Bull. Aust. Math. Soc. **109** (2024), 529–540
doi:10.1017/S0004972723000783

GROUPS WITH FEW NONPOWER SUBGROUPS

JIWEI ZHENG, WEI ZHOU✉ and D. E. TAYLOR

(Received 22 May 2023; accepted 29 June 2023; first published online 10 August 2023)

Abstract

For a group G and $m \geq 1$, let G^m denote the subgroup generated by the elements g^m, where g runs through G. The subgroups not of the form G^m are the nonpower subgroups of G. We classify the groups with at most nine nonpower subgroups.

2020 *Mathematics subject classification*: primary 20D25; secondary 20D60.

Keywords and phrases: counting subgroups, power subgroups, nonpower subgroups.

1. Introduction

For a group G and $m \geq 1$, the *power* subgroup G^m is the subgroup generated by the elements g^m, where g runs through G. A subgroup that is not a power subgroup is a *nonpower* subgroup. Let $\mathrm{ps}(G)$ and $\mathrm{nps}(G)$ denote the number of power and nonpower subgroups of G. It is immediate that every power subgroup is a characteristic subgroup of G. But the converse is false, as illustrated by $M_{n,p}$ defined in Section 3: it has a unique maximal noncyclic subgroup, which is characteristic but not a power subgroup.

The study of nonpower subgroups was initiated by Szász [7] who proved that G is cyclic if and only if $\mathrm{nps}(G) = 0$. The terminology 'nonpower subgroup' was introduced by Zhou *et al.* [9]. They proved that a noncyclic group G is finite if and only if $\mathrm{nps}(G)$ is finite. Furthermore, if G is a finite noncyclic group, it was proved by Zhou and Ping that $\mathrm{nps}(G) \geq 3$. Therefore, from now on, we assume that all groups under consideration are finite.

For the most part, our notation follows Gorenstein [6]. In particular, $\Phi(G)$ denotes the Frattini subgroup of G, and for subgroups H and K, $[H, K]$ is generated by the commutators $[x, y] = x^{-1}y^{-1}xy$ with $x \in H$ and $y \in K$. For a finite p-group G, let $\Omega_i(G)$ be the subgroup $\langle x \in G \mid x^{p^i} = 1\rangle$ for $i \geq 1$. We use [6, Ch. 5] as a reference for standard results about p-groups.

Anabanti *et al.* [1, 2] classified the groups G with $\mathrm{nps}(G) \in \{3, 4\}$ and showed that, for all $k > 4$, there are infinitely many groups G with $\mathrm{nps}(G) = k$.

This work was supported by the National Natural Science Foundation of China (11971391, 12071376).

The following theorem extends the classification to the groups G with $\mathrm{nps}(G) \le 9$. For completeness, we include the results for $\mathrm{nps}(G) \le 4$.

Let C_n denote the cyclic group of order n and let $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$ denote the alternating and symmetric groups of a set of size n. See Definition 2.5 for descriptions of the other groups referred to in the following theorem.

THEOREM 1.1. *For $0 \le k \le 9$, a group has exactly k nonpower subgroups if and only if, up to isomorphism, it is one of the following:*

- $k = 0$ *a cyclic group;*
- $k = 1$ *no examples;*
- $k = 2$ *no examples;*
- $k = 3$ $C_2 \times C_2$, Q_8 *or* $G_{n,3}$ *for* $n \ge 1$*;*
- $k = 4$ $C_3 \times C_3$*;*
- $k = 5$ $C_2 \times C_4$ *or* $G_{n,5}$ *for* $n \ge 1$*;*
- $k = 6$ $C_5 \times C_5$, $C_2 \times C_2 \times C_p$, $Q_8 \times C_p$, *where* $p > 2$ *is a prime, or* $G_{n,3} \times C_q$ *for* $n \ge 1$, *where* $q > 3$ *is a prime;*
- $k = 7$ D_8, $\mathrm{Alt}(4)$, $C_2 \times C_8$, Q_{16}, $M_{4,2}$, $C_3 \times C_9$, $M_{3,3}$, $G_{n,7}$ *or* $F_{n,7}$ *for* $n \ge 1$*;*
- $k = 8$ $C_7 \times C_7$ *or* $C_3 \times C_3 \times C_p$, *where* $p \ne 3$ *is a prime;*
- $k = 9$ $C_2 \times C_{16}$, $M_{5,2}$, $C_2 \times C_2 \times C_{p^2}$, $Q_8 \times C_{p^2}$, *where* $p > 2$ *is a prime, or* $G_{n,3} \times C_{q^2}$, *where* $q > 3$ *is a prime.*

2. Preliminaries

Recall that the *exponent* $\exp(G)$ of a finite group G is the least positive integer e such that $g^e = 1$ for all $g \in G$. The number of positive divisors of an integer n is denoted by $\tau(n)$.

LEMMA 2.1. *The power subgroups of a finite group G are the subgroups G^d, where d is a divisor of the exponent of G. Thus,* $\mathrm{ps}(G) \le \tau(\exp(G))$.

PROOF. Given $m \ge 1$, we prove that $G^m = G^n$, where $n = \gcd(m, e)$ and e is the exponent of G. To this end, we may write $n = am + be$ and $m = dn$ for some integers a, b and d. Then, for all g in G, $g^m = g^{nd} \in G^n$ and $g^n = g^{am+be} = g^{ma} \in G^m$, from which we get $G^m = G^n$. □

LEMMA 2.2 [1, Lemma 3]. *If A and B are finite groups such that $|A|$ and $|B|$ are coprime, then* $\mathrm{ps}(A \times B) = \mathrm{ps}(A)\,\mathrm{ps}(B)$ *and* $\mathrm{nps}(A \times B) = \mathrm{nps}(A)s(B) + \mathrm{ps}(A)\,\mathrm{nps}(B)$, *where $s(B)$ is the number of subgroups of B.*

COROLLARY 2.3. *For any finite abelian group G, we have* $\mathrm{ps}(G) = \tau(\exp(G))$.

