $c, m_X \in \mathcal{M}_5$ and

$$106 = \sum_{X \in \mathcal{S}_a(P)} t_X = c \sum_{X \in \mathcal{S}_a(P)} \prod_{Y \neq X} m_Y.$$

Since $c \in \mathcal{M}_5$ divides $106 = 2 \cdot 53$, we have $c = 1$. If $m_X > 1$ and $m_Y > 1$ for some $X \neq Y$, then $t_Z \geq m_X m_Y \geq 121$ for every $Z \in \mathcal{S}_a(P) \setminus \{X, Y\}$, which is impossible. If $m_X = 1$ for all X, then $106 = 6$. Hence, there is exactly one X with $m := m_X > 1$, and $106 = 1 + 5m$. But $m = 21 \notin \mathcal{M}_5$, a contradiction. □

Lemma 3.3. *Let $R := \mathrm{O}_5(G)$ and $\overline{G} := G/R$. For a nontrivial 5-subgroup $\overline{X}$ of $\overline{G}$ with preimage Y, let $f(\overline{X})$ be the number of $Q \in \mathcal{S}_a(G)$ with $QR = Y$ and $R \not\leq Q$. Then $f(\overline{X})$ is divisible by 5, and f is constant on conjugacy classes of $\overline{G}$.*

Proof. Every $Q \in \mathcal{S}_a(G)$ with $QR = Y$ lies in the 5-group Y, and $R < Y$ since $\overline{X} \neq 1$. Hence the first claim follows from Lemma 2.3. The second claim is clear. □

Proposition 3.4. *We have* $\mathrm{O}_5(G) = 1$.

Proof. Let R, $\overline{G}$ and f be as in Lemma 3.3, and let $|R| = 5^r$. Then $\mathrm{O}_5(\overline{G}) = 1$, and $\overline{G}$ is generated by its 5-elements by Lemma 2.6(b). Suppose that $R \neq 1$. We partition $\mathcal{S}_a(G)$ into the sets $\mathcal{A} := \{Q : Q \leq R\}$, $\mathcal{B} := \{Q : R < Q\}$ and $\mathcal{C} := \mathcal{S}_a(G) \setminus (\mathcal{A} \cup \mathcal{B})$. Then $|\mathcal{A}| = s_a(R)$, $|\mathcal{B}| = s_{a-r}(\overline{G})$ if $a > r$, $\mathcal{B} = \varnothing$ if $a \leq r$, and $\mathcal{A} = \varnothing$ if $a > r$. Moreover, $|\mathcal{C}| = \sum_{\overline{X}} f(\overline{X})$, where $\overline{X}$ runs through the nontrivial 5-subgroups of $\overline{G}$. If $\mathcal{C} = \varnothing$, then either $\mathcal{S}_a(G) = \mathcal{A}$ and $G = \langle \mathcal{S}_a(G) \rangle \leq R$, or $\mathcal{S}_a(G) = \mathcal{B}$ and R lies in the intersection of all members of $\mathcal{S}_a(G)$. Both contradict Lemma 2.6. Hence $\mathcal{C} \neq \varnothing$. Since $\mathcal{A} \cup \mathcal{B} \neq \varnothing$ (if $a > r$, then 5^{a-r} divides $|\overline{G}|$), we have $|\mathcal{C}| \leq 105$.

Let $\mathfrak{C}$ be a conjugacy class of $\overline{G}$ consisting of 5-subgroups $\overline{X}$ with $f(\overline{X}) > 0$. By Lemma 3.3, $|\mathfrak{C}| \cdot 5 \leq |\mathcal{C}| \leq 105$, so $|\mathfrak{C}| \leq 21$. Let T be the permutation group induced by $\overline{G}$ on $\mathfrak{C}$ by conjugation. Then T is transitive and generated by its 5-elements, and the image $\widehat{X}$ of $\overline{X} \in \mathfrak{C}$ in T is a normal 5-subgroup of the stabilizer of $\overline{X}$. If $\widehat{X} = 1$, then $\overline{X}$ normalizes all members of $\mathfrak{C}$, so any two members of $\mathfrak{C}$ normalize each other and $\langle \mathfrak{C} \rangle$ is a normal 5-subgroup of $\overline{G}$. Since $\mathrm{O}_5(\overline{G}) = 1$, this is impossible. Hence T is a transitive group of degree $|\mathfrak{C}| \leq 21$, generated by its 5-elements, whose point stabilizers have a nontrivial normal 5-subgroup. By the library of transitive groups in GAP, $|\mathfrak{C}| \in \{6, 11, 12, 16\}$ (see Section 5(1)). Summing over all such classes and using Lemma 3.3, we obtain $|\mathcal{C}| = 5k$ with $k \in \{6x+11y+12z+16w : x, y, z, w \geq 0\}$ and $1 \leq k \leq 21$. The only possibilities are $k \in \{6, 11, 12, 16, 17, 18\}$, so

