Research Article

Characterizing Finite Groups Using the Sum of the Orders of the Elements

Joshua Harrington, 1 Lenny Jones, 2 and Alicia Lamarche 2

1 Department of Mathematics, Cedar Crest College, Allentown, PA 18104, USA
2 Department of Mathematics, Shippensburg University, Shippensburg, PA 17257, USA

Correspondence should be addressed to Lenny Jones; lkjone@ship.edu

Received 24 August 2014; Accepted 24 October 2014; Published 13 November 2014

Academic Editor: Laszlo A. Szekely

Copyright © 2014 Joshua Harrington et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We give characterizations of various infinite sets of finite groups $G$ under the assumption that $G$ and the subgroups $H$ of $G$ satisfy certain properties involving the sum of the orders of the elements of $G$ and $H$. Additionally, we investigate the possible values for the sum of the orders of the elements of $G$.

1. Introduction

For any nonempty subset $X$ of a finite group $G$, we let $\psi(X)$ denote the sum of the orders of all elements of $X$ (counting multiplicities). Amiri et al. [1] gave a characterization of cyclic groups using $\psi$. They showed that if $C$ is a cyclic group and $G$ is a noncyclic group of the same order, then $\psi(G) < \psi(C)$. In 2011, H. Amiri and S. M. J. Amiri [2] turned their attention to the minimum value of $\psi(G)$, and they showed that, for nilpotent groups of a fixed order, the minimum value is attained when each Sylow subgroup has prime exponent. In addition, they showed that if there exists a nonnilpotent group of fixed order $n$, then the minimum value of $\psi(G)$, as $G$ ranges over all groups of order $n$, will be attained for a nonnilpotent group. Moreover, this minimum value of $\psi$ on such a nonnilpotent group is strictly smaller than the value of $\psi$ on any nilpotent group of order $n$. In the same article, H. Amiri and S. M. J. Amiri conjectured that if $H$ is a simple group and $G$ is a nonsimple group of order $|H|$, then $\psi(H) < \psi(G)$. However, this conjecture has recently been shown to be false [3]. In 2012, H. Amiri and S. M. J. Amiri [4] showed that $\psi(H) < \psi(A_n)$ for all proper subgroups $H \neq A_n$ of $S_n$, where $S_n$ is the symmetric group and $A_n$ is the alternating group.

In this paper, we give characterizations of various infinite sets of finite groups $G$, given certain restrictions on $\psi(G)$ or $\psi(H)$ (or both), where $H$ is a proper subgroup of $G$. More precisely, we prove the following.

Theorem 1. Let $G$ be a finite abelian group. Then $\psi(H)$ divides $\psi(G)$ for every subgroup $H$ of $G$ if and only if $G$ is cyclic of square-free order.

Theorem 2. Let $G$ be a finite abelian group. Then $\psi(H) < |G|$ for every proper subgroup $H$ of $G$ if and only if

\[ G = \mathbb{Z}_p \quad \text{or} \quad G = \left( \mathbb{Z}_p \right)^n = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p, \]

for any prime $p$ and any positive integer $n$.

Theorem 3. For any fixed $\epsilon > 0$, there exist infinitely many finite groups $G$, both abelian and nonabelian that satisfy the conditions in each of the following situations:

1. $\psi(G) < |G|^{1+\epsilon}$,
2. $\psi(G) > |G|^{2-\epsilon}$.

Theorem 4. Let $n$ be a positive integer. Then

\[ \psi(S_n) \leq n! \frac{\log(3)}{\log(2)} \quad \forall n \geq 1. \]

Moreover, the number $\log(3)/\log(2)$ is the smallest possible constant $C$ such that $\psi(S_n) \leq n!^C$ for all $n \geq 1$. 
2. Preliminaries and Notation

We assume that all groups in this paper are finite. For an element \( g \) in a group \( G \), we let \( o(g) \) denote the order of \( g \) in \( G \). For a group \( G \), a prime \( p \) that divides \( |G| \), and a positive integer \( z \), we define

\[
G_{p^z} = \{ g \in G \mid o(g) = p^z \}. \tag{3}
\]

We let \( S_n \) and \( A_n \) denote, respectively, the symmetric group and the alternating group on the set \( \{1, 2, \ldots, n\} \). We let \( \phi \) denote Euler’s totient function.