PROOF. From Lemma 2.2, it is no loss to assume that G is an abelian p-group. Then, by Lemma 2.1, it suffices to prove that, for different divisors m and n of $\exp(G)$, we have $G^n \ne G^m$. Let $\exp(G) = p^e$ and $e \ge i > j \ge 0$. Then $G^{p^i} = (G^{p^j})^{p^{i-j}} < G^{p^j}$. □

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

LEMMA 2.4 [9, Lemma 2]. *Suppose that N and H are subgroups of G such that $N \trianglelefteq G$ and $N \subseteq H$. If H/N is a nonpower subgroup of G/N, then H is a nonpower subgroup of G. Therefore,* $\mathrm{nps}(G) \geq \mathrm{nps}(G/N)$.

DEFINITION 2.5.

(i) For $n \geq 3$, $\langle a, b \mid a^n = b^2 = 1,\ b^{-1}ab = a^{-1}\rangle$ is a presentation for the *dihedral* group D_{2n} of order $2n$.

(ii) For $n \geq 3$, $\langle a, b \mid a^{2^{n-1}} = b^2 = z,\ z^2 = 1,\ b^{-1}ab = a^{-1}\rangle$ is a presentation for the *generalised quaternion* group Q_{2^n} of order 2^n.

(iii) For $n \geq 4$, $\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ b^{-1}ab = a^{-1+2^{n-2}}\rangle$ is a presentation for the *semidihedral* group S_{2^n} of order 2^n.

(iv) For $n \geq 4$ when $p = 2$ and $n \geq 3$ when p is an odd prime, a presentation for the *quasidihedral* group $M_{n,p}$ of order p^n is $\langle a, b \mid a^{p^{n-1}} = b^p = 1,\ b^{-1}ab = a^{1+p^{n-2}}\rangle$. The group $M_{3,p}$ is the *extraspecial* group of order p^3 and exponent p^2.

(v) For an odd prime p, $\langle x, y, z \mid x^p = y^p = z^p = 1,\ [x, z] = [y, z] = 1,\ [x, y] = z\rangle$ is a presentation for the *extraspecial* group $M(p)$ of order p^3 and exponent p.

(vi) For $k \geq 1$ and $n \geq 2$, $\langle a, b \mid a^{2^n} = b^k = 1,\ a^{-1}ba = b^{-1}\rangle$ is a presentation for the group $G_{n,k}$ of order $2^n k$. Note that $G_{1,k} = D_{2k}$ and $G_{n,2} = C_2 \times C_{2^n}$.

(vii) For $n \geq 1$ and a prime $p \equiv 1 \pmod 3$, choose $i \not\equiv 1 \pmod p$ such that $i^3 \equiv 1 \pmod p$. Then $\langle a, b \mid a^{3^n} = b^p = 1,\ a^{-1}ba = b^i\rangle$ is a presentation for the group $F_{n,p}$ of order $3^n p$.

(viii) For $n \geq 1$, $\langle a, b, c \mid a^{3^n} = b^2 = 1,\ bc = cb,\ b^a = c,\ c^a = bc\rangle$ is a presentation for the group $A_n = (C_2 \times C_2) \rtimes C_{3^n}$ of order $2^2 3^n$. When $n = 1$, $A_1 = \mathrm{Alt}(4)$.

(ix) For $n \geq 1$ and a prime p,

$$\langle a, b, c \mid [a, b] = c,\ a^p = b^{p^n} = c^p = 1,\ [a, c] = [b, c] = 1\rangle$$

is a presentation for the group $B^1_{n,p}$ of order p^{n+2}. Except for $B^1_{1,2} = D_8$, it is nonmetacyclic (see [4, Lemma 2.5]). The quotient mod $\langle c\rangle$ is $C_p \times C_{p^n}$ and, for p odd, $B^1_{1,p} = M(p)$.

(x) For $n \geq 1$ and a prime p,

$$\langle a, b, c \mid [a, b] = c,\ a^p = c,\ b^{p^n} = c^p = 1,\ [a, c] = [b, c] = 1\rangle$$

is a presentation for the group $B^2_{n,p}$ of order p^{n+2}. It is metacyclic: $\langle a\rangle$ is a normal cyclic subgroup with cyclic quotient. The quotient mod $\langle c\rangle$ is $C_p \times C_{p^n}$, $B^2_{1,2} = D_8$ and, for p odd, $B^2_{1,p} = M_{3,p}$.

There are some basic facts about a p'-group acting on a p-group in [6]. For the reader's convenience, we give these theorems as lemmas.

LEMMA 2.6 [6, Theorem 5.2.3]. *If A is a p'-group of automorphisms of the abelian p-group P, then $P = C_P(A) \times [P, A]$.*

LEMMA 2.7 [6, Theorem 5.3.5]. *If A is a p'-group of automorphisms of the p-group P, then $P = CH$, where $C = C_P(A)$ and $H = [P, A]$. In particular, if $H \subseteq \Phi(P)$, then $A = 1$.*

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

The p-groups with a cyclic maximal subgroup are well known. It is clear that C_{p^n} and $C_p \times C_{p^n}$ are the only abelian groups of this type. For the nonabelian case, we have the following lemma.

LEMMA 2.8 [6, Theorem 5.4.4]. *Let P be a nonabelian p-group of order p^n that contains a cyclic subgroup of index p. Then one of the following holds.*

(i) *p is odd and P is isomorphic to $M_{n,p}$, for $n \geq 3$.*
(ii) *$p = 2$, $n = 3$ and P is isomorphic to D_8 or Q_8.*
(iii) *$p = 2$, $n > 3$ and P is isomorphic to $M_{n,2}$, D_{2^n}, Q_{2^n} or S_{2^n}.*

The p-groups in Lemma 2.8 are well studied. We collect some basic facts in the following lemmas.