$$|\mathcal{C}| \in \{30, 55, 60, 80, 85, 90\} \quad \text{and} \quad |\mathcal{A} \cup \mathcal{B}| = 106 - |\mathcal{C}| \in \{76, 51, 46, 26, 21, 16\}.$$

If $a \leq r$, then $|\mathcal{A}| = s_a(R)$ is 1 or congruent to 6 modulo 25 by Proposition 2.1, since R is a 5-group. None of the numbers above has this property.

Hence $a > r$, and $t := s_{a-r}(\overline{G}) \in \{76, 51, 46, 26, 21, 16\}$. Every $Q \in \mathcal{C}$ satisfies $|QR/R| = 5^a/|Q \cap R| > 5^{a-r}$, since $Q \cap R < R$. Therefore, the Sylow 5-subgroup $\overline{P}$ of $\overline{G}$ has order larger than 5^{a-r}. By Proposition 2.1(b), t is congruent to 1 or 6 modulo 25, and $t \equiv 1 \pmod{25}$ only if $\overline{P}$ is cyclic. This leaves $t \in \{76, 51, 26\}$ and $\overline{P}$ cyclic. Let $\overline{X} = QR/R$ for some $Q \in \mathcal{C}$, and let $|\overline{X}| = 5^c > 5^{a-r}$. Since $\overline{P}$ is cyclic, the subgroups of order 5^c of $\overline{G}$ form a single conjugacy class $\mathfrak{C}$, and every subgroup of order 5^{a-r} is contained in one of them. Each member of $\mathfrak{C}$ contains exactly one subgroup of order 5^{a-r}, so $|\mathfrak{C}| \geq t \geq 26$. This contradicts $|\mathfrak{C}| \leq 21$. □

Lemma 3.5. *Let L be a nonabelian simple group.*

(a) If L has a nontrivial 5-subgroup Y with $|L : \mathrm{N}_L(Y)| \leq 106$, then L is isomorphic to A_5, A_6, $\mathrm{PSL}(2, 11)$, $\mathrm{PSL}(2, 25)$ or $\mathrm{PSL}(3, 5)$.

(b) If X is a nontrivial 5-subgroup of $\mathrm{Aut}(L)$ with $X \cap \mathrm{Inn}(L) = 1$, then $|L : \mathrm{C}_L(X)| > 106$.

Proof. In both cases we may assume that L has a proper subgroup of index at most 106. Then L has a maximal subgroup of index at most 106, and L is a primitive permutation group of degree at most 106.

(a) For the simple primitive groups of degree at most 106 other than A_m with $m \geq 25$, the claim was verified with GAP (see Section 5(2)). It remains to consider $L \cong A_m$ with $25 \leq m \leq 106$. Then $|L : \mathrm{N}_L(Y)| \leq 106 < \binom{m}{2}$. By [4, Theorem 5.2A] with $r = 2$, either $\mathrm{N}_L(Y)$ contains the stabilizer A_{m-1} of a point, or m is even and $\mathrm{N}_L(Y)$ stabilizes a partition into two blocks of size $m/2$ (the exceptional cases of that theorem have degree at most 9). In the second case, $|L : \mathrm{N}_L(Y)| \geq \frac{1}{2}\binom{m}{m/2} > 106$. Hence $A_{m-1} \leq \mathrm{N}_L(Y) < L$. Since A_{m-1} is maximal and simple, $\mathrm{N}_L(Y) = A_{m-1}$, $Y \trianglelefteq A_{m-1}$ and $Y = 1$, a contradiction.