We now state, without proof, two useful results from the literature, the first of which was mentioned previously in Section 1.

**Theorem 5** (see [1]). If \( C \) is a cyclic group and \( G \) is a noncyclic group of the same order, then \( \psi(G) < \psi(C) \).

**Lemma 6** (see [2]). If \( H \) and \( K \) are finite groups, then \( \psi(H \times K) \leq \psi(H)\psi(K) \), with equality if and only if \( \gcd(|H|, |K|) = 1 \).

The following lemma, which we also state without proof, is a special case of Theorem A in [2]..

**Lemma 7.** Let \( p \) be a prime and let \( n \) be a positive integer. If \( G \) is an abelian group with \( |G| = p^n \), then

\[
\psi(G) \geq \psi \left( \left( \mathbb{Z}_p \right)^n \right). \tag{4}
\]

Lemma 7 shows that the minimum value of \( \psi(G) \), as \( G \) ranges over all abelian \( p \)-groups of fixed order \( p^n \), is achieved on the elementary abelian group of that order. Lemma 7 will be useful in proving Theorem 2.

3. The Proof of Theorem 1

For the sake of convenience, we say that \( G \) is a \( \psi \)-divisible group if \( \psi(H) \) divides \( \psi(G) \) for all subgroups \( H \) of \( G \). We can deduce the following result concerning \( \psi \)-divisible groups from Lemma 6.

**Lemma 9.** Let \( H \) and \( K \) be finite groups with \( \gcd(|H|, |K|) = 1 \), and let \( G = H \times K \). Then \( G \) is a \( \psi \)-divisible group if and only if both \( H \) and \( K \) are \( \psi \)-divisible groups.

**Proof.** Suppose first that \( G \) is a \( \psi \)-divisible group. Assume, by way of contradiction and without loss of generality, that \( K \) is not \( \psi \)-divisible. Then there is some subgroup \( B \) of \( K \) such that \( \psi(B) \) does not divide \( \psi(K) \). Consider the subgroup \( H \times B \) of \( G \). Using Lemma 6, since \( G \) is a \( \psi \)-divisible group, we have that

\[
\psi((H \times B)) \equiv \psi(H) \equiv 1 \mod p,
\]

for some positive integer \( k \). But then \( \psi(B)k = \psi(K) \), which contradicts our assumption that \( \psi(B) \) does not divide \( \psi(K) \).

Suppose now that both \( H \) and \( K \) are \( \psi \)-divisible, and let \( W \) be a subgroup of \( G \). Since \( \gcd(|H|, |K|) = 1 \), it follows that \( W = A \times B \), where \( A \) is a subgroup of \( H \), and \( B \) is a subgroup of \( K \). Then, by Lemma 6, we have that

\[
\frac{\psi(G)}{\psi(W)} = \frac{\psi(H)}{\psi(A)} \cdot \frac{\psi(K)}{\psi(B)} \in \mathbb{Z}, \tag{9}
\]

which implies that \( G \) is a \( \psi \)-divisible group.

In light of Lemma 9, it is enough to focus our attention on \( p \)-groups, where \( p \) is a prime. Recall for a given positive integer \( z \) and a prime \( p \) that divides \( |G| \), that \( G_{p^z} \) is the subset of \( G \) containing all elements of order \( p^z \). Note that \( \psi(G_{p^z}) \equiv 0 \mod p \) when \( z \geq 1 \). Two obvious, but useful, consequences of this observation are given below.

**Lemma 10.** Let \( p \) be a prime and let \( G \) be a \( p \)-group. Then

\[
\psi(G) \equiv 1 \mod p.
\]

**Proof.** Let \( p^a \) be the exponent of \( G \). Then

\[
\psi(G) = \sum_{i=0}^{a} \psi \left( G_{p^i} \right) = 1 + \sum_{i=1}^{a} \psi \left( G_{p^i} \right) \equiv 1 \mod p. \tag{10}
\]

**Corollary 11.** Let \( p \) be a prime and let \( G \) be a \( p \)-group. If \( G \) is a \( \psi \)-divisible group and \( H \) is any proper subgroup of \( G \), then

\[
\frac{\psi(G)}{\psi(H)} \geq p + 1. \tag{11}
\]