LEMMA 2.9 [6, Theorem 5.4.3]. *For $P = M_{n,p}$:*

(i) *$P' = \langle a^{p^{n-1}} \rangle$;*
(ii) *$\Phi(P) = Z(P) = \langle a^p \rangle$; and*
(iii) *$\Omega_i(P) = \langle a^{p^{n-i-1}}, b\rangle$ is abelian of type (p^i, p), $1 \leq i \leq n-2$.*

LEMMA 2.10 [6, Theorem 5.4.5]. *Let P be a nonabelian 2-group of order 2^n in which $|P/P'| = 4$. Then P is isomorphic to D_{2^n}, Q_{2^n} or S_{2^n}.*

LEMMA 2.11 [6, Theorem 5.5.1]. *A nonabelian p-group P of order p^3 is extraspecial and is isomorphic to one of the groups $M_{3,p}$, $M(p)$, D_8 or Q_8.*

THEOREM 2.12. *There is no finite p-group G such that $G/N \simeq M_{n,p}$, where N is a central subgroup of G of order p contained in G'.*

PROOF. From the presentation of $M_{n,p}$ in Definition 2.5, we may suppose that G has a presentation of the form

$$\langle a, b, c \mid a^{p^{n-1}} = c^i, b^p = c^j,\ c^p = 1,\ b^{-1}ab = a^{1+p^{n-2}}c^k, ac = ca,\ bc = cb\rangle,$$

where $N = \langle c \rangle$, $0 \leq i, j, k < p$ and not all i, j, k are zero. Since $c \in Z(G)$, it is clear that a^p commutes with b and hence $z = a^{p^{n-2}} \in Z(G)$. Therefore, $[a, b] = zc^k \in Z(G)$ and it follows from elementary properties of commutators that $G' = \langle zc^k \rangle$, which is a contradiction. □

From Lemmas 2.2, 2.5 and Theorem 2.3 in [4], we deduce the following lemma.

LEMMA 2.13. *For a nonabelian p-group G generated by two elements, let $R = \Phi(G')G_3$, where $G_3 = [[G, G], G]$. Then:*

(i) *R is the only maximal subgroup of G' that is normal in G;*
(ii) *G is metacyclic if and only if G/R is metacyclic; and*
(iii) *if the type of G/G' is (p, p^n) and G/R has no cyclic maximal subgroup, then G/R is isomorphic to $B^1_{n,p}$ or $B^2_{n,p}$.*

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

PROOF. (i) and (ii) are the statements of Lemma 2.2 and Theorem 2.3 in [4].

(iii) Let $H = G/R$. Since $H' = (G/R)' = G'R/R = G'/R$, we have $H/H' \simeq G/G'$ and $H' \subseteq Z(H)$. Thus, we may assume that $H/H' = \langle aH', bH' \rangle$. Then $H = \langle a, b \rangle$ and $H' = \langle c \rangle$, where $c = [a, b]$ and $|c| = p$. Thus, $c \in Z(H)$. Since the type of H/H' is (p, p^n), we have $a^p = c^i$, $b^{p^n} = c^j$ for suitable integers i, j. If $p \nmid j$, then $\langle b \rangle$ is a cyclic maximal subgroup of G/R, contrary to our assumption. Thus, $b^{p^n} = 1$. If $p \nmid i$, replacing c with c^i, we have $H \simeq B^2_{n,p}$. If $p \mid i$, then $H \simeq B^1_{n,p}$. □

3. A catalogue of nonpower values

The value of nps(G) for the groups that occur in the proof of Theorem 1.1 can be computed from their presentation or from the Small Groups Database using the computer algebra system MAGMA [5]. For ease of reference, we include some general formulas here.

PROPOSITION 3.1. *For an integer n and a prime p we have:*

(i) *for* $n \geq 3$, $\mathrm{nps}(D_{2^n}) = 2^n - 1$;
(ii) *for* $n \geq 3$, $\mathrm{nps}(Q_{2^n}) = 2^{n-1} - 1$;
(iii) *for* $n \geq 4$, $\mathrm{nps}(S_{2^n}) = 3 \cdot 2^{n-2} - 1$;
(iv) *for* $n \geq 3$, $\mathrm{nps}(M_{n,p}) = p(n-1) + 1$ *(when* $p = 2$, *assume that* $n \geq 4$*)*;
(v) $\mathrm{nps}(M(p)) = p^2 + 2p + 2$;
(vi) *if* $p > 2$, *then* $\mathrm{nps}(G_{n,p^k}) = p(p^k - 1)/(p-1)$;
(vii) *if* $p \equiv 1 \pmod 3$, *then* $\mathrm{nps}(F_{n,p}) = p$;
(viii) *for* $n \geq 1$, $\mathrm{nps}(A_n) = 3n + 4$;
(ix) *for* $n \geq 1$, $\mathrm{nps}(B^1_{n,p}) \geq 17$ *except that* $\mathrm{nps}(B^1_{1,2}) = 7$;
(x) *for* $n \geq 1$, $\mathrm{nps}(B^2_{n,p}) \geq 11$ *except that* $\mathrm{nps}(B^2_{1,2}) = \mathrm{nps}(B^2_{1,3}) = 7$.

PROOF. (i), (ii) and (iii) follow from Proposition 11 and Theorems 16 and 17 of [1].

(iv) Suppose $G = M_{n,p}$. From Lemma 2.9, $Z(G) = \Phi(G) = G^p = \langle a^p \rangle$ and $\Omega_i(G) = \langle a^{p^{n-i-1}}, b \rangle$. The commutator $c = [a, b] = a^{p^{n-2}}$ has order p, $[a^i, b] = c^i$, $G' = \langle c \rangle$ and $(ba^j)^p = c^{jp(p-1)/2} a^{jp}$.