(b) Since 5 divides $|\mathrm{Out}(L)|$, L is not alternating. By Section 5(2), the only simple primitive group of degree at most 106 with $|\mathrm{Out}(L)|$ divisible by 5 is $\mathrm{PSL}(2,32)$. Then $\mathrm{Out}(L) \cong C_5$, so $|X| = 5$, and $|\mathrm{C}_L(X)| = 6$ by Section 5(2). Hence $|L : \mathrm{C}_L(X)| \geq 32736/6 > 106$. □

Proposition 3.6. *The group G is a direct product of simple groups, and each factor is isomorphic to one of A_5, A_6, $\mathrm{PSL}(2,11)$, $\mathrm{PSL}(2,25)$ and $\mathrm{PSL}(3,5)$.*

Proof. By Proposition 3.2 and Proposition 3.4, the Fitting subgroup of G is trivial. Hence $E := \mathrm{F}^*(G)$ is the direct product of the components $L_1, \ldots, L_k$ of G, and these are simple (see [8, Theorem 9.7]). Moreover, $\mathrm{C}_G(E) \leq E$ by [8, Theorem 9.8], so $\mathrm{C}_G(E) = \mathrm{Z}(E) = 1$. Since $\mathrm{O}_{5'}(G) = 1$, every L_i has order divisible by 5.

Suppose that some $Q \in \mathcal{S}_a(G)$ does not normalize some component L. Then some $q \in Q$ moves L, and the orbit Δ of L under $\langle q \rangle$ consists of $m := 5^j \geq 5$ components, which are permuted cyclically by q. Let E_Δ be the product of the components in Δ, and let S be a Sylow 5-subgroup of L. If $e \in \mathrm{N}_{E_\Delta}(Q)$, then $[e,q] = e^{-1}e^q \in Q \cap E_\Delta$. Moreover, for $e_1, e_2 \in E_\Delta$ we have $[e_1,q] = [e_2,q]$ if and only if $e_2 e_1^{-1} \in \mathrm{C}_{E_\Delta}(q)$. An element of $\mathrm{C}_{E_\Delta}(q)$ is determined by its component in L, so $|\mathrm{C}_{E_\Delta}(q)| \leq |L|$. Since $Q \cap E_\Delta$ is a 5-subgroup of E_Δ, we obtain

$$|E_\Delta : \mathrm{N}_{E_\Delta}(Q)| \geq \frac{|L|^m}{|L| \cdot |S|^m} = \frac{|L:S|^{m-1}}{|S|} \geq \frac{|L:S|^4}{|S|}.$$

By [9, Theorem 3.6], $|L| > |S|^2$, so $|L : S| > |S| \geq 5$ and $|L : S|^4/|S| > |S|^3 > 106$. Since the E_Δ-conjugates of Q lie in $\mathcal{S}_a(G)$, this is a contradiction.

Consequently, every member of $\mathcal{S}_a(G)$ normalizes every component, and Lemma 2.6(b) shows that $L_i \trianglelefteq G$ for all i. If all members of $\mathcal{S}_a(G)$ centralize L_i, then $L_i \leq \mathrm{Z}(G)$, which is impossible. Choose $Q \in \mathcal{S}_a(G)$ which acts nontrivially on L_i, and let X be the image of Q in $\mathrm{Aut}(L_i)$. The L_i-conjugates of Q lie in $\mathcal{S}_a(G)$, so $|L_i : \mathrm{N}_{L_i}(X)| \leq |L_i : \mathrm{N}_{L_i}(Q)| \leq 106$, where we identify L_i with $\mathrm{Inn}(L_i)$. If $X \cap \mathrm{Inn}(L_i) = 1$, then $[\mathrm{N}_{L_i}(X), X] \leq \mathrm{Inn}(L_i) \cap X = 1$ and $\mathrm{N}_{L_i}(X) = \mathrm{C}_{L_i}(X)$, which contradicts Lemma 3.5(b). Hence $Y := X \cap \mathrm{Inn}(L_i) \neq 1$ and $\mathrm{N}_{L_i}(X) \leq \mathrm{N}_{L_i}(Y)$. By Lemma 3.5(a), L_i is one of the five groups in the statement. Their outer automorphism groups are 2-groups. Since G embeds into $\prod_i \mathrm{Aut}(L_i)$, the group G/E is a 2-group, and Lemma 2.6(b) yields $G = E$. □

