FINITE GROUPS OF THE SAME TYPE AS SUZUKI GROUPS

SEYED HASSAN ALAVI, ASHRAF DANESHKHAH* AND HOSEIN PARVIZI MOSAED

Communicated by Alireza Abdollahi

Abstract. For a finite group $G$ and a positive integer $n$, let $G(n)$ be the set of all elements in $G$ such that $x^n = 1$. The groups $G$ and $H$ are said to be of the same (order) type if $|G(n)| = |H(n)|$, for all $n$. The main aim of this paper is to show that if $G$ is a finite group of the same type as Suzuki groups $Sz(q)$, where $q = 2^{2^m+1} \geq 8$, then $G$ is isomorphic to $Sz(q)$. This addresses to the well-known J. G. Thompson’s problem (1987) for simple groups.

1. Introduction

For a finite group $G$ and a positive integer $n$, let $G(n)$ consist of all elements $x$ satisfying $x^n = 1$. The order type of $G$ is defined to be the function whose value at $n$ is the order of $G(n)$. In 1987, J. G. Thompson [11, Problem 12.37] posed a problem which is related to algebraic number fields:

Is it true that a group is solvable if its type is the same as that of a solvable one?

This problem links to the set $\text{nse}(G)$ of the number of elements of the same order in $G$. Indeed, it turns out that if two groups $G$ and $H$ are of the same type, then $\text{nse}(G) = \text{nse}(H)$ and $|G| = |H|$. Therefore, if a group $G$ has been uniquely determined by its order and $\text{nse}(G)$, then Thompson’s problem is true. One may ask this problem for non-solvable groups, in particular, finite simple groups. In this direction, Shao et al [13] studied finite simple groups whose order is divisible by at most four primes. Following this investigation, such problem has been studied for some families of simple groups [1, 2, 3, 13] including Suzuki groups $Sz(q)$ with $q$ prime [10]. In this paper, we generalize the main result in [10] and prove that

---


Keywords: Suzuki group, Thompson’s problem, element order.

Received: 08 March 2017, Accepted: 08 July 2017.

*Corresponding author.
Theorem 1.1. Let $G$ be a group with $nse(G) = nse(Sz(q))$ and $|G| = |Sz(q)|$. Then $G$ is isomorphic to $Sz(q)$.

As noted above, as an immediate consequence of Theorem 1.1, we have that

**Corollary 1.2.** If $G$ is a finite group of the same type as $Sz(q)$, then $G$ is isomorphic to $Sz(q)$.

In order to prove Theorem 1.1, we use a partition of Suzuki groups $S := Sz(q)$, where $q = 2^{2m+1} \geq 8$, see Lemma 3.2, that is to say, a set of subgroups $H_i$ of $S$, for $i = 1, \ldots, s$, such that each nontrivial element of $S$ belongs to exactly one subgroup $H_i$. We use this information to determine the set $nse(S)$ in Proposition 3.3. It is also a main tool to show that 2 is an isolated vertex in the prime graph of a group $G$ satisfying hypotheses of Theorem 1.1, see Proposition 4.1. Then we show that $G$ is neither Frobenius, nor 2-Frobenius group. Finally, we obtain a section of $G$ which is isomorphic to $S$ and prove that $G$ is isomorphic to $S$.

Finally, we give some brief comments on the notation used in this paper. Throughout this article all groups are finite. Our group-theoretic notation is standard, and it is consistent with the notation in [4, 6, 7]. We denote a Sylow $p$-subgroup of $G$ by $G_p$. We also use $n_p(G)$ to denote the number of Sylow $p$-subgroups of $G$. For a positive integer $n$, the set of prime divisors of $n$ is denoted by $\pi(n)$, and if $G$ is a finite group, $\pi(G) := \pi(|G|)$, where $|G|$ is the order of $G$. We denote the set of elements’ orders of $G$ by $\omega(G)$ known as spectrum of $G$. The prime graph $\Gamma(G)$ of a finite group $G$ is a graph whose vertex set is $\pi(G)$, and two vertices $p$ and $q$ are adjacent if and only if $pq \in \omega(G)$. Assume further that $\Gamma(G)$ has $t(G)$ connected components $\pi_i$, for $i = 1, 2, \ldots, t(G)$. The positive integers $n_i$ with $\pi(n_i) = \pi_i$ are called order components of $G$. Clearly, $|G| = n_1 \cdots n_{t(G)}$. In the case where $G$ is of even order, we always assume that $2 \in \pi_1$, and $\pi_1$ is said to be the even component of $G$. In this way, $\pi_i$ and $n_i$ are called odd components and odd order components of $G$, respectively. Recall that $nse(G)$ is the set of the number of elements in $G$ with the same order. In other word, $nse(G)$ consists of the numbers $m_i(G)$ of elements of order $i$ in $G$, for $i \in \omega(G)$. Here, $\phi$ is the Euler totient function.

