A QUESTION OF ZHOU, SHI AND DUAN ON NONPOWER SUBGROUPS OF FINITE GROUPS

C.S. Anabanti
Institut für Analysis & Zahlentheorie, Technische Universität Graz, Austria, and Department of Mathematics and Applied Mathematics, University of Pretoria, South Africa.
E-Mail anabanti@math.tugraz.at, chimere.anabanti@up.ac.za, chimere.anabanti@unn.edu.ng

A.B. Aroh
Department of Mathematics, University of Nigeria, Nsukka, Nigeria.
E-Mail blaise.aroh.231881@unn.edu.ng

S.B. Hart
Department of Economics, Mathematics and Statistics, Birkbeck, University of London, UK.
E-Mail s.hart@bbk.ac.uk

A.R. Oodo
Department of Mathematics, University of Nigeria, Nsukka, Nigeria.
E-Mail amara.oodo.231880@unn.edu.ng

Abstract. A subgroup $H$ of a group $G$ is called a power subgroup of $G$ if there exists a non-negative integer $m$ such that $H = \langle g^m : g \in G \rangle$. Any subgroup of $G$ which is not a power subgroup is called a nonpower subgroup of $G$. Zhou, Shi and Duan, in a 2006 paper, asked whether for every integer $k (k \geq 3)$, there exist groups possessing exactly $k$ nonpower subgroups. We answer this question in the affirmative by giving an explicit construction that leads to at least one group with exactly $k$ nonpower subgroups, for all $k \geq 3$, and infinitely many such groups when $k$ is composite and greater than 4. Moreover, we describe the number of nonpower subgroups for the cases of elementary abelian groups, dihedral groups, and 2-groups of maximal class.

Mathematics Subject Classification (2020): 20D25, 20D60, 20E34.
Key words: Counting subgroups, nonpower subgroups, finite groups.

1. Introduction. A subgroup $H$ of a group $G$ is called a power subgroup of $G$ if there exists a non-negative integer $m$ such that $H = \langle g^m : g \in G \rangle$. The identity subgroup and the whole group are examples of power subgroups of any group $G$. If $H$ is a power subgroup of $G$, then $H$ is normal in $G$; but the converse is not necessarily true. For instance, no subgroup of index 2 in the quaternion group $Q_8$ of order 8 is a power subgroup of $Q_8$, even though they are...
normal subgroups. A subgroup of $G$ which is not a power subgroup is called a \textit{nonpower subgroup} of $G$.

Let $k$ be the number of nonpower subgroups of a group $G$. The authors (Zhou, Shi and Duan) of [4] proved the following:

(a) $k \in (0, \infty)$ if and only if $G$ is a finite noncyclic group;
(b) $k = 0$ if and only if $G$ is a cyclic group;
(c) $k = \infty$ if and only if $G$ is an infinite noncyclic group.

They also remarked that neither $k = 1$ nor $k = 2$ is possible in any group. With respect to the case $k \geq 3$, they asked (see [4, Problem]):

\textbf{Question 1.} (Zhou, Shi and Duan) \textit{For any integer $k$ $(k \geq 3)$, do there exist groups possessing exactly $k$ nonpower subgroups?}

In this paper, we show that the answer to this question is yes. In fact, we prove that there is at least one group possessing exactly $k$ nonpower subgroups for each $k \geq 3$ (see Theorem 5). Our method of proof also shows that there are infinitely many such groups for each $k > 4$ and $k$ not prime. The constructions we used are given in Section 2; part of it involves the direct product of a dihedral group with a carefully chosen cyclic group.

There are further questions one could ask. For example, given a positive integer $n$, what is the maximum number of nonpower subgroups in a group of order $n$? To supply further examples of the possible numbers of nonpower subgroups in a group of a given order, we also explore in Section 3 some special cases: elementary abelian $p$-groups, dihedral groups, and 2-groups of maximal class. For example, we observe (see Corollary 10) that the elementary abelian $p$-group $C_p \times C_p$ ($p$ prime) contains exactly $p + 1$ nonpower subgroups, and the generalised quaternion group $Q_{2^n}$ (where $n \geq 3$) contains exactly $2^{n-1} - 1$ nonpower subgroups (see Theorem 16). All the groups studied here are finite.