Theorem 3.7. *Every critical group is a 5-group.*

Proof. Suppose that G is critical and not a 5-group. By Proposition 3.6, P is a direct product of groups isomorphic to C_5 or the extraspecial group 5_+^{1+2} of exponent 5. In particular, P has exponent 5, and Lemma 2.7 applied to $X = H = P$ and $K = 1$ shows $a \geq n-2$, since $s_a(P) \leq 81$. The subgroups of index 5 or 25 in P containing $\Phi(P)$ show that $d(P) \leq 3$, since $\frac{5^4-1}{5-1} = 156$ and $\frac{(5^4-1)(5^3-1)}{(5^2-1)(5-1)} = 806$. Since P is not cyclic, G is one of the following: $L_1 \times L_2$ or $L_1 \times L_2 \times L_3$ with $L_i \in \{A_5, A_6, \mathrm{PSL}(2,11)\}$, $\mathrm{PSL}(2,25)$, $\mathrm{PSL}(3,5)$, $L_1 \times \mathrm{PSL}(2,25)$ or $L_1 \times \mathrm{PSL}(3,5)$ with $L_1 \in \{A_5, A_6, \mathrm{PSL}(2,11)\}$. For all these groups and $a \in \{n-2, n-1\}$ with $a \geq 1$, we have $s_a(G) \geq 156$ (see Section 5(3)). This is a contradiction. □

4 5-groups

In this section, G is a critical group. By Theorem 3.7, $G = P$ is a 5-group. Let $d := d(P)$ be the minimal number of generators, $F := \Phi(P)$ and $V := P/F \cong C_5^d$. For a subspace $U \leq V$ let H_U be its preimage in P, and let $f(U)$ be the number of $Q \in \mathcal{S}_a(P)$ with $QF = H_U$.

Lemma 4.1. *Let $L \leq V$ be a line and let $g \in H_L \setminus F$ with $g^{5^a} = 1$. Suppose that $5^{a-1} < |F|$. Then $f(L) \geq 5$ and $f(L) \equiv 0 \pmod 5$.*

Proof. Let $\mathcal{A}$ be the set of subgroups of order 5^{a-1} of F containing $\langle g^5 \rangle$. Since $|\langle g^5 \rangle| \leq 5^{a-1} < |F|$, we have $|\mathcal{A}| \equiv 1 \pmod 5$ by [1, Theorem 5.14] (if $|\langle g^5 \rangle| = 5^{a-1}$, then $\mathcal{A} = \{\langle g^5 \rangle\}$). Conjugation by g permutes $\mathcal{A}$, so g normalizes some $A \in \mathcal{A}$. Then $Q := \langle g \rangle A$ has order 5^a and $QF = H_L$. Hence $f(L) > 0$.

For $Q \in \mathcal{S}_a(P)$ with $QF = H_L$, we have $|Q \cap F| = |Q||F|/|H_L| = 5^{a-1} < |F|$, so $F \not\leq Q$. Since $F < H_L$, Lemma 2.3 yields $f(L) \equiv 0 \pmod 5$. □

For a p-group X let $\mho_1(X) := \langle x^p : x \in X \rangle$ and $\Omega_1(X) := \langle x \in X : x^p = 1 \rangle$. Recall that X is *regular* if for all $x, y \in X$ there exists $c \in \mho_1(\langle x, y \rangle')$ with $x^p y^p = (xy)^p c$ (see [1, §7]). Moreover, X is *absolutely regular* if $|X : \mho_1(X)| < p^p$ (see [1, §9]). Absolutely regular p-groups are regular by [1, Theorem 9.8(a)].