2. Preliminaries

In this section, we introduce the some known results which will be used in the proof of the main result.

**Lemma 2.1.** [8, Theorem 9.1.2] Let $G$ be a finite group, and let $n$ be a positive integer dividing $|G|$. Then $n$ divides $|G(n)|$.

The proof of the following result is straightforward by Lemma 2.1. Recall that $nse(G) = \{m_i(G) \mid i \in \omega(G)\}$.

**Lemma 2.2.** Let $G$ be a finite group. Then for every $i \in \omega(G)$, $\phi(i)$ divides $m_i(G)$, and $i$ divides $\sum_{j \mid i} m_j(G)$. Moreover, if $i > 2$, then $m_i(G)$ is even.

**Lemma 2.3** (Theorem 3 in [15]). Let $G$ be a finite group of order $n$. Then the number of elements whose orders are multiples of $t$ is either zero, or a multiple of the greatest divisor of $n$ that is prime to $t$. 

In what follows, recall that \(t(G)\) is the number of connected components of the prime graph \(\Gamma(G)\).

**Lemma 2.4.** [5, Theorem 1] Let \(G\) be a Frobenius group of even order with kernel \(K\) and complement \(H\). Then \(t(G) = 2\), \(\pi(H)\) and \(\pi(K)\) are vertex sets of the connected components of \(\Gamma(G)\).

A group \(G\) is called 2-Frobenius if there exists a normal series \(1 \leq H \leq K \leq G\) such that \(G/H\) and \(K\) are Frobenius groups with kernel \(K/H\) and \(H\) respectively.

**Lemma 2.5.** [5, Theorem 2] Let \(G\) be a 2-Frobenius group of even order. Then \(t(G) = 2\), \(\pi(G/K) \cup \pi(H) = \pi_1\), \(\pi(K/H) = \pi_2\), and \(G/K\) and \(K/H\) are cyclic groups and \(|G/K|\) divides \(|\text{Aut}(K/H)|\).

### 3. Elements of the same order in Suzuki groups

In this section, we determine the set of the number of elements of the same order in Suzuki groups.

**Lemma 3.1** ([14]). Let \(S = \text{Sz}(q)\) with \(q = 2^{2m+1} \geq 8\). Then \(\omega(S)\) consists of all factors of 4, \(q - 1\) and \(q \pm \sqrt{2q} + 1\).

Let \(G\) be a group, and let \(H_1, \ldots, H_t\) be subgroups of \(G\). Then the set \(\{H_1, \ldots, H_t\}\) forms a partition of \(G\) if each non-trivial element of \(G\) belongs to exactly one subgroup \(H_i\) of \(G\). Lemma 3.2 below introduces a partition of Suzuki groups.

**Lemma 3.2.** Let \(S = \text{Sz}(q)\) with \(q = 2^{2m+1} \geq 8\), and let \(\mathbb{F} := \text{GF}(q)\). Then

\[
(a) \text{ } S \text{ possesses cyclic subgroups } U_1 \text{ and } U_2 \text{ of orders } q + \sqrt{2q} + 1 \text{ and } q - \sqrt{2q} + 1, \text{ respectively};
\]

\[
(b) \text{ if } 1 \neq u \in U_i, \text{ for } i = 1, 2, \text{ then } S(u) = U_i. \text{ Moreover, } |N_S(U_i) : U_i| = 4;
\]

\[
(c) S \text{ possesses a cyclic subgroup } V \text{ of order } q - 1 \text{ and } |N_S(V) : V| = 2;
\]

\[
(d) S \text{ possesses a 2-subgroup } W \text{ of orders } q^2 \text{ and exponent } 4 \text{ and } |S : N_S(W)| = q^2 + 1. \text{ Moreover, the elements of } W \text{ are of the form}
\]

\[
(3.1) \quad w(a, b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & a\pi & 1 & 0 \\ a^2(a\pi) + ab + b\pi & a(a\pi) + b & a & 1 \end{pmatrix},
\]

where \(a, b \in \mathbb{F}\) and \(\pi \in \text{Aut}(\mathbb{F})\) maps \(x\) to \(x^{2^m+1}\), for all \(x \in \mathbb{F}\).