We end this introductory section by briefly establishing the notation we will use. For a positive integer $n$, we write $C_n$ for the cyclic group of order $n$, with $D_{2n}$ being the dihedral group of order $2n$.

\textbf{Notation.} Let $G$ be a group. We write $s(G)$ for the total number of subgroups in $G$. Also, we write $ps(G)$ for the number of power subgroups, and $nps(G)$ for the number of non-power subgroups. For example, in $C_2 \times C_2$ we have $s(G) = 5$, $ps(G) = 2$ and $nps(G) = 3$.

\section{Groups with exactly \(k\) nonpower subgroups.} In this section, we give constructions that supply, for each $k \geq 3$, at least one finite group containing exactly $k$ nonpower subgroups. Moreover, for $k \neq 4$ and $k$ not prime, our constructions give infinitely many finite groups containing exactly $k$ nonpower subgroups.

\textbf{Remark 2.} Let $G$ be a finite group. If $n$ is coprime to $|G|$, then $G^n = G$ as the map $g \mapsto g^n$, while not a homomorphism, is certainly a bijection from $G$ to itself in this case. More generally, $G^{mn} = G^m$ for any positive integer $m$. 
**Lemma 3.** Let $A$ and $B$ be finite groups such that $|A|$ and $|B|$ are coprime. Then every subgroup of $A \times B$ is of the form $U \times V$, where $U \leq A$ and $V \leq B$. Moreover, a subgroup of $A \times B$ is a power subgroup if and only if it is of the form $U \times V$, where $U$ is a power subgroup of $A$ and $V$ is a power subgroup of $B$. In particular,

\begin{align*}
(1) \quad s(A \times B) &= s(A) \times s(B); \\
(2) \quad nps(A \times B) &= s(A) \times s(B) - ps(A) \times ps(B).
\end{align*}

**Proof.** Let $G = A \times B$. The fact that the subgroups of $G$ in this case are the direct products of subgroups of $A$ and $B$ is well-known, but we include the proof for completeness. Suppose $H \leq G$ and let $(a, b) \in H$. Since $|A|$ and $|B|$ are coprime, the orders $r$ and $s$ of $a$ and $b$ respectively are also coprime. Therefore, there exist integers $q$ and $t$ such that $rq + st = 1$. Now $(a, b)^{st} = (a, 1)$ and $(a, b)^{rq} = (1, b)$. Hence, $(a, 1)$ and $(1, b)$ are elements of $H$. It follows that $H = U \times V$, where $U = \{a \in A : (a, 1) \in H\}$ and $V = \{b \in B : (1, b) \in H\}$. Therefore, $s(G) = s(A) \times s(B)$.

Consider the power subgroup $G^m$ of $G$, for a positive integer $m$. We have that $G^m = A^m \times B^m$, because this group is generated by elements $(x, y)^m = (x^m, y^m)$, and we have observed that $(x^m, y^m)$ is contained in a subgroup $H$ if and only if $(x^m, 1) \in H$ and $(1, y^m) \in H$. For the converse, suppose that $U = A^\ell$ and $V = B^m$, for some positive integers $m$ and $\ell$. We may assume that $\ell$ divides $|A|$ and $m$ divides $|B|$, by Remark 2. Now, let $n = \ell m$. Since $\ell$ and $m$ are therefore coprime, we have that $A^n = A^\ell$, and $B^m = B^m$. Therefore, $U \times V = G^n$. Thus, a subgroup of $G$ is a power subgroup if and only if it is of the form $U \times V$, where $U$ is a power subgroup of $A$ and $V$ is a power subgroup of $B$. In particular, $nps(G) = ps(A) \times ps(B)$. Hence, $nps(G) = s(G) - ps(G) = s(A) \times s(B) - ps(A) \times ps(B)$. \hfill \Box

Let $n$ be a positive integer. Zhou et al. showed that $nps(C_n) = 0$. We also note that $s(C_n) = ps(C_n) = \tau(n)$, where $\tau(n)$ is the number of divisors of $n$.

**Corollary 4.** Suppose $G = A \times C_n$, where $n$ is a positive integer and $A$ is a finite group whose order is coprime to $n$. Then $nps(G) = \tau(n) \times nps(A)$.