Therefore, for $1 \leq i \leq n-1$, we have $G^{p^i} = \langle a^{p^i} \rangle$ and so ps(G) = n. The maximal subgroups of G are the cyclic subgroups $\langle a \rangle$ and $\langle a^i b \rangle$, $1 \leq i < p$, and the noncyclic subgroup $\langle a^p, b \rangle$. Therefore, the proper noncyclic subgroups of G are the abelian groups $\Omega_i(G)$ of type (p^i, p), $1 \leq i \leq n-2$. Thus, G has $n-1$ noncyclic subgroups each of which, except $\Omega_1(G)$, has p maximal cyclic subgroups. There are $p+1$ cyclic subgroups in $\Omega_1(G)$. Therefore, $s(G) = (n-1) + p(n-2) + (p+1) + 1 = p(n-1) + n + 1$ and $\mathrm{nps}(G) = p(n-1) + 1$.

(v) The exponent of $M(p)$ is p; therefore, it has $(p^3 - 1)/(p-1)$ subgroups of order p. Every subgroup of order p^2 is normal and hence contains the centre (of order p). Therefore, there are $(p^3 - p)/(p^2 - p)$ subgroups of order p^2. In total there are $p^2 + 2p + 2$ proper subgroups all of which are nonpower subgroups.

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

(vi), (vii) We only prove that $\mathrm{nps}(G_{n,p^k}) = p(p^k - 1)/(p-1)$. Then $\mathrm{nps}(F_{n,p}) = p$ is obtained similarly.

Recall that $G_{n,p^k} = \langle a, b \mid a^{2^n} = b^{p^k} = 1,\ a^{-1}ba = b^{-1}\rangle$. Thus, $\langle a^2\rangle \subseteq Z(G_{n,p^k})$. Then we have $G_{n,p^k}/\langle a^2\rangle \simeq D_{2p^k}$. Since the number of Sylow 2-subgroups of D_{2p^k} is p^k, the number of Sylow 2-subgroups of G_{n,p^k} is also p^k. Thus, the Sylow 2-subgroups of G_{n,p^k} are self-normalising. For $0 \le j \le k-1$, $\langle b^{p^{k-j}}\rangle$ is the unique subgroup of order p^j of G_{n,p^k}. Let H_j be a subgroup of G_{n,p^k} and $|H_j| = 2^n p^j$. Then the Sylow 2-subgroups of H_j are self-normalising. Thus, every subgroup of order $2^n p^j$ in G_{n,p^k} contains p^j Sylow 2-subgroups of G_{n,p^k}. Thus, there are exactly p^{k-j} subgroups of order $2^n p^j$ in G_{n,p^k} and they are conjugate to each other in G_{n,p^k}. The number of those subgroups is $p(p^k - 1)/(p-1)$. Now we prove that the other subgroups of G_{n,p^k} are power subgroups. Since $\langle a^2\rangle \subseteq Z(G_{n,p^k})$, for $0 \le i \le n-1$ and $0 \le s \le k$, $\langle a^{2^{n-i}}, b^{p^{k-s}}\rangle$ is the unique subgroup of order $2^i p^s$ in G_{n,p^k} and $\langle a^{2^{n-i}}, b^{p^{k-s}}\rangle = G_{n,p^k}^{2^{n-i}p^{k-s}}$. This completes the proof.

(viii) The power subgroups of A_n are distinct except that $A_n^2 = A_n^1$. The $2n-1$ subgroups Q, $\langle a^{3^i}\rangle$ and $Q\langle a^{3^i}\rangle$, where $1 \le i < n$ and $Q = \langle b, c\rangle$, are the proper nontrivial normal subgroups of A_n. The other subgroups are $\langle a\rangle$, $\langle a^{3^i}b\rangle$, $\langle a^{3^i}c\rangle$, $\langle a^{3^i}bc\rangle$ for $0 \le i \le n$. Thus, A_n has $5(n+1)$ subgroups; therefore, $\mathrm{nps}(A_n) = 3n + 4$.

(ix) There are n proper power subgroups of $B^1_{n,p}$; their orders are p^i for $0 \le i < n$. We claim that $\mathrm{nps}(B^1_{n,p})$ is an increasing function of n and p by counting the subgroups. Since $B^1_{1,p}$ is well known, we only consider the case $n \ge 2$. We count subgroups by considering their exponent. First, notice that $\Omega_{n-1}(B^1_{n,p}) = \langle a\rangle \times \langle b^p\rangle \times \langle c\rangle \simeq C_p \times C_{p^{n-1}} \times C_p$, which implies that all the subgroups of exponent $\le p^{n-1}$ are in $\Omega_{n-1}(B^1_{n,p})$. Thus, the number of subgroups with exponent $\le p^{n-1}$ is $s(C_p \times C_{p^{n-1}} \times C_p)$, which is an increasing function of n and p. Next, we consider the subgroups of exponent p^n. Considering the number of elements of order p^n, we see that there are p^2 cyclic subgroups of order p^n. Let H be a subgroup of order p^{n+1} with $\exp(H) = p^n$. Then $c \in H$ and $\exp(H/\langle c\rangle) = p^n$. Since $B^1_{n,p}/\langle c\rangle \simeq C_p \times C_{p^n}$, we see that the number of such subgroups H is p. Therefore, the number of subgroups of exponent p^n is $p^2 + p + 1$. Thus, $\mathrm{nps}(B^1_{n,p})$ is an increasing function of n and p, as claimed. By direct calculation or from MAGMA [5], we find that $\mathrm{nps}(B^1_{2,2}) = 20$ and $\mathrm{nps}(B^1_{1,3}) = \mathrm{nps}(M(3)) = 17$.

(x) There are n proper power subgroups of $B^2_{n,p}$; their orders are p^i for $0 \le i \le n-2$ and p^n. Similarly, $\mathrm{nps}(B^2_{n,p})$ is an increasing function of n and p. By direct calculation or from MAGMA [5], we find that $\mathrm{nps}(B^2_{2,2}) = 12$, $\mathrm{nps}(B^2_{2,3}) = 20$ and $\mathrm{nps}(B^2_{1,5}) = \mathrm{nps}(M_{3,5}) = 11$. □

REMARK 3.2. It can be shown that:

(i) for $n \ge 2$, $\mathrm{nps}(B^1_{n,p}) = p^2(2n-1) + p(n+1) + 2$; and
(ii) for $n \ge 2$, $\mathrm{nps}(B^2_{n,p}) = (p+1)(2 + p(n-1))$.