**Lemma 12.** Let \( a \) and \( n \) be positive integers, and let \( p \) be a prime. Suppose that \( G = (\mathbb{Z}_p^n)^a \). Then \( G \) is a \( \psi \)-divisible group if and only if \( a = n = 1 \).

\[\square\]
Proof. Clearly, $G$ is a $\psi$-divisible group if $a = n = 1$, so assume that $an \geq 2$. First suppose that $a = 1$, so that $n \geq 2$. Then, using Proposition 8 with $a = 1$, we have

$$\psi(G) = \frac{p^{2(n+1)} - p^{n+2} + p - 1}{p^{n+1} - 1} = p^n - p + 1. \quad (12)$$

Let $H$ be a subgroup of $G$ such that $H = (Z_p)^{n-1}$. Then $\psi(H) = p^n - p + 1$ by Proposition 8, and thus

$$\frac{\psi(G)}{\psi(H)} = \frac{p^{n+1} - p + 1}{p^n - p + 1} = p + \frac{p^2 - 2p + 1}{p^n - p + 1} \notin Z. \quad (13)$$

since $p^2 - 2p + 1 < p^n - p + 1$. Hence, $G$ is not a $\psi$-divisible group when $a = 1$.

Now assume that $a \geq 2$, and let $H$ be a subgroup of $G$ such that $H = (Z_p)^{n-1}$. Again, using Proposition 8, we can write

$$\frac{\psi(G)}{\psi(H)} = \frac{p^{n+1} - A}{B} \quad (14)$$

where

$$A = p^{n+1}(p-1) - (p-1), \quad (15)$$

$$B = p^{(n+1)a-n}(p^n - 1) + p - 1.$$ 

Since $a \geq 2$, it follows that $A < B$, and hence $\psi(G)/\psi(H) \notin Z$. Thus, $G$ is not a $\psi$-divisible group and the proof is complete.

**Lemma 13.** Let $p$ be a prime and suppose that $G = Z_p \times H$, where

$$H = Z_{p^a} \times Z_{p^b} \times \cdots \times Z_{p^n}, \quad (16)$$

is nontrivial, with $a_1 \leq a_2 \leq \cdots \leq a_t$. Then $G$ is not a $\psi$-divisible group.

**Proof.** Let $(x, y) \in Z_p \times H$, and define

$$A = \{(x, y) \mid x \neq 0, y \neq 0\}, \quad (17)$$

$$B = \{(x, 0) \mid x \neq 0\},$$

$$C = \{(0, y) \mid y \in H\}.$$

Then $Z_p \times H = A \cup B \cup C$ and

$$\psi(G) = \psi(A) + \psi(B) + \psi(C)$$

$$= (p-1)(\psi(H) - 1) + (p-1)p + \psi(H) \quad (18)$$

$$= p\psi(H) + p^2 - 2p + 1.$$ 

Thus

$$\frac{\psi(G)}{\psi(H)} = \frac{p + \frac{p^2 - 2p + 1}{\psi(H)}}{\psi(H)} \notin Z, \quad (19)$$

since

$$p^2 - 2p + 1 < p^2 - p + 1 = \psi(Z_p) \leq \psi((Z_p)^1) \leq \psi(H). \quad (20)$$

**Lemma 14.** Let

$$G = Z_{p^{a_1}} \times Z_{p^{a_2}} \times \cdots \times Z_{p^{a_t}}, \quad (21)$$

where $a_1 \leq a_2 \leq \cdots \leq a_t$ are not all equal. Then

$$\sum_{i=0}^{a_{t-1}} \psi(G_{p^i}) < \frac{1}{p^2 - p}. \quad (22)$$

**Proof.** Note that $a_i \geq 2$ and $t \geq 2$ since $a_i$ are not all equal. Suppose that

$$a_1 \leq a_2 \leq \cdots \leq a_{k-1} < a_k = a_{k+1} = \cdots = a_t, \quad (23)$$

and define

$$b_i = \begin{cases} a_i & \text{if } i < k \\ a_i - 1 & \text{if } k \leq i < t \\ a_i & \text{if } i = t. \end{cases} \quad (24)$$