**Proof.** We have that $s(C_n) = ps(C_n) = \tau(n)$. Therefore in Equation (2), we have $nps(G) = (s(A) - ps(A)) \tau(n) = \tau(n) \times nps(A)$. \hfill \Box

Before the next result we note that if $p$ is an odd prime, then $nps(D_{2p}) = p$. This is because $D_{2p}$ has exactly $p + 3$ subgroups; the $p$ cyclic subgroups of order 2 are the nonpower subgroups. The remaining groups (the trivial subgroup, the cyclic subgroup of index 2, and the whole group) are the power subgroups $D^2_{2p}$, $D^3_{2p}$ and $D^1_{2p}$, respectively. For a full description of nonpower subgroups in arbitrary dihedral groups, see Section 3.

**Theorem 5.** Let $k$ be a positive integer, with $k \geq 3$. Then there exists a finite group $G$ with exactly $k$ nonpower subgroups. If $k$ is composite and $k > 4$, then there are infinitely many such groups.
Proof. Let \( k \) be a positive integer with \( k \geq 3 \). Then either \( k \) is divisible by 4, or \( k \) is divisible by an odd prime \( p \) (or both). Suppose first that \( k \) is divisible by an odd prime \( p \). Let \( q \) be any odd prime other than \( p \), and let \( r = \frac{k}{p} - 1 \). Then \( \tau(q^r) = \frac{k}{p} \). We observe that \( nps(D_{2p}) = p \). Therefore, by Corollary 4, we get \( nps(D_{2p} \times C_{q^r}) = k \). On the other hand, if \( k \) is divisible by 4, then let \( r = \frac{k}{4} - 1 \), and let \( q \) be any prime greater than 3. A quick calculation shows that \( nps(C_3 \times C_3) = 4 \); whence \( nps((C_3 \times C_3) \times C_{q^r}) = k \). We note that, in each case, if \( k > 4 \) and \( k \) is composite, then the exponent \( r \) is strictly positive. Therefore, since there are infinitely many choices for \( q \), there are infinitely many finite groups \( G \) with exactly \( k \) nonpower subgroups. \( \square \)

3. Special cases.

**Notation.** For a prime \( p \) and a positive integer \( n \), we write \( C_p^n \) for the elementary abelian \( p \)-group of finite rank \( n \), and denote the number of subgroups of rank \( r \) in \( C_p^n \) by \( N_p(n, r) \).

***Theorem 6.*** ([3, Theorem 1]) Let \( V \) be a vector space of dimension \( n \) over the finite field \( GF(q) \), where \( q \) is a prime power. The number of subspaces of \( V \) of dimension \( r \) is

\[
\left( \frac{q^n - 1}{q - 1} \right) \left( \frac{q^{n-1} - 1}{q^2 - 1} \right) \cdots \left( \frac{q^{n-r+1} - 1}{q^r - 1} \right).
\]

**Remark.** (a) The group \( G = C_p^n \) can be realised as an \( n \)-dimensional vector space (say \( V \)) over \( GF(p) \). Now, the number of subgroups of rank \( r \) in \( C_p^n \) is equal to the number of subspaces of dimension \( r \) in \( V \). In the light of Theorem 6 therefore, given any prime \( p \) and positive integers \( n \) and \( r \), with \( n > r \geq 2 \), we have that

\[
(3) \quad N_p(n, r) = \left( \frac{p^n - 1}{p - 1} \right) \left( \frac{p^{n-1} - 1}{p^2 - 1} \right) \cdots \left( \frac{p^{n-r+1} - 1}{p^r - 1} \right) = \prod_{k=0}^{r-1} \left( \frac{p^{n-k} - 1}{p^{k+1} - 1} \right).
\]

(b) \( N_p(n, 0) = 1 = N_p(n, n) \) for any prime \( p \) and natural number \( n \), and for \( n > 1 \),

\[
N_p(n, 1) = \frac{p^n - 1}{p - 1} = \sum_{k=0}^{n-1} p^k = N_p(n, n - 1).
\]

**Proposition 7.** For prime \( p \) and positive integers \( n \) and \( r \) (with \( n > r \geq 2 \)), we have:

(a) \( N_p(n - 1, r) = \left( \frac{p^{n-r} - 1}{p^r - 1} \right) N_p(n - 1, r - 1) \);

(b) \( N_p(n, r) = p^r N_p(n - 1, r) + N_p(n - 1, r - 1) \).