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

LEMMA 3.3. *Let* $G = D_{2p} \times \underbrace{C_2 \times \cdots \times C_2}_{n}$. *For* $n \geq 1$ *and a prime* $p > 2$, *we have* $\mathrm{nps}(G) \geq 3p + 4$ *and equality holds when* $n = 1$.

PROOF. For all $n \geq 1$, the exponent of G is $2p$ and the only proper nontrivial power subgroup is G^2 of order p. The group $D_{2p} \times C_2$ has $3p + 7$ subgroups; therefore, G has at least $3p + 4$ nonpower subgroups. □

LEMMA 3.4. *Let* $X_{n,p} = D_{2p} \times \underbrace{C_3 \times \cdots \times C_3}_{n}$. *For* $n \geq 1$ *and a prime* $p > 3$, *we have* $\mathrm{nps}(X_{n,p}) = (p + 3)s(C_3^n) - 6 \geq 10$, *where* $\underbrace{C_3 \times \cdots \times C_3}_{n}$ *is denoted by* C_3^n *for short. For* $n \geq 1$, $\mathrm{nps}(X_{n,3}) \geq \mathrm{nps}(X_{1,3}) = 10$.

PROOF. By simple calculation, $s(D_{2p}) = p + 3$ and $\mathrm{ps}(D_{2p}) = 3$. Let $p > 3$. Then, from Lemma 2.2, $\mathrm{nps}(X_{n,p}) = \mathrm{nps}(D_{2p})s(C_3^n) + ps(D_{2p})\,\mathrm{nps}(C_3^n) = \mathrm{nps}(D_{2p})s(C_3^n) + ps(D_{2p})(s(C_3^n) - 2) = (p + 3)s(C_3^n) - 6$. In particular, $\mathrm{nps}(X_{1,5}) = 10$. For any $n \geq 1$, $\mathrm{ps}(X_{n,3}) = 3$. Thus, $\mathrm{nps}(X_{n,3})$ is an increasing function for n. Then a straightforward calculation shows that $\mathrm{nps}(X_{1,3}) = 10$, and this completes the proof. □

LEMMA 3.5 [8, Theorem 3.3]. *For* $n_2 \geq n_1 \geq 1$ *and a prime* p, *the total number of subgroups of* $C_{p^{n_1}} \times C_{p^{n_2}}$ *is*

$$\frac{(n_2 - n_1 + 1)p^{n_1+2} - (n_2 - n_1 - 1)p^{n_1+1} - (n_2 + n_1 + 3)p + (n_2 + n_1 + 1)}{(p - 1)^2}.$$

LEMMA 3.6. *For* $n_2 \geq n_1 \geq 1$ *and a prime* p, *the value of* $\mathrm{nps}(C_{p^{n_1}} \times C_{p^{n_2}})$ *is*

$$\frac{(n_2 - n_1 + 1)p^{n_1+2} - (n_2 - n_1 - 1)p^{n_1+1} - (n_2 + n_1 + 3)p + (n_2 + n_1 + 1)}{(p - 1)^2} - (n_2 + 1).$$

PROOF. This follows from Lemma 3.5 and Corollary 2.3. □

EXAMPLE 3.7. We have $\mathrm{nps}(C_p \times C_{p^n}) = pn + 1$ and $\mathrm{nps}(C_{p^2} \times C_{p^2}) = (p + 1)(p + 2)$.

4. The groups with at most nine nonpower subgroups

In proving Theorem 1.1, we use Theorem 1.3 of [2] and the theorems of [7] and [9], which we summarise in the following lemma.

LEMMA 4.1. *For a finite group* G:

(1) *G is cyclic if and only if* $\mathrm{nps}(G) = 0$;
(2) *if G is noncyclic, then* $\mathrm{nps}(G) \geq 3$;
(3) *if* $\mathrm{nps}(G) = 3$, *then G is* $C_2 \times C_2$, Q_8 *or* $G_{n,3}$ *for* $n \geq 1$; *and*
(4) *if* $\mathrm{nps}(G) = 4$, *then G is* $C_3 \times C_3$.

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

Let $\mathrm{Syl}_p(G)$ denote the set of Sylow subgroups of G. Recall that $P \in \mathrm{Syl}_p(G)$ has $|G : N_G(P)|$ conjugates and we have $|G : N_G(P)| \equiv 1 \pmod p$. Moreover, $N_G(P)$ is self-normalising; therefore, it also has $|G : N_G(P)|$ conjugates.

LEMMA 4.2. *Let G be a finite group and let P be a Sylow p-subgroup of G such that $P \neq N_G(P) \neq G$. Then $\mathrm{nps}(G) \leq 9$ if and only if, for some $n \geq 1$ and a prime $q > 3$:*

(1) $\mathrm{nps}(G) = 6$, $p = 2$ *and* $G \simeq G_{n,3} \times C_q$; *or*
(2) $\mathrm{nps}(G) = 9$, $p = 2$ *and* $G \simeq G_{n,3} \times C_{q^2}$.

PROOF. Since $P \neq N_G(P) \neq G$, both P and $N_G(P)$ have at least $p + 1$ conjugates and so $2(p + 1) \leq \mathrm{nps}(G) \leq 9$, from which we get p is 2 or 3. If $Q \in \mathrm{Syl}_q(G)$ for some prime $q \neq p$ and $N_G(Q) \neq G$, then $2(p + 1) + q + 1 \leq \mathrm{nps}(G) \leq 9$, which is impossible. Therefore, for $q \neq p$, all Sylow q-subgroups are normal. Thus, $G = NP$, where N is a nilpotent normal subgroup such that $N \cap P = 1$. Then $[N_N(P), P] \subseteq N \cap P = 1$ and, consequently, $N_G(P) = PC_N(P)$. If $|G : N_G(P)| > p + 1$, then $2(2p + 1) \leq 9$, which is a contradiction. Thus, $|G : N_G(P)| = p + 1$.