Let

$$\tilde{G} = Z_{p^{b_1}} \times Z_{p^{b_2}} \times \cdots \times Z_{p^{b_t}}, \quad (25)$$

and observe that

$$\sum_{i=0}^{a_{t-1}} \psi(G_{p^i}) = \sum_{i=0}^{b_{t-1}} \psi(\tilde{G}_{p^i}) \geq \psi(\tilde{G}_{p^t}). \quad (26)$$

Thus, we may assume without loss of generality that $k = t$. Let $H$ be a subgroup of $G$ such that

$$H = Z_{p^{a_1}} \times Z_{p^{a_2}} \times \cdots \times Z_{p^{a_{t-1}}}. \quad (27)$$

Since $\psi(H) = \sum_{i=0}^{a_{t-1}} \psi(G_{p^i})$, we have that

$$\psi(G_{p^{a_t}}) = \psi(G_{p^t}) = \psi(p^{a_t}) \prod_{i=1}^{t-1} p^{a_i}$$

$$= (p^2 - p)a_1 \sum_{i=1}^{t-1} (p^{2a_i-2} - 1)$$

$$> (p^2 - p) (p^{2a_t-2} - 1) + 1$$

$$= (p^2 - p) (p^{a_{t-1}} - 1) + 1 \quad (28)$$

$$\geq (p^2 - p) \psi(H)$$

$$= (p^2 - p) \sum_{i=0}^{a_{t-1}} \psi(G_{p^i}),$$

from which the lemma follows.

We are now in a position to establish Theorem 1. For the convenience of the reader, we restate Theorem 1 below as Theorem 15 using the $\psi$-divisible terminology.

**Theorem 15.** Let $G$ be an abelian group. Then $G$ is a $\psi$-divisible group if and only if $G$ is cyclic of square-free order.
Proof. If $G$ is cyclic of square-free order, then the fact that $G$ is a $\psi$-divisible group follows immediately from Lemma 6. So, now assume conversely that $G$ is a $\psi$-divisible group. To establish the theorem, it is enough, by Lemmas 6, 12, and 13, to show for a prime $p$ that

$$G = Z_{p^n_1} \times Z_{p^n_2} \times \cdots \times Z_{p^n_t}, \tag{29}$$

where $t \geq 2$ with $2 \leq a_1 \leq a_2 \leq \cdots \leq a_t$ not all equal, is not a $\psi$-divisible group. Let $G$ be as in (29), and assume by way of contradiction that $G$ is a $\psi$-divisible group. Let $H$ be a subgroup of $G$ with

$$H = Z_{p^{n_1}} \times Z_{p^{n_2}} \times Z_{p^{n_3}} \times \cdots \times Z_{p^{n_t}}. \tag{30}$$

Note that $\psi(G_{p^n}) = p\psi(H_{p^n}).$ Using this observation, Lemma 14, and Corollary 11, it follows that

$$1 + \frac{1}{p^k - p} > 1 + \frac{\sum_{i=0}^{t} \frac{1}{\psi(G_{p^n})}}{\psi(G_{p^n})}$$

$$= \frac{\psi(G)}{\psi(G_{p^n})} = \frac{\psi(G)}{p\psi(H_{p^n})} \tag{31}$$

$$\geq \frac{\psi(H)}{p\psi(H)} \geq \frac{p + 1}{p}. \tag{32}$$

Using the fact that $p > 0$ to solve the inequality

$$1 + \frac{1}{p^k - p} > \frac{p + 1}{p}, \tag{33}$$

we get that $1 < p < 2$, which is impossible, and the proof is complete. \qed

The following is immediate from Theorem 15.

Corollary 16. If $G$ is an abelian $\psi$-divisible group, then every proper subgroup of $G$ is a $\psi$-divisible group.

Remark 17. The converse of Corollary 16 is false. For example, let $G = Z_p \times Z_p$, where $p$ is a prime. Then every proper subgroup of $G$ is a $\psi$-divisible group, but $G$ is not a $\psi$-divisible group by Lemma 12.

3.1. A Remark on Nonabelian $\psi$-Divisible Groups. The non-abelian situation is much less clear than the abelian case. In fact, we have been unable to find a single nonabelian $\psi$-divisible group, although we are somewhat hesitant to conjecture their nonexistence. On the other hand, using Lemma 9, we are able to construct infinitely many nonabelian groups that are not $\psi$-divisible. Since $\psi(S_3) = 13$, we see that $S_3$ is not $\psi$-divisible. Then, by Lemma 9, it follows that $G = Z_p \times S_3$ is not $\psi$-divisible for any prime $p$.