**Proof.** Setting \( n = n - 1 \) and \( r = r - 1 \) in Equation (3), we have that

\[
(4) \quad N_p(n - 1, r - 1) = \left( \frac{p^{n-1} - 1}{p - 1} \right) \cdots \left( \frac{p^{n-r+1} - 1}{p^r - 1} \right) = \prod_{k=0}^{r-2} \left( \frac{p^{n-(k+1)} - 1}{p^{k+1} - 1} \right).
\]
Setting \( n = n - 1 \) in Equation (3), we have that

\[
N_p(n - 1, r) = \left(\frac{p^{n-1} - 1}{p - 1}\right) \cdots \left(\frac{p^{n-r+1} - 1}{p^{r-1} - 1}\right) \left(\frac{p^{n-r} - 1}{p^r - 1}\right) = \prod_{k=0}^{r-1} \left(\frac{p^{n-(k+1)} - 1}{p^{k+1} - 1}\right)
\]

\[(5) \quad = N_p(n - 1, r - 1) \left(\frac{p^{n-r} - 1}{p^r - 1}\right) \text{ (from Equation (4))},
\]

which settles the (a) part. For the (b) part, we multiply Equation (5) by \( p^r \), add the result to Equation (4) and regroup the terms to get the desired result. \( \square \)

The recurrence relations given in Proposition 7 would be a good source for OEIS https://oeis.org/. We now turn to the first main result of this study; see Theorem 8.

**Theorem 8.** For prime, \( p \) and a natural number \( n > 1 \),

\[
nps(C_p^n) = s(C_p^n) - 2 = \sum_{r=1}^{n-1} N_p(n, r).
\]

**Proof.** Let \( p \) be a prime and \( n > 1 \) be an integer. We write \( G = C_p^n \). For \( m \in \mathbb{N} \cup \{0\} \),

\[
G^m = \begin{cases} 
\{1\}, & \text{if } m \equiv 0 \mod p \\
G, & \text{if } m \not\equiv 0 \mod p.
\end{cases}
\]

This tells us that the only power subgroups of \( G \) are the unique subgroups of ranks 0 and \( n \) (viz; the two trivial subgroups). That is, \( nps(G) = s(G) - 2 \). In particular, the nonpower subgroups of \( G \) are the subgroups of ranks 1, 2, \ldots, \( n - 1 \). Thus, the number of nonpower subgroups of \( G \) is \( \sum_{r=1}^{n-1} N_p(n, r) \). \( \square \)

The following result is an immediate consequence of Theorem 8.

**Corollary 9.** Let \( n > 1 \) and \( p \) be prime. Then the elementary abelian \( p \)-group \( C_p^n \) contains exactly \( \sum_{r=1}^{n-1} N_p(n, r) \) nonpower subgroups.

In particular, when \( n = 2 \), we have the following.

**Corollary 10.** Let \( p \) be prime. The elementary abelian \( p \)-group \( C_p^2 \) contains exactly \( p + 1 \) nonpower subgroups.

**Definition.** A 2-group of maximal class is a group of order \( 2^n \) and nilpotency class \( n - 1 \) for \( n \geq 3 \).

**Remark.** It is known (for instance, see Theorem 1.2 and Corollary 1.7 of [1]) that any 2-group of maximal class belongs to one of the following three classes:

(i) \( \langle x, y | x^{2^{n-1}} = y^2 = 1, xy = yx^{-1} \rangle, n \geq 3 \) (Dihedral);
(ii) \( \langle x, y \mid x^{2n-1} = 1, x^{2n-2} = y^2, xy = yx^{-1} \rangle, n \geq 3 \) (Generalised quaternion);

(iii) \( \langle x, y \mid x^{2n-1} = y^2 = 1, xy = yx^{2n-2} \rangle, n \geq 4 \) (Semidihedral).

**Definition.** For \( n \geq 3 \), we write

\[
D_{2n} := \langle x, y \mid x^n = 1 = y^2, xy = yx^{-1} \rangle
\]

for the dihedral group of order \( 2n \).