If $p = 3$, then $\mathrm{nps}(G)$ is 8 or 9. Thus, for $Q \in \mathrm{Syl}_2(G)$, we have $Q \trianglelefteq G$ and $G = N_G(P)Q$. If $[P, Q] \subseteq \Phi(Q)$, it follows from Lemma 2.7 that $[P, Q] = 1$. But then $Q \subseteq C_G(P) \subseteq N_G(P)$, which is a contradiction. Thus, Q has at least three subgroups that are not normal in G. Hence, G has at least 11 nonpower subgroups, contrary to $\mathrm{nps}(G) \leq 9$. Therefore, for the remainder of the proof, we take $p = 2$.

If P is not cyclic, it follows from Lemma 4.1 that $\mathrm{nps}(P) \geq 3$. Then, in addition to the three conjugates of P and the three conjugates of $N_G(P)$, there would be at least three nonpower subgroups H such that H/N is a nonpower subgroup of $G/N \simeq P$. In this case, $\mathrm{nps}(P) = 3$, $\mathrm{nps}(G) = 9$ and P is either $C_2 \times C_2$ or Q_8. But $\mathrm{nps}(G) = 9$ implies that the proper subgroups of P are normal in G, which is a contradiction since P is generated by its proper subgroups. Therefore, P is cyclic.

Let $R \in \mathrm{Syl}_r(N)$. Then R acts by conjugation on the three conjugates of P. If $r > 3$, then $R \subseteq N_G(P)$, from which we get $R \subseteq N_G(P) \cap N \subseteq C_G(P)$. For $Q \in \mathrm{Syl}_3(G)$, we have $[R, Q] \subseteq R \cap Q = 1$ and so $R \subseteq C_G(Q)$. Consequently, $G = PQ \times A$, where A is a nilpotent group whose order is not divisible by two or three. From Lemma 2.2,

$$\mathrm{nps}(G) = \mathrm{nps}(QP)s(A) + \mathrm{ps}(QP)\,\mathrm{nps}(A).$$

It follows from $\mathrm{nps}(G) \leq 9$ that $\mathrm{nps}(A) = 0$ and so A is cyclic. Furthermore, $s(A) \leq 3$; therefore, A is either trivial or a cyclic group of order r or r^2 for some prime $r > 3$.

The permutation action of G on the conjugates of P defines a homomorphism $G \to \mathrm{Sym}(3)$ with kernel $K = \bigcap_{g \in G} N_G(P)^g$. Since $|Q : C_Q(P)| = 3$, we have $\Phi(Q) \subseteq C_Q(P) \subseteq K$. Therefore, $M = (P \cap K) \times \Phi(Q) \times A$ is a normal subgroup of G. The group P acts on the elementary abelian group $\overline{Q} = Q/\Phi(Q)$ and it follows from Lemma 2.6 that $\overline{Q} = C_{\overline{Q}}(P) \times [P, \overline{Q}]$. Thus, $[P, \overline{Q}] \simeq C_3$ and

$$G/M \simeq \mathrm{Sym}(3) \times \underbrace{C_3 \times \cdots \times C_3}_{n}.$$

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

If $n \geq 1$, it follows from Lemmas 3.4 and 2.4 that $\mathrm{nps}(G) \geq 10$, contrary to assumption. Thus, $Q/\Phi(Q) \simeq C_3$; therefore, Q is cyclic. But now $Q = [P, Q] \times C_Q(P)$; therefore, $C_Q(P) = 1$ and $|Q| = 3$.

Let a be a generator of P and let b a generator of Q. Then $a^{-1}ba = b^{-1}$ and so $QP \simeq G_{n,3}$ for some n. The assumption $N_G(P) \neq P$ implies that $A \neq 1$. Thus, G is either $G_{n,3} \times C_r$ or $G_{n,3} \times C_{r^2}$ for some prime $r > 3$. □

REMARK 4.3. The group $G = \mathrm{Sym}(3) \times C_3$ satisfies the hypothesis of the lemma (with $p = 2$) except that $\mathrm{nps}(G) = 10$.

LEMMA 4.4. *Let G be a finite group and let P be a Sylow p-subgroup of G such that $P = N_G(P) \neq G$. Then $\mathrm{nps}(G) \leq 9$ if and only if, for some $n \geq 1$, one of the following holds.*

(1) $\mathrm{nps}(G) = 3$, *$p = 2$ and $G \simeq G_{n,3}$.*
(2) $\mathrm{nps}(G) = 5$, *$p = 2$ and $G \simeq G_{n,5}$.*
(3) $\mathrm{nps}(G) = 7$, *$p = 2$ and $G \simeq G_{n,7}$.*
(4) $\mathrm{nps}(G) = 7$, *$p = 3$ and $G \simeq F_{n,7}$.*
(5) $\mathrm{nps}(G) = 7$, *$p = 3$ and $G \simeq \mathrm{Alt}(4)$.*

PROOF. The Sylow subgroup P has $m = |G : N_G(P)|$ conjugates. Since $m \equiv 1 \pmod p$ and $N_G(P) \neq G$, we have $m \geq p + 1$ and the conjugates of P are nonpower subgroups. The assumption $\mathrm{nps}(G) \leq 9$ implies that $p \in \{2, 3, 5, 7\}$.

If $p = 2$, then $m \in \{3, 5, 7, 9\}$; if $p = 3$, then $m \in \{4, 7\}$; if $p = 7$, then $m = 8$. However, if $p = 5$, then $m = 6$ and G is a group of twice odd order. It is an elementary fact that a group of twice odd order has a subgroup H of index two, which, in this case, contains P. Then $|H : P| = 3$, which is impossible. Thus, in all cases m is a power of a prime q and, for $Q \in \mathrm{Syl}_q(G)$, we have $G = PQ$ and $|Q| = m$.

The permutation action on $\mathrm{Syl}_p(G)$ defines a homomorphism $G \to \mathrm{Sym}(m)$ whose kernel $K = \bigcap_{g \in G} P^g$ is a proper subgroup of P.