\[
(e) \text{ the conjugates of } U_1, U_2, V \text{ and } W \text{ form a partition of } S.
\]

**Proof.** All parts of this result follow from Lemma 3.1 and Theorem 3.10 in [9] except for the facts that \(|N_S(V) : V| = 2\) and \(|S : N_S(W)| = q^2 + 1\) which can be found in the proof of Theorem 3.10 in [9]. \(\square\)

**Proposition 3.3.** Let \(S = \text{Sz}(q)\) with \(q = 2^{2m+1} \geq 8\). Then the set \(nse(S)\) consists of exactly one the following numbers

\[
(a) 1, (q - 1)(q^2 + 1), q(q - 1)(q^2 + 1);
\]

\[
(b) \phi(i)q^2(q \pm \sqrt{2q} + 1)(q - 1)/4, \text{ where } i > 1 \text{ divides } q \pm \sqrt{2q} + 1;
\]
(c) $\phi(i)q^2(q^2 + 1)/2$, where $i > 1$ divides $q - 1$.

Proof. Suppose that $i \in \omega(S)$ is an even number. Then by Lemma 3.1, we have that $i = 2$ or $i = 4$ and $i$ divides the order of subgroup $W$ as in Lemma 3.2(d). Then each element of $W$ is of the form $w(a,b)$ as in (3.1). Obviously,

$$w(a,b)w(c,d) = w(a + c, b + d + (a\pi)c).$$

This in particular shows that $w(0,b)$ (with $b \neq 0$) are the only elements of $W$ of order 2. Therefore, the number of involutions in $W$ is $q - 1$. Since $W$ is a part of the partition introduced in Lemma 3.2(e), the elements of order 2 of $S$ belong to exactly one of the conjugates of $W$. Thus by Lemma 3.2(d), there are $q^2 + 1$ conjugates of $W$ implying that there are exactly $m_2(S) = (q - 1)(q^2 + 1)$ involutions in $S$. It also follows from Lemma 3.2(d) that the number of elements of order 4 in $W$ is $q^2 - q$, and hence applying the partition in Lemma 3.2(e), we conclude that $S$ consists of $m_4(S) = q(q - 1)(q^2 + 1)$ elements of order 4. This proves part (a).

Suppose now $i \in \omega(S)$ is an odd number. Then, by Lemma 3.1, $i$ divides the order of one of the cyclic subgroups $U_1$, $U_2$ and $V$ as in Lemma 3.2, say $H$. Assume $i = np^k$ with $p$ odd. Since $H$ is a part of the partition introduced in Lemma 3.2(e), the elements of order $i$ are contained in $H$ and its conjugates. Since also $H$ is cyclic, there are $\phi(i)$ elements of order $i$ in each conjugates of $H$ including $H$.

Now we consider each possibility of $H$. If $H = U_t$ of order $q \pm \sqrt{2q} + 1$, for $t = 1, 2$, then by Lemma 3.2(b), $|N_S(U_t) : U_t| = 4$, and so $|S : N_S(U_t)| = |S|/4|U_t|$, for $t = 1, 2$. So there are $|S|/4|U_t|$ conjugates of $U_t$ implying that there are exactly $m_i(S) = \phi(i)q^2(q - 1)(q \pm \sqrt{2q} + 1)/4$ elements of order $i$ in $S$. This follows part (b). If $H = V$, then Lemma 3.2(c) implies that $|N_S(V) : V| = 2$, and so the same argument as in the previous cases, we conclude that $m_i(S) = \phi(i)|S|/2|V| = \phi(i)q^2(q^2 + 1)/2$. This follows (c). \qed

4. Proof of the Main Theorem

In this section, we prove Theorem 1.1. From now on, set $S := Sz(q)$, where $q = 2^{2m+1} \geq 8$, and recall that $G$ is a finite group with $nse(G) = nse(S)$ and $|G| = |S|$. Therefore, by Proposition 3.3, $nse(S)$ consists of

$$m_1(S) = 1;$$
$$m_2(S) = (q - 1)(q^2 + 1);$$
$$m_4(S) = q(q - 1)(q^2 + 1);$$

(4.1)
$$m_i(S) = \phi(i)q^2(q \pm \sqrt{2q} + 1)(q - 1)/4, \text{ where } i > 1 \text{ divides } q \pm \sqrt{2q} + 1;$$
$$m_i(S) = \phi(i)q^2(q^2 + 1)/2, \text{ where } i > 1 \text{ divides } q - 1.$$

Proposition 4.1. The vertex 2 is an isolated vertex in $\Gamma(G)$.