Proposition 4.2. *If $a \leq n - 3$, then P is regular.*

Proof. Suppose that P is irregular. Then P is not absolutely regular, that is, $|P : \mho_1(P)| \geq 5^5$. Applying Lemma 2.7 to $H = P$ and $K = \mho_1(P)$ shows that $|\mho_1(P)| \geq 5^a$, since $|P| \geq 5^{a+3}$. Let $K \leq \mho_1(P)$ be a normal subgroup of P of order 5^{a-1} and $\overline{P} := P/K$. The preimages of the subgroups of order 5 of $\overline{P}$ are subgroups of order 5^a of P, so $s_1(\overline{P}) \leq 106$. Since $K \leq \mho_1(P)$, we have $\mho_1(\overline{P}) = \mho_1(P)/K$ and $|\overline{P} : \mho_1(\overline{P})| = |P : \mho_1(P)| \geq 5^5$. Hence, $\overline{P}$ is not absolutely regular. If $\overline{P}$ is not of maximal class, then $\overline{P}$ has a normal subgroup of order 5^5 and exponent 5 by [1, Theorem 12.1(a)], so $s_1(\overline{P}) \geq (5^5 - 1)/4 = 781$. Therefore, $\overline{P}$ is of maximal class. If $|\overline{P}| = 5^5$, then $|\overline{P} : \mho_1(\overline{P})| \geq 5^5$ forces $\mho_1(\overline{P}) = 1$, and again $s_1(\overline{P}) = 781$. Hence $|\overline{P}| \geq 5^6$. If $|\overline{P}| \geq 5^7$, then $s_1(\overline{P}) \geq 156$ by [1, Lemma 12.3]. Finally, all 39 groups of maximal class of order 5^6 satisfy $s_1 \geq 156$ (see Section 5(4)). In each case, $s_1(\overline{P}) \geq 156$ contradicts $s_1(\overline{P}) \leq 106$. □

Proposition 4.3. *We have $a = n - 2$.*

Proof. The subgroups of index 5 in P correspond to the hyperplanes of V. Hence $s_{n-1}(P) = (5^d - 1)/4 \neq 106$ and $a \leq n - 2$. Suppose that $a \leq n - 3$. Applying Lemma 2.7 to $H = P$ and $K = F$ yields $|F| \geq 5^a$. By Proposition 4.2, P is regular. By [1, Theorem 7.2], the elements x with $x^{5^a} = 1$ form a subgroup. It contains all members of $\mathcal{S}_a(P)$, so it is P by Lemma 2.6(b). Hence, Lemma 4.1 applies to every line $L \leq V$. Since every $Q \in \mathcal{S}_a(P)$ satisfies $QF < P$, we have

$$106 = s_a(F) + \sum_{0 \neq U < V} f(U). \tag{4.1}$$

If $d \geq 3$, then (4.1) yields $106 \geq \sum_L f(L) \geq 31 \cdot 5$, a contradiction. Hence $d = 2$ (note that P is not cyclic), and (4.1) reads $106 = s_a(F) + \sum_{i=0}^{5} f(L_i)$, where $L_0, \ldots, L_5$ are the lines of V and $f(L_i) = s_a(H_{L_i}) - s_a(F)$. Every proper subgroup H of P with $|H| > 5^a$ satisfies $s_a(H) \leq s_a(P) = 106$,

and $s_a(H) \neq 106$ by the minimality of P. Moreover, $s_a(H)$ is congruent to 1 or 6 modulo 25 by Proposition 2.1(b), and if $s_a(H) \equiv 1 \pmod{25}$, then H is cyclic and $s_a(H) = 1$. Since $|F| = 5^{n-2} > 5^a$, it follows that $s_a(F)$ and all $s_a(H_{L_i})$ lie in $\{1, 6, 31, 56, 81\}$.

If $s_a(F) \geq 6$, then every $f(L_i)$ is a positive difference of two elements of $\{6, 31, 56, 81\}$, so $f(L_i) \geq 25$ and $106 \geq 6 + 6 \cdot 25$, a contradiction. Hence $s_a(F) = 1$, and F is cyclic by Proposition 2.1(b). Hence H_{L_i} has a cyclic subgroup of index 5, so H_{L_i} is abelian or isomorphic to $M_{5^{n-1}}$ by [1, Theorem 1.2]. In particular, $|\Omega_1(H_{L_i})| \leq 25$, which gives $s_1(H_{L_i}) \leq 6$. For $a \geq 2$, we have $s_a(H_{L_i}) \leq 6$ by the proof of [1, Theorem 5.3]. Therefore $f(L_i) = s_a(H_{L_i}) - 1 \leq 5$ and $106 \leq 1 + 6 \cdot 5$, a contradiction. □

