Annales Mathematicae et Informaticae
***40** (2012) pp. 13–23*
http://ami.ektf.hu

A characterization of Symmetric group S_r, where r is prime number

Alireza Khalili Asboei[a], Seyed Sadegh Salehi Amiri[a]
Ali Iranmanesh[b], Abolfazl Tehranian[a]

[a]Department of Mathematics, Science and Research Branch
Islamic Azad University, Tehran, Iran
khaliliasbo@yahoo.com, salehisss@yahoo.com, tehranian1340@yahoo.com

[b]Department of Mathematics, Faculty of Mathematical Sciences
Tarbiat Modares University, Tehran, Iran
iranmanesh@modares.ac.ir

Submitted November 9, 2011 — Accepted April 11, 2012

Abstract

Let G be a finite group and $\pi_e(G)$ be the set of element orders of G. Let $k \in \pi_e(G)$ and m_k be the number of elements of order k in G. Set $\mathrm{nse}(G) := \{m_k \mid k \in \pi_e(G)\}$. In this paper, we prove the following results:

1. If G is a group such that $\mathrm{nse}(G) = \mathrm{nse}(S_r)$, where r is prime number and $|G| = |S_r|$, then $G \cong S_r$.
2. If G is a group such that $\mathrm{nse}(G) = \mathrm{nse}(S_r)$, where $r < 5 \times 10^8$ and $r - 2$ are prime numbers and r is a prime divisor of $|G|$, then $G \cong S_r$.

Keywords: Element order, set of the numbers of elements of the same order, Symmetric group

MSC: 20D06, 20D20, 20D60

1. Introduction

If n is an integer, then we denote by $\pi(n)$ the set of all prime divisors of n. Let G be a finite group. Denote by $\pi(G)$ the set of primes p such that G contains an element of order p. Also the set of element orders of G is denoted by $\pi_e(G)$. A finite group G is called a simple K_n-group, if G is a simple group with $|\pi(G)| = n$. Set $m_i = m_i(G) := |\{g \in G|$ the order of g is $i\}|$ and $\mathrm{nse}(G) := \{m_i | i \in \pi_e(G)\}$. In fact, m_i is the number of elements of order i in G and $\mathrm{nse}(G)$ is the set of sizes of elements with the same order in G. Throughout this paper, we denote by ϕ the Euler's totient function. If G is a finite group, then we denote by P_q a Sylow q-subgroup of G and by $n_q(G)$ the number of Sylow q-subgroup of G, that is, $n_q(G) = |Syl_q(G)|$. Also we say $p^k \parallel m$ if $p^k \mid m$ and $p^{k+1} \nmid m$. For a real number x, let $\varphi(x)$ denote the number of primes which are not greater than x, and $[x]$ the greatest integer not exceeding x. For positive integers n and k, let $t_n(k) = \prod_{i=1}^{k}(\prod_{n/(i+1)<p\leq n/i} p)^i$, where p is a prime. Denote by $\gcd(a, b)$ the greatest common divisor of positive integers a and b, and by $\exp_m(a)$ the exponent of a modulo m for the relatively prime integers a and m with $m > 1$. If m is a positive integer and p is a prime, let $|m|_p$ denote the p-part of m; in the other words, $|m|_p = p^k$ if $p^k \mid m$ but $p^{k+1} \nmid m$. For a finite group H, $|H|_p$ denotes the p-part of $|H|$. All further unexplained notations are standard and refer to [1], for example. In [2] and [3], it is proved that all simple K_4-groups and Mathieu groups can be uniquely determined by $\mathrm{nse}(G)$ and the order of G. In [4], it is proved that the groups A_4, A_5 and A_6 are uniquely determined only by $\mathrm{nse}(G)$. In [5], the authors show that the simple group $PSL(2, q)$ is characterizable by $\mathrm{nse}(G)$ for each prime power $4 \leq q \leq 13$. In this work it is proved that the Symmetric group S_r, where r is a prime number is characterizable by $\mathrm{nse}(G)$ and the order of G. In fact the main theorems of our paper are as follow:

Theorem 1. *Let G be a group such that nse(G)=nse(S_r), where r is a prime number and $|G| = |S_r|$. Then $G \cong S_r$.*

Theorem 2. *Let G be a group such that nse(G)=nse(S_r), where $r < 5 \times 10^8$ and $r - 2$ are prime numbers and $r \in \pi(G)$. Then $G \cong S_r$.*

In this paper, we use from [6] for proof some Lemmas, but since some part of the proof is different, we were forced to prove details get'em. We note that there are finite groups which are not characterizable by $\mathrm{nse}(G)$ and $|G|$. For example see the Remark in [2].