Proof. Assume the contrary. Then there is an odd prime divisor $p$ of $|G|$ such that $2p \in \omega(G)$. Let $f(n)$ be the number of elements of $G$ whose orders are multiples of $n$. Then by Lemma 2.3, $f(2)$ is a
multiple of the greatest divisor of $|G|$ that is prime to 2. Since $(q^2 + 1)(q - 1)$ is the greatest divisor of $|G|$ which is coprime to 2, there exists a positive integer $r$ such that $f(2) = (q^2 + 1)(q - 1)r$ and $(r, 2) = 1$. On the other hand, by Lemma 2.2, it is obvious that $m_2(G) = m_2(S)$, and so

$$f(2) = m_2(G) + \sum_{i > 2 \text{ is even}} m_i(G),$$

with $m_i$ as in (4.1). Now applying Proposition 3.3, there is a non-negative integer $\alpha$ such that

$$f(2) = (q^2 + 1)(q - 1) + \alpha q(q^2 + 1)(q - 1) + g(2),$$

where

$$g(2) = \sum_{i|q \pm \sqrt{2q} + 1 \atop i \neq 1} \beta_i \cdot m_i(S) + \sum_{i|q - 1 \atop i \neq 1} \gamma_i \cdot m_i(S)$$

for some non-negative integers $\beta_i$ and $\gamma_i$. Since $2p \in \omega(G)$, we have that $\alpha q(q^2 + 1)(q - 1) + g(2) > 0$. Then

$$g(2) = (q^2 + 1)(q - 1)(r - 1 - \alpha q).$$

We now prove that $q^2$ divides $g(2)$. It follows from Lemma 3.1 that 2 is an isolated vertex of $\Gamma(S)$. Then a Sylow 2-subgroup of $S$, say $S_2$, acts fixed point freely (by conjugation) on the set of elements of order $i \neq 1, 2, 4$ (see Proposition 3.3 and (4.1)). Thus $|S_2|$ divides $m_i(S)$ with $i \neq 1, 2, 4$. Hence $q^2$ divides $m_i(S)$ implying that $g(2)$ is a multiple of $q^2$.

We now consider the following two cases:

1. Let $g(2) \neq 0$. Then $q^2$ divides $r - 1 - \alpha q$, and so $q^2 + \alpha q + 1 \leq r$. This implies that $|G| = q^2(q^2 + 1)(q - 1) < (q^2 + 1)(q - 1)r = f(2)$, which is impossible.

2. Let $g(2) = 0$. Then $r - 1 - \alpha q = 0$ and $\alpha \neq 0$, and so $m_{2p}(G) = q(q^2 + 1)(q - 1)$. Therefore

$$f(p) = \sum_{p \mid i} m_i(G) = \alpha' q(q^2 + 1)(q - 1) + \sum_{i|q \pm \sqrt{2q} + 1 \atop i \neq 1} \beta_i' \cdot m_i(S) + \sum_{i|q - 1 \atop i \neq 1} \gamma_i' \cdot m_i(S),$$

where $\alpha'$, $\beta_i'$ and $\gamma_i'$ are non-negative integers. Since $m_{2p} = q(q^2 + 1)(q - 1)$, we have that $\alpha' > 0$. On the other hand, by Lemma 2.3, $f(p) = q(q^2 + 1)(q - 1)r'/|G_p|$ with $r'$ a positive integer. Thus

$$q^2(q^2 + 1)(q - 1)r' = \frac{|G_p|}{\alpha' q(q^2 + 1)(q - 1) + \sum_{i|q \pm \sqrt{2q} + 1 \atop i \neq 1} \beta_i' \cdot m_i(S) + \sum_{i|q - 1 \atop i \neq 1} \gamma_i' \cdot m_i(S)}.$$  

Since $q^2$ divides both $q^2(q^2 + 1)(q - 1)r'/|G_p|$ and $m_i(S)$ in (4.2), it follows that $q^2$ divides $\alpha' q(q^2 + 1)(q - 1)$. Then $q \mid \alpha'$, and so $|G| = q^2(q^2 + 1)(q - 1) \leq \alpha' q(q^2 + 1)(q - 1) \leq f(p)$, which is impossible. □