Proposition 4.4. *We have $d = 2$.*

Proof. By Proposition 4.3, $a = n - 2$. The subgroups of index 25 in P containing F correspond to the subspaces of codimension 2 in V. If $d \geq 4$, there are at least $\frac{(5^4-1)(5^3-1)}{(5^2-1)(5-1)} = 806$ of them, a contradiction. Suppose that $d = 3$. Let Γ_1 and Γ_2 be the sets of subgroups of index 5 and 25 containing F. Since $|F| = 5^{n-3}$, Hall's enumeration principle [1, Theorem 5.2] applied to $\mathcal{S}_a(P)$ gives

$$s_a(P) = \sum_{M \in \Gamma_1} s_a(M) - 5 \sum_{H \in \Gamma_2} s_a(H) = \sum_{M \in \Gamma_1} \frac{5^{d(M)} - 1}{4} - 5 \cdot 31,$$

since $s_a(H) = 1$ for $H \in \Gamma_2$. Every $M \in \Gamma_1$ satisfies $M/F \cong C_5^2$, so $d(M) \geq 2$, and $s_a(P) = 106$ becomes $\sum_{M \in \Gamma_1} (5^{d(M)} - 1)/4 = 261$. Since $156 + 30 \cdot 6 > 261$, every summand is 6 or 31, and $261 = 3 \cdot 31 + 28 \cdot 6$ shows that exactly three summands equal 31. Hence exactly three members $M_1, M_2, M_3 \in \Gamma_1$ satisfy $d(M_i) = 3$, and $d(M) = 2$ for the others. Since $\Phi(M) \leq \Phi(P) = F$, we have $\Phi(M) = F$ if $d(M) = 2$, and $|F : \Phi(M_i)| = 5$. Every subgroup of index 25 in P is a maximal subgroup of some $M \in \Gamma_1$ and contains $\Phi(M)$. Therefore, the intersection of all members of $\mathcal{S}_a(P)$ contains $\Phi(M_1) \cap \Phi(M_2) \cap \Phi(M_3)$, which has index at most 5^3 in F. By Lemma 2.6(c), $|F| \leq 5^3$ and $n \leq 6$. This contradicts Section 5(5). □

We use left normed commutators: for elements x, y, z of a group let $x^y := y^{-1}xy$, $[x, y] := x^{-1}x^y$ and $[x, y, z] := [[x, y], z]$, and similarly $[X, Y, Z] := [[X, Y], Z]$ for subgroups X, Y, Z.

Proposition 4.5. *The following hold:*

(a) Three maximal subgroups M of P satisfy $d(M) = 3$, and the other three satisfy $d(M) = 2$.

(b) $\bigcap_M \Phi(M) = 1$, where M runs through the maximal subgroups of P.

(c) F is elementary abelian.

(d) $[F, P] \leq \mathrm{Z}(P)$.

(e) $\mho_1(P) \leq \mathrm{Z}(P)$.

(f) $|P| \leq 5^5$.

Proof. By Proposition 4.3 and Proposition 4.4, $d = 2$ and $a = n - 2$. Let $M_0, \ldots, M_5$ be the maximal subgroups of P. Any two of them intersect in F, so F is a maximal subgroup of every M_i, and every other subgroup of index 25 in P is a maximal subgroup of exactly one M_i.

(a) Since M_i has exactly $(5^{d(M_i)}-1)/4$ maximal subgroups, we obtain

$$106 = s_a(P) = \sum_{i=0}^{5} \frac{5^{d(M_i)}-1}{4} - 5,$$

that is, $\sum_{i=0}^{5}(5^{d(M_i)}-1)/4 = 111$. Since $(5^4-1)/4 = 156 > 111$, all summands lie in $\{1, 6, 31\}$. Let x_1, x_6 and x_{31} be the number of summands equal to 1, 6 and 31 respectively. Then $x_1+x_6+x_{31} = 6$ and $x_1 + 6x_6 + 31x_{31} = 111$. Subtracting yields $x_6 + 6x_{31} = 21$, and the only solution with $x_6 + x_{31} \leq 6$ is $x_6 = x_{31} = 3$, $x_1 = 0$.[1]

(b) The intersection of all members of $\mathcal{S}_a(P)$ is $F \cap \bigcap_i \Phi(M_i) = \bigcap_i \Phi(M_i)$. Hence the claim follows from Lemma 2.6(c).