If $N_G(Q) \neq G$, then Q has at least $q + 1$ conjugates; therefore, $m + q + 1 \leq 9$. In this case, either $p = 2$ and $|Q| = 3$ or $p = 3$ and $|Q| = 4$. Furthermore, we must have $Q = N_G(Q)$. Otherwise, both Q and $N_G(Q)$ would have at least $q + 1$ conjugates. From the structure of $\mathrm{Sym}(3)$ and $\mathrm{Sym}(4)$, we have $KQ \trianglelefteq G$ and, by the Frattini argument [6, Theorem 1.3.7], $G = KN_G(Q)$ and $Q \neq N_G(Q)$, which is a contradiction. Therefore, $Q \trianglelefteq G$ and $[K, Q] \subseteq K \cap Q = 1$ and hence $K \subseteq C_G(Q)$.

The order of Q is either q or q^2; therefore, Q is abelian.

Case 1: $p = 2$ and $m \in \{3, 5, 7, 9\}$. We have $G = Q \rtimes P$, where P is a 2-group and Q is an abelian group of order m. We treat each value of m separately.

Case 1a: $p = 2$ and $|Q| = 3$. In this case, $|Q| = 3$ and $G/K \simeq \mathrm{Sym}(3)$. Since $|P/K| = 2$, we have $\Phi(P) \subseteq K$ and so $\Phi(P) \trianglelefteq G$. If P is not cyclic, then $G/\Phi(P) \simeq \mathrm{Sym}(3) \times C_2 \times \cdots \times C_2$ and it follows from Lemmas 2.4 and 3.3 that $\mathrm{nps}(G) \geq 13$, contrary to assumption. Thus, P is cyclic. If a generates P and b generates Q, then $b^a = b^{-1}$ and $G \simeq G_{n,3}$.

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

Case 1b: $p = 2$ and $|Q| = 5$. In this case, $|Q| = 5$ and QK/K is a normal subgroup of G/K. Therefore, $|G/K|$ is either 10 or 20. If $|G/K| = 20$, then $G/K = \langle x, b \mid x^4 = b^5 = 1, x^{-1}bx = b^2 \rangle$. This group has 14 subgroups, 4 of which are power subgroups; therefore, there are 10 nonpower subgroups. From Lemma 2.4, $\mathrm{nps}(G) \geq 10$, contrary to our assumption. Thus, $|G/K| = 10$. If P is not cyclic, then $G/\Phi(P) \simeq D_{10} \times C_2 \times \cdots \times C_2$ and, using Lemma 3.3, we arrive at a contradiction, as in Case 1a. Thus, P is cyclic. If a generates P and b generates Q, then $b^a = b^{-1}$ and so $G \simeq G_{n,5}$.

Case 1c: $p = 2$ and $|Q| = 7$. In this case, $|Q| = 7$, $G/K \simeq D_{14}$ and P has seven conjugates. If P is not cyclic, then $\mathrm{nps}(P) \geq 3$ and it follows from Lemma 2.4 that $\mathrm{nps}(G) \geq 10$, contrary to assumption. Thus, P is cyclic and $G \simeq G_{n,7}$.

Case 1d: $p = 2$ and $|Q| = 9$. Since $\mathrm{nps}(G) \leq 9$, all subgroups are normal except the Sylow 2-subgroups. In particular, if R is a subgroup of Q of order three, then $R \trianglelefteq G$; therefore, $RP \trianglelefteq G$. But then P is not maximal. Thus, all maximal subgroups are normal. This implies that G is nilpotent and this contradiction shows that there are no examples in this case.

Case 2: $p = 3$. In this case, $G = Q \rtimes P$, where P is a 3-group and $|Q| \in \{4, 7\}$.

Case 2a: $p = 3$ and $|Q| = 4$. We must have $Q \simeq C_2 \times C_2$, otherwise $Q \simeq C_4$ and then $Q \subseteq C_G(P)$, which contradicts the assumption that $P = N_G(P)$.

It follows that Q has three subgroups R_1, R_2 and R_3 of order two and P acts transitively on them. Then R_1, R_2, R_3 and the four conjugates of P are not normal in G, from which we get $\mathrm{nps}(G) \geq 7$. Let K be the kernel of the action of P on $\{R_1, R_2, R_3\}$. Then $K = C_P(Q)$, $|P : K| = 3$ and so $K \trianglelefteq G$. Then R_1K, R_2K and R_3K are permuted by P and, if $K \neq 1$, we would have $\mathrm{nps}(G) \geq 10$. Therefore, $K = 1$, $|P| = 3$ and so $G \simeq \mathrm{Alt}(4)$.

Case 2b: $p = 3$ and $|Q| = 7$. For $Q \in \mathrm{Syl}_7(G)$, we have $|Q| = 7$ and P is cyclic; otherwise, $\mathrm{nps}(P) \geq 3$ and we obtain a contradiction by applying Lemma 2.4 to G/Q. The image of the homomorphism $G \to \mathrm{Sym}(7)$ is the group $F_{1,7}$ of order 21. We may write $P = \langle a \rangle$ and $Q = \langle b \rangle$, where $a^{3^n} = 1$, $b^7 = 1$ and $b^a = b^2$. Thus, $G \simeq F_{n,7}$.

Case 3: $p = 7$ and $|Q| = 8$. All subgroups are normal except the Sylow 7-subgroups. As in Case 1d, we see that all maximal subgroups of G are normal and so G is nilpotent, which is a contradiction. □

REMARK 4.5. For $n \geq 2$, the groups $\langle x, b \mid x^{2^n} = b^5 = 1, x^{-1}bx = b^2 \rangle$ have exactly 10 nonpower subgroups and their Sylow 2-subgroups are self-normalising.