4. The Proof of Theorem 2

We say a group $G$ is a $\mathcal{B}_\psi$-group if $\psi(H) < |G|$ for all proper subgroups $H$ of $G$. For the convenience of the reader, we use this new terminology to restate Theorem 2 below as Theorem 18.

Theorem 18. Let $G$ be a finite abelian group. Then $G$ is a $\mathcal{B}_\psi$-group if and only if

$$G = Z_{p^n} \quad \text{or} \quad G = (Z_{p^n})^n, \tag{33}$$

for any prime $p$ and any positive integer $n$.

Proof. Using Proposition 8, it is easy to show that if

$$G = Z_{p^n} \quad \text{or} \quad G = (Z_{p^n})^n, \tag{34}$$

for any prime $p$ and any positive integer $n$, then $G$ is a $\mathcal{B}_\psi$-group.

So, assume conversely that $G$ is an abelian $\mathcal{B}_\psi$-group, and write

$$G = A_1 \times A_2 \times \cdots \times A_k, \tag{35}$$

where $|A_i| = p_i^{n_i}$ and $p_1 < p_2 < \cdots < p_k$ are primes. Assume first that $k \geq 2$, and let $H$ be a subgroup of $G$ such that

$$H = B_1 \times B_2 \times \cdots \times B_k, \tag{36}$$

where $|B_i| = p_i^{n_i - 1}$. We claim that $\psi(H) > |G|$. To see this, we have

$$\psi(H) = \psi(B_1) \prod_{i=2}^{k} \psi(A_i) \tag{37}$$

$$\geq \prod_{i=2}^{k} \psi((Z_{p_i})^{a_i}) \tag{38}$$

$$= \prod_{i=2}^{k} (p_i - p_i + 1) \prod_{i=2}^{k} (p_i^{a_i + 1} - p_i + 1) \tag{39}$$

by (Proposition 8)

$$= \left( - \frac{p_i - 1}{p_i} \right)^{k} \prod_{i=2}^{k} \left( p_i - \frac{p_i - 1}{p_i} \right) \tag{40}$$

which shows that $G$ is not a $\mathcal{B}_\psi$-group if $k \geq 2$. Hence, assume that $k = 1$ so that $G$ is a $p$-group for some prime $p$. Suppose that $|G| = p^n$ and write

$$G = Z_{p^n_1} \times Z_{p^n_2} \times \cdots \times Z_{p^n_t}, \tag{41}$$
where
\[ \alpha = \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_t = \beta. \]  
(39)
Assume first that \( t \geq 2 \). Let \( B = \mathbb{Z}_{p^\alpha} \times \cdots \times \mathbb{Z}_{p^\alpha} \), where \( B \) is trivial if \( t = 2 \), so that \( |B| = p^{\alpha_t - \beta} \). Let \( H \) be a subgroup of \( G \) such that
\[ H \cong \mathbb{Z}_{p^\alpha} \times B \times \mathbb{Z}_{p^\beta}. \]
(40)
Then
\[ |G| = p^n > \psi(H) = \psi(H_{p^\beta}) \geq \phi(p^\beta) \cdot |\mathbb{Z}_{p^\alpha} \times B| = p^{n\beta - 2}(p - 1). \]
(41)
Thus \( \beta = 1 \) and \( G = (\mathbb{Z}_p)^n \), where \( n \geq 2 \).

Now suppose that \( t = 1 \) so that \( G = \mathbb{Z}_{p^a} \). Let \( H \) be the subgroup of \( G \) with \( H = \mathbb{Z}_{p^t} \). Then, using Proposition 8, we have
\[ |G| = p^a > \psi(H) = \frac{p^{2(a-1)+1}}{p+1} > \frac{p^{2a-1}}{p+1}, \]
(42)
which implies that \( p+1 > p^{a-1} \). Hence, \( \alpha \leq 2 \) and \( G = \mathbb{Z}_p \) or \( G = \mathbb{Z}_{p^a} \), which completes the proof of the theorem. \( \square \)

5. Investigating the Range of \( \psi \)

It is easy to get bounds on \( \psi(G) \) as the next proposition shows.