**Remark.** \( D_{2n} = \{1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\} \). In \( D_{2n} \), each element of \( \{y, xy, \ldots, x^{n-1}y\} \) is an involution. In particular, there are \( n + 1 \) involutions in \( D_{2n} \) when \( n \) is even.

**Theorem 11.** ([2]) For \( n > 2 \), \( s(D_{2n}) = \tau + u \), where \( \tau \) is the number of positive divisors of \( n \) and \( u \) is the sum of the positive divisors of \( n \).

**Proposition 12.** Let \( G = D_{2n}, n > 2 \). Writing \( u \) for the sum of positive divisors of \( n \) and \( r \) for the number of even proper divisors of \( n \), we have the following: (i) if \( n \) is odd, then \( nps(G) = u - 1 \); (ii) if \( n \) is even, then \( nps(G) = s(G) - (r + 2) \); (iii) if \( n \) is a power of 2, then \( nps(G) = u \); (iv) if \( n = 2p \) for an odd prime \( p \), then \( nps(G) = s(G) - 3 = 3p + 4 \).

**Proof.** Let \( \tau \) denote the number of positive divisors of \( n \) and \( u \) denote the sum of positive divisors of \( n \). By Theorem 11, \( s(G) = \tau + u \).

Let \( m \in \mathbb{N} \cup \{0\} \) be arbitrary. Then

\[
G^{2m+1} = \langle 1, x^{2m+1}, \ldots, x^{-(2m+1)}, y, xy, \ldots, x^{n-1}y \rangle.
\]

As \( \{1, y, xy, \ldots, x^{n-1}y\} \subseteq G^{2m+1} \), we see immediately that \( |G^{2m+1}| > \frac{1}{2}|G| \). The fact that \( G^{2m+1} \) is a subgroup of \( G \) helps us to conclude that \( G^{2m+1} = G \).

On the other hand,

\[
G^{2m} = \langle 1, x^{2m}, x^{4m}, \ldots, x^{-4m}, x^{-2m} \rangle = \langle x^{2m} \rangle.
\]

(i) Let \( n \) be odd. Then \( \langle x^{2m} \rangle \) is of the form \( \langle x^v \rangle \), where \( v \) is a positive divisor of \( n \). Therefore the set of all power subgroups of \( G \) is given as

\[
\{G\} \cup \{\langle x^v \rangle \mid v \text{ is a positive divisor of } n\}.
\]

Thus \( ps(G) = \tau + 1 \), and we conclude that \( nps(G) = (\tau + u) - (\tau + 1) = u - 1 \).

(ii) Let \( n \) be even. Then \( \langle x^{2m} \rangle \) is of the form \( \langle x^\mu \rangle \), where \( \mu \) is an even proper divisor of \( n \). Therefore the set of all power subgroups of \( G \) is given as

\[
\{\{1\}, G\} \cup \{\langle x^\mu \rangle \mid \mu \text{ is an even proper divisor of } n\}.
\]

So \( ps(G) = r + 2 \), where \( r \) is the number of even proper divisors of \( n \). Whence, \( nps(G) = s(G) - (r + 2) \).
(iii) Let \( n = 2^\ell \geq 4 \). In the light of (6), the set of power subgroups of \( G \) is
\[
\{\{1\}, G, \langle x^2 \rangle, \langle x^4 \rangle, \langle x^8 \rangle, \ldots, \langle x^{n/2} \rangle \},
\]
where \( \langle x^2 \rangle \cong C_{n/2} \), \( \langle x^4 \rangle \cong C_{n/4} \), \( \langle x^8 \rangle \cong C_{n/8} \), \ldots, \( \langle x^{n/2} \rangle \cong C_2 \). So \( ps(G) = \tau \). Therefore, \( nps(G) = s(G) - ps(G) = (\tau + u) - \tau = u \).