(c) Since $\Phi(F) \leq \Phi(M)$ for every maximal subgroup M, we obtain $\Phi(F) = 1$ by (b).

(d) Let $M = \langle g \rangle F$ be a maximal subgroup of P, let $h \in P \setminus M$ and $\overline{P} := P/\Phi(M)$. Since $\overline{F}$ is an abelian normal subgroup of $\overline{P}$, the map $\delta\colon \overline{F} \to \overline{F}$, $x \mapsto [x, \overline{h}]$ is a homomorphism. Since F is abelian and $[F, g] \leq M' \leq \Phi(M)$, the group $\overline{M}$ centralizes $\overline{F}$. Together with $\overline{P} = \langle \overline{h} \rangle \overline{M}$, this implies that the image of $[F, P, P]$ in $\overline{P}$ is $\delta^2(\overline{F})$. Since $\overline{P}$ is nilpotent, δ is nilpotent. As $\overline{F}$ is an elementary abelian group of order $|F : \Phi(M)| = 5^{d(M)-1} \leq 25$ by (a), we obtain $\delta^2 = 0$, that is, $[F, P, P] \leq \Phi(M)$. Since M was arbitrary, (b) yields $[F, P, P] = 1$.

(e) By (c) and (d), P has nilpotency class at most 3, so P is regular by [1, Theorem 7.1(b)]. Since $P' \leq F$ has exponent 5, it follows that $(gh)^5 = g^5h^5$ for all $g, h \in P$. Hence $(g^5)^h = (g^h)^5 = (g[g, h])^5 = g^5[g, h]^5 = g^5$ for all $g, h \in P$.

(f) Let $P = \langle x, y \rangle$ and $w := [x, y]$. Since $P' = \langle w \rangle [P', P]$ with $[P', P] \leq [F, P] \leq \mathrm{Z}(P)$, (e) yields $F = P'\mho_1(P) = \langle w \rangle Z$ with $Z \leq \mathrm{Z}(P)$. By (a), there exists a maximal subgroup $M = \langle g \rangle F$ of P with $d(M) = 2$. Then $M' = [F, g] = \langle [w, g] \rangle$. Moreover, $\mho_1(M) = \langle g^5 \rangle$, since $(g^i f)^5 = g^{5i} f^5 = g^{5i}$ for $f \in F$ by the proof of (e). Hence $|\Phi(M)| = |M'\mho_1(M)| \leq 25$. On the other hand, $|F : \Phi(M)| = 5^{d(M)-1} = 5$. Therefore, $|F| \leq 5^3$ and $|P| \leq 5^5$. □

Proof of Theorem A. If there is a group H with $s_a(H) = 106$ for some a, then there is a critical group G. By Theorem 3.7, $G = P$ is a 5-group. By Proposition 4.5(f), $|P| \leq 5^5$, which contradicts Section 5(5). □

Proof of Corollary B. Let $n < 106$ with $n \equiv 1 + p \pmod{p^2}$. Since every odd number is a Sylow 2-number [11], we may assume that $p > 2$. For $p = 3$, the integers $n < 100$ are Frobenius 3-numbers by [10], and 103 is a prime, hence a Sylow 3-number by [11]. For $p = 5$, we have $n \in \{6, 31, 56, 81\}$, and these values occur as $s_a(P)$ for 5-groups P (see Section 5(5)). For $p = 7$, we have $n \in \{8, 57\}$, and $8 = s_1(C_7^2)$, $57 = s_1(C_7^3)$. For $p \geq 11$, we have $n = 1 + p = s_1(C_p^2)$. (In fact, all these integers occur as $s_a(P)$ for p-groups P of order at most p^7, see [3, Appendix A.1].) Hence, the claim follows from Theorem A. □

[1] A positive answer to [2, Problem 1375] would exclude this configuration directly, but `SmallGroup`$(5^5, 4)$ has exactly four two-generator maximal subgroups and shows that the answer is negative (see the file `problem1375.g` attached to this pdf).