Proposition 19. Let \( G \) be a finite group. Then
\[ |G| \leq \psi(G) \leq |G|^2, \]
with equality holding in both inequalities in (43) if and only if \( G \) is trivial.

Proof. For any \( g \in G \), we have that \( 1 \leq o(g) \leq |G| \). Thus, the proposition follows from the definition of \( \psi \).
\( \square \)

A natural question to ask is whether there exist nontrivial groups \( G \) with \( \psi(G) \) arbitrarily close to the bounds given in (43). Theorem 3 provides an affirmative answer to this question.

5.1. The Proof of Theorem 3

Proof of Theorem 3. To prove part (1) of Theorem 3, first let \( G = S_3 \times (\mathbb{Z}_p)^n \), where \( p \geq 13 \) is a prime and \( n \) is a positive integer. Then, using Lemma 6, and Proposition 8 with \( a = 1 \), we have that
\[ \psi(G) = \psi(S_3) \psi((\mathbb{Z}_p)^n) = 13(p^{n+1} - p + 1). \]
(44)
Solving the equation
\[ 13(p^{n+1} - p + 1) = |G|^c = (6p^n)^c, \]
(45)
for \( c \) gives
\[ c = \frac{\log(13(p^{n+1} - p + 1))}{\log(6p^n)}. \]
(46)
Since
\[ 13(p^{n+1} - p + 1) - 6p^n > 13(p^{n+1} - p + 1) - 13p^n = 13(p^n - 1)(p - 1) > 0, \]
(47)
it follows that \( c > 1 \). Then, since \( p \geq 13 \), we have
\[ \frac{1 + 2}{n} = \frac{\log(p^{n+2})}{\log(p^n)} \geq \frac{\log(13p^{n+1})}{\log(p^n)} \]
\[ > \frac{\log(13p^{n+1})}{\log(6p^n)} > c > 1. \]
(48)
A similar computation gives the same conclusion when \( G = (\mathbb{Z}_p)^n \), and the proof of part (1) of Theorem 3 is complete.

To prove part (2) of Theorem 3, first let \( G = S_3 \times \mathbb{Z}_p \), where \( p \geq 13 \) is prime and \( a \) is a positive integer. Then, using Lemma 6, and Proposition 8 with \( n = 1 \), we have that
\[ \psi(G) = \psi(S_3) \psi(\mathbb{Z}_p) = 13\left(\frac{2a+1}{p} \right). \]
(49)
Solving the equation
\[ 13\left(\frac{2a+1}{p} \right) = |G|^c = (6p)^c \]
(50)
for \( c \) gives
\[ c = \frac{\log(13(\frac{2a+1}{p})))}{\log(6p^a)}. \]
(51)
Since
\[ 13(2a+1) + 13 < 36(2a+1) + 36a = 36p^{2a}(p+1), \]
(52)
it follows that \( c < 2 \). Also, since \( p^2 > p + 1 \), we see that
\[ p^{2a-1} \cdot \frac{p^2}{p+1} < \frac{p^{2a+1}}{p+1} < \frac{p^{2a+1} + 1}{p+1}. \]
(53)
Thus,
\[ 2 - \frac{3}{a+1} = \frac{\log(p^{2a-1})}{\log(p^{a+1})} < \frac{\log(13p^{2a-1})}{\log(p^{a+1})} \]
\[ < \frac{\log(13p^{2a-1})}{\log(6p^a)} \]
(54)
(since \( p \geq 13 \))
\[ < c \quad \text{(by (53))}. \]
Therefore,
\[ 2 - \frac{3}{a+1} < c < 2. \] (55)

A similar computation yields the same conclusion when \( G = \mathbb{Z}_{p^r} \), which completes the proof of Theorem 3.