(iv) Let \( n = 2p \) for an odd prime \( p \). In the light of (6), the set of power subgroups of \( G \) is
\[
\{\{1\}, G \} \cup \{\langle x^\mu \rangle \mid \mu \text{ is an even proper divisor of } 2p\} = \{\{1\}, G, \langle x^2 \rangle \},
\]
where \( \langle x^2 \rangle \cong C_p \). Hence, \( ps(G) = 3 \), and we conclude that \( nps(G) = s(G) - 3 = \tau + u - 3 = 4 + (1 + 2 + p + 2p) - 3 = 3p + 4 \). \qed

**Corollary 13.** Given an integer \( n \geq 3 \), \( s(D_{2^n}) = 2^n + n - 1 \) and \( nps(D_{2^n}) = 2^n - 1 \).

**Proof.** The results follow from a direct application of Theorem 11 and Proposition 12(iii) since the number of positive divisors of \( 2^{n-1} \), which is the same as the number of subgroups of \( D_{2^n} \) in \( \langle x \rangle \), is \( n \), and the sum of positive divisors of \( 2^{n-1} \), which is the same as the number of subgroups of \( D_{2^n} \) not contained in \( \langle x \rangle \), is \( 2^n - 1 \). \qed

**Definition.** For \( n \geq 3 \), we write
\[
Q_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, xy = yx^{-1} \rangle
\]
for the generalised quaternion group of order \( 2^n \).

**Remark.** \( Q_{2^n} = \{1, x, \ldots, x^{2^{n-1}-1}, y, xy, \ldots, x^{2^{n-1}-1}y\} \). Each element of \( \{y, xy, \ldots, x^{2^{n-1}-1}y\} \) has order 4 in \( Q_{2^n} \), and the element \( x^{2^{n-2}} \) is the unique involution in \( Q_{2^n} \).

**Definition.** For \( n \geq 4 \), we write
\[
SD_{2^n} := \langle x, y \mid x^{2^{n-1}} = y^2 = 1, xy = yx^{2^{n-2}-1} \rangle
\]
for the semidihedral group of order \( 2^n \).

**Remark.** \( SD_{2^n} = \{1, x, \ldots, x^{2^{n-1}-1}, y, xy, \ldots, x^{2^{n-1}-1}y\} \). In \( SD_{2^n} \), any element of \( \{xy, x^3y, \ldots, x^{2^{n-1}-1}y\} \cup \{x^{2^{n-3}}, x^{-(2^{n-3})}\} \) has order 4 while elements of \( \{y, x^2y, \ldots, x^{2^{n-2}-2}y\} \cup \{x^{2^{n-2}}\} \) are involutions. \( SD_{2^n} \) contains \( 2^{n-2} + 1 \) involutions and \( 2^{n-2} + 2 \) elements of order 4.

**Lemma 14.** Let \( G \) be any of the three 2-groups of maximal class. If \( A \) is a noncyclic proper normal subgroup of \( G \), then \( [G : A] = 2 \).
Proof. Let $G$ be any of the three 2-groups of maximal class and of order $2^n$, and let $A$ be a noncyclic proper normal subgroup of $G$. Clearly, $A \not\subseteq \langle x \rangle$. Let $a \in A$ be such that $a \in \{y, xy, \ldots, x^{2^{n-1} - 1}y\}$. Now, suppose $G$ is either dihedral or generalised quaternion. We have that $a = x^i y$ for some $i \in \{0, 1, \ldots, 2^{n-1} - 1\}$. Using the relation $xy = yx^{-1}$, we obtain that $xax^{-1} = x^2(x^i y) = x^2 a$. As $A$ is normal in $G$ and $a \in A$, we deduce that $(xax^{-1})a^{-1} = x^2 \in A$. So $\langle x^2 \rangle \subseteq A$. Let $G$ be a semidihedral group. If $a = x^{2i+1}y$ for some $i \in \{0, 1, \ldots, 2^{n-2} - 1\}$, then using the relation $xy = yx^{2^{n-2} - 1}$, we obtain that $xax^{-1} = yx^{-2i-3}$. Therefore $a(xax^{-1}) = x^{2i+1}yyx^{-2i-3} = x^{-2}$. As $A$ is normal in $G$ and $a \in A$, we conclude that $x^{-2} \in A$; whence $\langle x^{-2} \rangle = \langle x^2 \rangle \subseteq A$. If $a = x^{2i}y$ for some $i \in \{0, 1, \ldots, 2^{n-2} - 1\}$, then using the relation $xy = yx^{2^{n-2} - 1}$, we obtain that $xax^{-1} = yx^{2^{n-2}-2i-2}$. So $a(xax^{-1}) = x^{2i}yyx^{2^{n-2}-2i-2} = x^{2^{n-2} - 2} \in A$. But the order of $x^{2^{n-2} - 2}$ is the same as the order of $x^2$; whence $\langle x^{2^{n-2} - 2} \rangle = \langle x^2 \rangle \subseteq A$. In all the cases, we have these three in common: $[G : \langle x^2 \rangle] = 4, \langle x^2 \rangle \subseteq A \subseteq G$ and $\langle x^2 \rangle \neq A \neq G$. Therefore $[G : A] = 2$. \hfill $\square$