5 Computations

All computations were done with GAP 4.16.1 [5]. The code is attached to this pdf: `transitive.g` for (1), `simple.g`, `outer-automorphisms.g` and `psl2-32.g` for (2), `products.g` for (3), `maximal-class.g` for (4) and `small-5-groups.g` for (5). To compute $s_a(H)$ for a group H, we computed the conjugacy classes of subgroups of a Sylow 5-subgroup S, collected the members of order 5^a, sorted them into conjugacy classes of H and added the indices of their normalizers.

(1) The transitive groups of degree at most 21 which are generated by 5-elements and whose point stabilizers have a nontrivial normal 5-subgroup are A_5 of degree 6 and 12, $C_{11} \rtimes C_5$ of degree 11 and $C_2^4 \rtimes C_5$ of degree 16.

(2) Among the nonabelian simple primitive groups of degree at most 106 other than A_m with $m \geq 25$, those with a nontrivial 5-subgroup having at most 106 conjugates are A_5, A_6, $\mathrm{PSL}(2,11)$, $\mathrm{PSL}(2,25)$ and $\mathrm{PSL}(3,5)$. Among all simple primitive groups of degree at most 106 other than alternating groups of degree at least 7, only $\mathrm{PSL}(2,32)$ has an outer automorphism group of order divisible by 5, and every subgroup X of order 5 of $\mathrm{Aut}(\mathrm{PSL}(2,32))$ with $X \cap \mathrm{Inn}(\mathrm{PSL}(2,32)) = 1$ satisfies $|\mathrm{C}_{\mathrm{PSL}(2,32)}(X)| = 6$.

(3) For the 24 groups listed in the proof of Theorem 3.7, the smallest value of $s_a(G)$ with $a \in \{n-2, n-1\}$ is 156, attained by $A_5 \times A_5$ $(a = 1)$ and $\mathrm{PSL}(2,25)$ $(a = 1)$.

(4) The groups of maximal class of order 5^6 are $\mathtt{SmallGroup}(5^6, i)$ with $630 \leq i \leq 668$. They satisfy $s_1 \in \{156, 781, 1406, 2031, 3281\}$.

(5) For all noncyclic groups P of order 5^m with $m \leq 5$ and for all groups of order 5^6 with $d(P) = 3$, the values $s_a(P)$ with $1 \leq a \leq m-1$ and $s_a(P) \leq 181$ are exactly $6, 31, 56, 81, 156, 181$. In particular, $s_a(P) \neq 106$.

Acknowledgment

Anthropic Claude Opus 5.5 assisted in the preparation of this paper. I have checked all details and take full responsibility for the contents of this paper.

References

[1] Y. Berkovich, *Groups of prime power order. Vol. 1*, de Gruyter Expositions in Mathematics, Vol. 46, Walter de Gruyter GmbH & Co. KG, Berlin, 2008.

[2] Y. Berkovich and Z. Janko, *Groups of prime power order. Vol. 2*, de Gruyter Expositions in Mathematics, Vol. 47, Walter de Gruyter GmbH & Co. KG, Berlin, 2008.

[3] L. B. Blaas, *Strong pseudo Frobenius numbers*, Master's thesis, Leibniz Universität Hannover, 2022.

[4] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, Vol. 163, Springer-Verlag, New York, 1996.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.16.1*; 2026, `https://www.gap-system.org`.

[6] M. Hall, *On the number of Sylow subgroups in a finite group*, J. Algebra **7** (1967), 363–371.

[7] P. Hall, *On a Theorem of Frobenius*, Proc. London Math. Soc. (2) **40** (1935), 468–501.

[8] I. M. Isaacs, *Finite group theory*, Graduate Studies in Mathematics, Vol. 92, American Mathematical Society, Providence, RI, 2008.

[9] W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague, *Composition factors from the group ring and Artin's theorem on orders of simple groups*, Proc. London Math. Soc. (3) **60** (1990), 89–122.

[10] B. Sambale, *Pseudo Frobenius numbers*, Expo. Math. **37** (2019), 200–206.

[11] B. Sambale, *Pseudo Sylow numbers*, Amer. Math. Monthly **126** (2019), 60–65.

[12] Q. Zhang and H. Qu, *On Hua-Tuan's conjecture II*, Sci. China Math. **54** (2011), 65–74.