**Proposition 4.2.** The group $G$ has a normal series $1 \leq H \leq K \leq G$ such that $H$ and $G/K$ are $\pi_1$-groups and $K/H$ is a non-abelian simple group, $H$ is a nilpotent group and $|G/K|$ divides $|\text{Out}(K/H)|$. 
Proof. By Proposition 4.1, the vertex 2 is an isolated vertex in the prime graph \( \Gamma(G) \) of \( G \). This implies that the number \( t(G) \) of connected components of the prime graph \( \Gamma(G) \) is at least two. The assertion follows from [16, Theorem A] provided that \( G \) is neither a Frobenius group, nor a 2-Frobenius group.

Let \( G \) be a Frobenius group with kernel \( K \) and complement \( H \). Then by Lemma 2.4, we must have \( t(G) = 2 \), \( \pi(H) \) and \( \pi(K) \) are vertex sets of the connected components of \( \Gamma(G) \). By Proposition 4.1, the vertex 2 is an isolated vertex in \( \Gamma(G) \). Then either (i) \( |K| = q^2 \) and \( |H| = (q^2 + 1)(q - 1) \), or (ii) \( |H| = q^2 \) and \( |K| = (q^2 + 1)(q - 1) \). Both cases can be ruled out as \( |H| \) must divide \( |K| - 1 \).

Let \( G \) be a 2-Frobenius group. Then Lemma 2.5 implies that \( t(G) = 2 \) and \( G \) has a normal series \( 1 \trianglelefteq H \trianglelefteq K \trianglelefteq G \) such that \( G/H \) and \( K \) are Frobenius groups with kernel \( K/H \) and \( H \) respectively, \( \pi(G/K) \cup \pi(H) = \pi_1, \pi(K/H) = \pi_2 \) and \( |G/K| \) divides \( |\text{Aut}(K/H)| \). Since 2 is an isolated vertex of \( \Gamma(G) \) by Proposition 4.1, \( |K/H| = (q^2 + 1)(q - 1) \) and \( |G/K|, |H| = q^2 \). Since also \( K \) is a Frobenius group with kernel \( H \), there is a positive integer \( \alpha \) such that \( (q^2 + 1)(q - 1) \) divides \( 2^\alpha - 1 \), which is a contradiction. \( \square \)

4.1. Proof of Theorem 1.1.

Proof. Let \( S := \text{Sz}(q) \), where \( q = 2^{2m+1} \geq 8 \). Suppose that \( G \) is a finite group with \( nse(G) = nse(S) \) and \( |G| = |S| \). By applying Proposition 4.2, the group \( G \) has a normal series \( 1 \trianglelefteq H \trianglelefteq K \trianglelefteq G \) such that \( H \) and \( G/K \) are \( \pi_1 \)-groups and \( K/H \) is a non-abelian simple group. Since 3 is a prime divisor of all finite non-abelian simple groups except for Suzuki groups. Moreover, 3 is coprime to \( |K/H| \). Then \( K/H \cong \text{Sz}(q') \), where \( q' = 2^{2m'+1} \). This, in particular, implies that \( 2^{4m'+2} \) divides \( 2^{4m+2} \), and hence \( m' \leq m \). On the other hand, \( H \) and \( G/K \) are \( \pi_1 \)-groups. Then \( (q^2 + 1)(q - 1) \) divides \( |K/H| \), and so \( (q^2 + 1)(q - 1) \) divides \( (q^2 + 1)(q' - 1) \). Since now \( m' \leq m \), we must have \( m = m' \). Therefore \( K/H \cong S \). Now \( |G| = |K/H| = |S| \), and hence \( G \cong S \). \( \square \)

Acknowledgments

The authors are grateful to the anonymous referees and the editor for careful reading of the manuscript and for corrections and suggestions.

References


Seyed Hassan Alavi
Department of Mathematics, Faculty of Science, Bu-Ali Sina University, Hamedan, Iran
Email: alavi.s.hassan@basu.ac.ir
Email: alavi.s.hassan@gmail.com

Ashraf Daneshkhah
Department of Mathematics, Faculty of Science, Bu-Ali Sina University, Hamedan, Iran
Email: adanesh@basu.ac.ir
Email: daneshkhah.ashraf@gmail.com

Hosein Parvizi Mosaed
Alvand Institute of Higher Education, Hamedan, Iran
Email: h.parvizi.mosaed@gmail.com