5.2. The Proof of Theorem 4. It is clear that estimating \( \psi(S_n) \) is, up to scaling, equivalent to estimating the average order 
\[ \mu_n := \psi(S_n)/n! \] of an element in \( S_n \). This problem was first raised by Erdős and Turán [5] in 1968 when they conjectured that
\[ \log(\mu_n) = O\left(\sqrt{\frac{n}{\log n}}\right). \] (56)

Conjecture (56) was proven by Schmutz [6] in 1989 when he showed that
\[ \log(\mu_n) \leq 7.7\sqrt{\frac{n}{\log n}} \quad \text{for } n \text{ sufficiently large.} \] (57)

It follows from (57) that
\[ \psi(S_n) \leq (n!)^{h(n)} \quad \text{for } n \text{ sufficiently large,} \] (58)

where
\[ h(n) = \frac{7.7\sqrt{n/\log(n)}}{\log(n!)} + 1. \] (59)

The proof of (57) is nontrivial and requires some very technical results concerning partitions. In 1991, Goh and Schmutz [7] sharpened (57) by proving that
\[ \log(\mu_n) \sim c\left(\sqrt{\frac{n}{\log n}}\right), \] (60)

where
\[ c = 2\int_0^\infty \log\left(\log\left(\frac{e}{1-e^{-t}}\right)\right) dt. \] (61)

The proof of (60) also requires some partition theory.

In the spirit of Theorem 3, it is our goal here to determine, if possible, the smallest possible constant \( C \) such that
\[ \psi(S_n) \leq (n!)^C \quad \forall n \geq 1, \] (62)
in a nontrivial manner. In other words, does there exist a smallest real number \( C < 2 \) for which (62) is true, and can we determine it? Theorem 4 provides an affirmative answer to these questions. There are two advantages to the bound given for \( \psi(S_n) \) in Theorem 4 over the results in [6, 7]. First of all, Theorem 4 is proven for all \( n \geq 1 \), not just for sufficiently large values of \( n \). The second advantage is that the proof of Theorem 4 that we present here does not rely on any results from partition theory. We use the following result, due to Massias [8] in 1984.

**Theorem 20.** Let \( g_n \) denote the largest order of an element in \( S_n \). Then
\[ \log(g_n) \leq 1.05314\sqrt{n \log(n)}. \] (63)

In 1903, Landau [9] proved that \( \log(g_n) \sim \sqrt{n \log(n)} \), but Theorem 20 represents the first explicit upper bound for \( \log(g_n) \). Although somewhat technical, Massias’ proof of Theorem 20 uses elementary analytic techniques requiring little more than calculus.

We also need the following lemmas.

**Lemma 21.** Let \( n \geq 2 \) be an integer and let \( \sigma, \tau \in S_n \), with \( \sigma = (ab) \). If \( r \) fixes either \( a \) or \( b \), then \( o(\sigma r) \leq n \cdot o(r) \).

**Proof.** Observe that if \( r \) fixes both \( a \) and \( b \), then
\[ o(\sigma r) = \text{lcm}(o(\sigma), o(r)) = o(\sigma) \cdot o(r) = 2 \cdot o(r) \leq n \cdot o(r). \]

So, suppose that \( r \) fixes \( b \), but not \( a \). Then we may write
\[ r = r_1 r_2 = (ax_1x_2 \cdots x_j) r_2, \] (65)

for some \( j \) with \( 2 \leq j \leq n - 1 \), where \( r_1 \) and \( r_2 \) are disjoint, and \( x_i \neq b \) for all \( i \). Thus,
\[ o(\sigma r) = o\left((ax_1x_2 \cdots x_j b) r_2\right) = \text{lcm}(j + 1, o(r_2)) \]
\[ = \frac{(j + 1) o(r_2)}{\gcd(j + 1, o(r_2))} \leq n \cdot o(r_2) \leq n \cdot o(r), \] (66)

which completes the proof.

**Lemma 22.** If \( n \geq 4 \), then
\[ \sqrt{n - 1}(n^{3/2} - 1) > n^2 - n. \] (67)

**Proof.** If \( n \geq 4 \), then
\[ n^2 = n^{1/2} \cdot n^{3/2} \geq 2n^{3/2} > 2n^{3/2} - 1. \] (68)

Thus,
\[ n^{3/2} - 1 = \sqrt{(n^{3/2} - 1)^2} \]
\[ = \sqrt{n^3 - (2n^{3/2} - 1)} > \sqrt{n^3 - n^2} = n\sqrt{n - 1}, \] (69)

from which the lemma follows.