2. Preliminary Results

We first quote some lemmas that are used in deducing the main theorems of this paper.

Let $\alpha \in S_n$ be a permutation and let α have t_i cycles of length i, $i = 1, 2, \ldots, l$, in its cycle decomposition. The cycle structure of α is denote by $1^{t_1}2^{t_2}\ldots l^{t_l}$, where $1t_1 + 2t_2 \cdots + lt_l = n$. One can easily show that two permutations in S_n are conjugate if and only if they have the same cycle structure.

Lemma 2.1 ([6]).
(i) $\varphi(x) - \varphi(x/2) \geq 7$ for $x \geq 59$.

(ii) $\varphi(x) - \varphi(x/4) \geq 12$ *for* $x \geq 61$.
(iii) $\varphi(x) - \varphi(6x/7) \geq 1$ *for* $x \geq 37$.

Lemma 2.2 ([6]). *If* $n \geq 402$, *then* $(2/n)t_n(6) > e^{1.201n}$. *If* $n \geq 83$, *then* $(2/n)t_n(6) > e^{0.775n}$.

Lemma 2.3 ([6]). *Let p be a prime and k a positive integer.*
(i) If $|n!|_p = p^k$, *then* $(n-1)/(p-1) \geq k \geq n/(p-1) - 1 - [\log_p n]$.
(ii) If $|n!/m!|_p = p^k$ *and* $0 \leq m < n$, *then* $k \leq (n-m-1)/(p-1) + [\log_p n]$.

Lemma 2.4 ([7]). *Let* $\alpha \in S_n$ *and assume that the cycle decomposition of* α *contains* t_1 *cycles of length* 1, t_2 *cycles of length* $2, \ldots, t_l$ *cycles of length* l. *Then the order of conjugacy class of* α *in* S_n *is* $n!/1^{t_1}2^{t_2}\ldots l^{t_l}t_1!t_2!\ldots t_l!$.

Lemma 2.5 ([8]). *Let G be a finite group and m be a positive integer dividing* $|G|$. *If* $L_m(G) = \{g \in G | g^m = 1\}$, *then* $m \mid |L_m(G)|$.

Lemma 2.6 ([9]). *Let G be a finite group and* $p \in \pi(G)$ *be odd. Suppose that P is a Sylow p-subgroup of G and* $n = p^s m$, *where* $(p,m) = 1$. *If P is not cyclic and* $s > 1$, *then the number of elements of order n in G is always a multiple of* p^s.

Lemma 2.7 ([4]). *Let G be a group containing more than two elements. Let* $k \in \pi_e(G)$ *and* m_k *be the number of elements of order k in G. If* $s = \sup\{m_k | k \in \pi_e(G)\}$ *is finite, then G is finite and* $|G| \leq s(s^2-1)$.

Let m_n be the number of elements of order n. We note that $m_n = k\phi(n)$, where k is the number of cyclic subgroups of order n in G. Also we note that if $n > 2$, then $\phi(n)$ is even. If $n \in \pi_e(G)$, then by Lemma 2.2 and the above notation we have

$$\begin{cases} \phi(n) \mid m_n \\ n \mid \sum_{d|n} m_d \end{cases} \tag{2.1}$$

In the proof of the main theorem, we often apply (2.1) and the above comments.

3. Proof of the Main Theorem 1

We now prove the theorem 1 stated in the introduction. Let G be a group such that $\text{nse}(G) = \text{nse}(S_r)$, where r is a prime number and $|G| = |S_r|$. The following Lemmas reduce the problem to a study of groups with the same order with S_r.

Lemma 3.1. $m_r(G) = m_r(S_r) = (r-1)!$ *and if* $S \in Syl_r(G)$, $R \in Syl_r(S_r)$, *then* $|N_G(S)| = |N_{S_r}(R)|$.