PROOF OF THEOREM 1.1. From Lemmas 4.2 and 4.4, we may suppose that G is nilpotent. If P is a noncyclic p-group, then $\mathrm{nps}(P) \geq 3$. Suppose that $H \neq 1$ is a group whose order is not divisible by p. If $\mathrm{nps}(P \times H) \leq 9$, then, from Lemma 2.2, there are two possibilities: (i) $\mathrm{nps}(P) = 3$ and H is a cyclic group whose order is a prime or the square of a prime; (ii) $\mathrm{nps}(P) = 4$ and H is a cyclic group of prime order.

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

From Lemma 4.1, if $\mathrm{nps}(P) = 3$, then G is $C_2 \times C_2 \times C_r$, $C_2 \times C_2 \times C_{r^2}$, $Q_8 \times C_r$ or $Q_8 \times C_{r^2}$, where $r > 2$ is a prime. If $\mathrm{nps}(P) = 4$, then G is $C_3 \times C_3 \times C_r$, where $r \neq 3$ is a prime.

Thus, from now on, we may suppose that G is a noncyclic p-group. Then $G/\Phi(G)$ is an elementary abelian group of order p^d. The proper subgroups of $G/\Phi(G)$ are nonpower subgroups; therefore, $\mathrm{nps}(G) \leq 9$ implies that $d = 2$ and $p \in \{2, 3, 5, 7\}$.

The group G can be generated by two elements; therefore, $G/G' = C_{p^m} \times C_{p^n}$ for some $m \leq n$. It follows from Example 3.7 and Lemma 2.4 that $m = 1$. Thus, G/G' is one of $C_p \times C_p$ for $p \in \{2, 3, 5, 7\}$, $C_2 \times C_{2^n}$ for $n \in \{2, 3, 4\}$ or $C_3 \times C_9$. If G is abelian, this completes the proof. From now on, we assume that $G' \neq 1$.

Suppose that $G/G' \simeq C_2 \times C_2$. It follows from Lemma 2.10 that G is isomorphic to D_{2^n}, S_{2^n} or Q_{2^n}. From Proposition 3.1, the only possibilities are D_8, Q_8 and Q_{16}.

Since $G' \neq 1$, there exists $R \trianglelefteq G$ such that $|G'/R| = p$. We shall determine the structure of G/R for each choice of G/G'.

Suppose that p is odd and $G/G' \simeq C_p \times C_p$. From Lemma 2.11, G/R is an extraspecial group of order p^3: that is, $M_{3,p}$ or $M(p)$. From Proposition 3.1(iv) and (v), $\mathrm{nps}(M_{3,p}) = 2p + 1$ and $\mathrm{nps}(M(p)) = p^2 + 2p + 2$. Thus, $p = 3$ and $G/R \simeq M_{3,3}$. The group $M_{3,3}$ has a cyclic subgroup of order nine; therefore, it is metacyclic. It follows from Lemma 2.13 that G is metacyclic and so G has a cyclic normal subgroup that properly contains G': that is, G has a cyclic subgroup of index three. Therefore, by Lemma 2.8, $G \simeq M_{n,3}$. (This argument is based on the MathSciNet review of [3] by Marty Isaacs.) But, from Lemma 2.9, if $M = M_{n,p}$, then M' is its unique normal subgroup of order p and $M/M' \simeq C_p \times C_{p^{n-2}}$. Thus, $R = 1$ and $G \simeq M_{3,3}$.

Suppose that $G/G' \simeq C_2 \times C_{2^n}$ $(n = 2, 3, 4)$ or $C_3 \times C_9$. If G/R has a cyclic subgroup of prime index, it follows from Lemma 2.8 that G/R is isomorphic to $M_{n+2,2}$ or $M_{4,3}$. The assumption that $\mathrm{nps}(G) \leq 9$ excludes $M_{6,2}$ and $M_{4,3}$. Then, from Theorem 2.12, $R = 1$ and hence G is isomorphic to $M_{4,2}$ or $M_{5,2}$.

We may suppose that the exponent of G/R is 2^n or 9. Lemma 2.13 shows that G/R is either $B^1_{n,p}$ or $B^2_{n,p}$ for $p \in \{2, 3\}$ and $n \geq 2$. Proposition 3.1(ix) and (x) shows that none of these groups satisfy our assumptions. This completes the proof. □

References

[1] C. S. Anabanti, A. B. Aroh, S. B. Hart and A. R. Oodo, 'A question of Zhou, Shi and Duan on nonpower subgroups of finite groups', *Quaest. Math.* **45**(6) (2022), 901–910.

[2] C. S. Anabanti and S. B. Hart, 'Groups with a given number of nonpower subgroups', *Bull. Aust. Math. Soc.* **106**(2) (2022), 315–319.

[3] Y. Berkovich, 'Short proofs of some basic characterization theorems of finite p-group theory', *Glas. Mat. Ser. III* **41**(61) (2) (2006), 239–258.

[4] N. Blackburn, 'On prime-power groups with two generators', *Proc. Cambridge Philos. Soc.* **54** (1958), 327–337.

[5] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* **24** (1997), 235–265.

[6] D. Gorenstein, *Finite Groups*, Harper's Series in Mathematics (Harper and Row, New York–Evanston–London, 1968).

https://doi.org/10.1017/S0004972723000783 Published online by Cambridge University Press

[7] F. Szász, 'On cyclic groups', *Fund. Math.* **43** (1956), 238–240.
[8] M. Tărnăuceanu, 'An arithmetic method of counting the subgroups of a finite abelian group', *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **53**(101) (4) (2010), 373–386.
[9] W. Zhou, W. Shi and Z. Duan, 'A new criterion for finite noncyclic groups', *Comm. Algebra* **34**(12) (2006), 4453–4457.

JIWEI ZHENG, School of Mathematics and Statistics,
Southwest University, Chonqing 400715, P.R. China
e-mail: 1179157500@qq.com

WEI ZHOU, School of Mathematics and Statistics,
Southwest University, Chonqing 400715, P.R. China
e-mail: zh_great@swu.edu.cn

D. E. TAYLOR, School of Mathematics and Statistics,
The University of Sydney, New South Wales 2006, Australia
e-mail: Donald.Taylor@sydney.edu.au