Proposition 15. Let $G$ be any of the three 2-groups of maximal class, and of order $2^n$ for some $n \geq 4$. Given $k \in \{1, 2, \ldots, n - 2\}$, the number of subgroups of order $2^{n-k}$ is $2^k + 1$.

Proof. Let $G = G_{2^n}$ be any of the three 2-groups of maximal class, and of order $2^n$ for some $n \geq 4$, and let $k \in \{1, 2, \ldots, n - 2\}$ be arbitrary. We show that there are $2^k + 1$ subgroups of size $2^{n-k}$. The first case ($k = 1$) follows from the well-known fact that there are 3 subgroups of index 2 in $G$; the subgroups of index 2 in $G$ are $\langle x \rangle, \langle x^2, y \rangle$ and $\langle x^2, xy \rangle$, where $\langle x \rangle \cong C_{2^{n-1}}$ and $\langle x^2, y \rangle \cong G_{2^{n-1}} \cong \langle x^2, xy \rangle$.

Let $H$ be a non-trivial subgroup of $G$. Recall that every non-trivial subgroup of a 2-group is contained in an index 2-subgroup of the group. Let $k \in \{1, 2, \ldots, n - 2\}$, and suppose $H$ is a subgroup of size $2^{n-k}$ in $G$. In the light of Lemma 14, $H$ is contained in either $\langle x \rangle$ or one of the noncyclic subgroups of index 2 in any (noncyclic) subgroup of $G$ which is isomorphic to $G_{2^{n-k} + 1}$. But there are $2^k$ noncyclic subgroups of index $2^k$ in $G_{2^n}$ for any $k \in \{1, 2, \ldots, n - 2\}$, where $n \geq 4$. Thus, the subgroups of size $2^{n-k}$ (i.e., subgroups of index $2^k$) in $G_{2^n}$ are the unique cyclic subgroup of size $2^{n-k}$ and the $2^k$ non-cyclic subgroups of index $2^k$. Therefore there are $1 + 2^k$ subgroups of size $2^{n-k}$ in $G_{2^n}$. \hfill $\square$

Theorem 16. Given an integer $n \geq 3$, $s(Q_{2^n}) = 2^{n-1} + n - 1$ and $nps(Q_{2^n}) = 2^{n-1} - 1$.

Proof. In the light of Proposition 15, the number of subgroups of size $2^k$ in $Q_{2^n}$ and $D_{2^n}$ are equal for each $k \in \{2, 3, \ldots, n - 1\}$. As the the number of subgroups of index 2 in both $D_8$ and $Q_8$ is 3, one sees immediately that the assertion is also true.
for both $D_8$ and $Q_8$. The distinction between the number of subgroups of various sizes in $Q_{2^n}$ and $D_{2^n}$ (where $n \geq 3$) is in the subgroups of size 2. In particular, we have only one subgroup of size 2 in $Q_{2^n}$ as opposed to $D_{2^n}$, where there are $2^{n-1} + 1$ subgroups of size 2. Thus,