**Lemma 23.** If \( n \geq 20 \) is an integer, then
\[ (n - 2)! > e^{2.10628(n - 12)}. \] (70)

**Proof.** The lemma is easily verified for \( n = 20 \). We proceed by induction on \( n \). Then
\[ ((n + 1) - 2)! = (n - 1)(n - 2)! \]
\[ > (n - 1)e^{2.10628(n - 12)} \quad \text{(by induction)} \]
\[ = \frac{n - 1}{e^{2.10628}} e^{2.10628(n - 11)} \]
\[ > e^{2.10628(n - 12) - 1}, \] (71)

since \( n - 1 > e^{2.10628} \) when \( n \geq 20 \), and the proof is complete.
Lemma 24. Let \( f(x) = x - 12 - \sqrt{(x-1)} \log(x-1) \). Then \( f(x) > 0 \) for all \( x \geq 20 \).

Proof. The proof is straightforward using calculus.

Lemma 25. If \( n \geq 20 \) is an integer, then

\[
(n - 1)^{\frac{\log(3)}{\log(2)} - 1} \left( n^{\frac{\log(3)}{\log(2)} - 1} \right) \\
> n(n - 1) e^{0.5314 \sqrt{(n-1) \log(n-1)}}.
\]

Proof. Let

\[
A = (n - 1)^{\frac{\log(3)}{\log(2)} - 1} \left( n^{\frac{\log(3)}{\log(2)} - 1} \right).
\]

Since \( \log(3)/\log(2) > 3/2 \), we have

\[
A > \sqrt{(n-1)! (n^{3/2} - 1)} = \sqrt{n-1} (n^{3/2} - 1) \sqrt{(n-2)!} \\
> (n^2 - n) e^{0.5314 (n-12)} (\text{by Lemmas 22 and 23}) \\
> (n^2 - n) e^{0.5314 \sqrt{(n-1) \log(n-1)}} (\text{by Lemma 24}).
\]

Proof of Theorem 4. The proof is by induction on \( n \). It is easy to verify computationally that the theorem is true for all \( n \), with \( 1 \leq n \leq 20 \). For \( n \geq 20 \), let \( \sigma_1 = (1) \) and \( \sigma_i = (i - 1 \ n) \) for each \( i \) with \( 2 \leq i \leq n \). Then \( \{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n\} \) is a complete set of left coset representatives for \( S_{n-1} \) in \( S_n \). Thus,

\[
\psi(S_n) = \sum_{i=1}^{n} \psi(\sigma_S n-1) \\
= \sum_{i=1}^{n} \sum_{\tau \in S_{n-1}} o(\sigma_i \tau) \\
= \psi(S_{n-1}) + \sum_{i=2}^{n} \sum_{\tau \in S_{n-1}} o(\sigma_i \tau) \\
\leq \psi(S_{n-1}) + \sum_{i=2}^{n} \sum_{\tau \in S_{n-1}} n \cdot o(\tau) (\text{by Lemma 21}) \\
\leq \psi(S_{n-1}) + \sum_{i=2}^{n} n \cdot e^{0.5314 \sqrt{(n-1) \log(n-1)}} (\text{by Theorem 20})
\]

In Table 1, we compare the rounded values of \( \psi(S_n) \), \( (n!)^{\log(3)/\log(2)} \), \( (n!)^2 \), and the bound for \( \psi(S_n) \) given in (60), for \( n = 2, \ldots, 10 \). The bound given in (58) is much worse for these small values of \( n \) than any bound given in Table 1, so we omit it.

Remark 26. The sequence \( \{\psi(S_n)\}_{n=1}^{\infty} \) is listed in the On-Line Encyclopedia of Integer Sequences and can be found at http://oeis.org/A060014.

We end with the following conjecture, which is supported by numerical evidence.

Conjecture 27. Let \( n \) be a positive integer. Then

\[
\psi(A_n) \leq \left( \frac{n!}{2} \right)^{\log(7)/\log(3)} \quad \forall n \geq 1.
\]

Moreover, the number \( \log(7)/\log(3) \) is the smallest possible constant \( C \) such that \( \psi(A_n) \leq (n!/2)^C \) for all \( n \geq 1 \).

Remark 28. The sequence \( \{\psi(A_n)\}_{n=1}^{\infty} \) is listed in the On-Line Encyclopedia of Integer Sequences and can be found at http://oeis.org/A060015.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.
Acknowledgments

The authors thank the referees for the valuable comments.

References


Submit your manuscripts at http://www.hindawi.com