$$s(Q_{2^n}) = s(D_{2^n}) - (2^{n-1} + 1) + 1$$

$$= 2^{n-1} + n - 1 \text{ (by Corollary 13).}$$

For the second part, let $m \in \mathbb{N} \cup \{0\}$ be arbitrary, and $G = Q_{2^n}$ for $n \geq 3$. Firstly, $G^{4m+1} = \langle 1, x^{4m+1}, \ldots, x^{-(4m+1)}, y, xy, \ldots, x^{2^{n-1} - 1}y \rangle$. But $\{1, y, xy, \ldots, x^{2^{n-1} - 1}y\} \subseteq G^{4m+1}$; whence $|G^{4m+1}| \geq \frac{1}{2}|G|$. As $G^{4m+1}$ is a subgroup of $G$, we conclude that $G^{4m+1} = G$. Secondly, $G^{4m+3} = \langle 1, x^{4m+3}, \ldots, x^{-(4m+3)}, y^{-1}, (xy)^{-1}, \ldots, (x^{2^{n-1} - 1}y)^{-1} \rangle$. As $|\{1, y^{-1}, (xy)^{-1}, \ldots, (x^{2^{n-1} - 1}y)^{-1}\}| \geq \frac{1}{2}|G|$, we deduce that $G^{4m+3} = G$. Thirdly, $G^{4m+2} = \langle 1, x^{4m+2}, \ldots, x^{-(4m+2)}, x^{2^{n-2}} \rangle = \langle x^2 \rangle \cong C_{2^{n-2}}$. Finally, $G^{4m} = \langle 1, x^{4m}, x^{8m}, \ldots, x^{-8m}, x^{-4m} \rangle = \langle x^4 \rangle$. If $G = Q_8$, then $\langle x^{4m} \rangle \cong \{1\}$. If $G = Q_{16}$, then $\langle x^{4m} \rangle \cong \{1\}$ or $\langle x^4 \rangle$, where $\langle x^4 \rangle \cong C_2$. Now, let $n \geq 5$, and suppose $\langle x^{4m} \rangle \neq \{1\}$. Then $\langle x^{4m} \rangle$ is exactly one of the following occurring subgroups of $Q_{2^n}$:

$$\langle x^{2^{n-2}} \rangle, \langle x^{2^{n-3}} \rangle, \ldots, \langle x^4 \rangle,$$

where

$$\langle x^{2^{n-2}} \rangle \cong C_2, \langle x^{2^{n-3}} \rangle \cong C_4, \ldots, \langle x^4 \rangle \cong C_{2^{n-3}}.$$

Therefore, $ps(Q_{2^n}) = n$; whence $nps(Q_{2^n}) = 2^{n-1} + (n - 1) = 2^{n-1} - 1$. \qed

**Theorem 17.** Given an integer $n \geq 4$,

$$s(SD_{2^n}) = 3(2^{n-2}) + n - 1 \text{ and } nps(SD_{2^n}) = 3(2^{n-2}) - 1.$$

**Proof.** In the light of Proposition 15, the number of subgroups of size $2^k$ in $SD_{2^n}$ and $D_{2^n}$ are equal for each $k \in \{2, 3, \ldots, n - 1\}$. The distinction between the number of subgroups of various sizes in $SD_{2^n}$ and $D_{2^n}$ is in the subgroups of size 2. In particular, we have only $2^{n-2} + 1$ subgroups of size 2 in $SD_{2^n}$ whilst there are $2^{n-1} + 1$ subgroups of size 2 in $D_{2^n}$. Thus,

$$s(SD_{2^n}) = s(D_{2^n}) - (2^{n-1} + 1) + (2^{n-2} + 1)$$

$$= 3(2^{n-2}) + n - 1 \text{ (by Corollary 13).}$$

For the second part, let $m \in \mathbb{N} \cup \{0\}$ be arbitrary, and $G = SD_{2^n}$ for $n \geq 4$. Then

$$G^{4m+1} = G = G^{4m+3}$$

follows from similar arguments as in the proof of Theorem 16. On the other hand, the results for $G^{4m}$ and $G^{4m+2}$ are also the same with the results for the generalised quaternion cases. Thus, $ps(SD_{2^n}) = n$; whence $nps(SD_{2^n}) = 3(2^{n-2}) + (n - 1) - n = 3(2^{n-2}) - 1$. \qed
Acknowledgement. The first author was supported by the Austrian Science Fund (FWF): P30934-N35, F05503 and F05510.

References

1. Y. Berkovich, *Groups of prime power order, Volume 1*, De Gruyter Expositions in Mathematics, Vol. 46, De Gruyter, Berlin, 2008.
2. S. Cavior, The subgroups of dihedral groups, *Mathematics Magazine* 48 (1975), 107.
3. M. Sved, Gaussians and Binomials, *Ars Combinatoria* 17A (1984), 325–351.
4. W. Zhou, W. Shi, and Z. Duan, A new criterion for finite noncyclic groups, *Communications in Algebra* 34 (2006), 4453–4457.

Received 22 December, 2020.