Proof. Since $m_r(G) \in \text{nse}(G)$ and $\text{nse}(G) = \text{nse}(S_r)$, then by (2.1) there exists $k \in \pi_e(S_r)$ such that $p \mid 1 + m_k(S_r)$. We know that $m_k(S_r) = \sum |cl_{S_r}(x_i)|$ such that $|x_i| = k$. Since $r \mid 1 + m_k(S_r)$, then $(r, m_k(S_r)) = 1$. If the cyclic structure of x_i for any i is $1^{t_1}2^{t_2}\ldots l^{t_l}$ such that $t_1, t_2, \ldots, t_l$ and $1, 2, \ldots, l$ are not equal to r, then $r \mid r!/1^{t_1}2^{t_2}\cdots l^{t_l}t_1!t_2!\dots t_l!$, that is $r \mid |cl_{S_r}(x_i)|$ for any i. Therefore $(r, m_k(S_r)) \neq 1$, which is a contradiction. Thus there exist $i \in \mathbb{N}$ such that $t_i = r$ or one of the numbers $1, 2, \dots$ or l is equal to r. If there exist $i \in \mathbb{N}$ such that $t_i = r$, then the cyclic structure of x_i is 1^r. Hence $|x_i| = 1$, which is a contradiction. If one of the numbers $1, 2, \dots$ or l is equal to r, then the cyclic structure of x_i is r^1. Hence $|x_i| = r$ and $k = r$. Therefore $m_r(G) = m_r(S_r)$, since $|G| = |S_r|$, then $n_r(G) = n_r(S_r) = m_r(G)/(r-1) = (r-2)!$. Hence if $S \in Syl_r(G)$, $R \in Syl_r(S_r)$, then $|N_G(S)| = |N_{S_r}(R)| = r(r-1)$. □

Lemma 3.2. *G has a normal series $1 \leq N < H \leq G$ such that $r \mid |H/N|$ and H/N is a minimal normal subgroup of G/N.*

Proof. Suppose $1 = N_0 < N_1 < \cdots < N_m = G$ is a chief series of G. Then there exists i such that $p \mid |N_i/N_{i-1}|$. Let $H = N_i$ and $N = N_{i-1}$. Then $1 \leq N < H \leq G$ is a normal series of G, H/N is a minimal normal subgroup of G/N, and $r \mid |H/N|$. Clearly, H/N is a simple group. □

Lemma 3.3. *Let $r \geq 5$ and let $1 \leq N < H \leq G$ be a normal series of G, where H/N is a simple group and $r \mid |H/N|$. Let $R \in Syl_r(G)$ and $Q \in Syl_r(G/N)$.*
(i) $|N_{G/N}(Q)| = |N_{H/N}(Q)||G/H|$ and $|N_N(R)||N_{G/N}(Q)| = |N_G(R)| = r(r-1)$.
(ii) If $P \in Syl_p(N)$ with $|P| = p^k$, where p is a prime and $k \geq 1$, then either $|H/N| \mid \prod_{i=0}^{k-1}(p^k - p^i)$ or $p^k|N_{G/N}(Q)| \mid r(r-1)$.

Proof. (i) By Frattini's argument, $G/N = N_{G/N}(Q)(H/N)$. Thus

$$G/H \cong N_{G/N}(Q)/N_{H/N}(Q).$$

So the first equality holds. Since we have

$$N_{G/N}(Q) \cong N_G(R)N/N \cong N_G(R)/N_N(R),$$

the second equality is also true.

(ii) By Frattini's argument again, $H = N_H(P)N$. Thus, we have $H/N \cong N_H(P)/N_N(P)$. Since H/N is a simple group, $C_H(P)N_N(P) = N_H(P)$ or $N_N(P)$. If $C_H(P)N_N(P) = N_H(P)$, then $r \mid |C_H(P)|$. Without loss of generality, we may assume $R \leq C_H(P)$. It means that $N_N(R) \geq P$. Then $p^k|N_{G/N}(Q)| \mid r(r-1)$ by (i). If $C_H(P)N_N(P) = N_N(P)$, then $C_H(P) \leq N_N(P)$. Thus $|N_H(P)/N_N(P)| \mid |N_H(P)/C_H(P)|$. Since $|H/N| = |N_H(P)/N_N(P)|$ and $N_H(P)/C_H(P)$ is isomorphic to a subgroup of $Aut(P)$, $|H/N| \mid |Aut(P)|$. Since $|Aut(P)| \mid \prod_{i=0}^{k-1}(p^k - p^i)$, $|H/N| \mid \prod_{i=0}^{k-1}(p^k - p^i)$. □

Lemma 3.4. *Let $r \geq 5$ and let $1 \leq N < H \leq G$ be a normal series of G with H/N simple and $r \mid |H/N|$. If $|N|_p|G/H|_p = p^k$ with $k \geq 1$ and $|H/N|$ not dividing $\Pi_{i=0}^{k-1}(p^k - p^i)$, then $p^k \mid (r-1)$.*

Proof. Assume $|N|_p = p^k$. If $t = 0$, then $p^k \mid |G/H|$. By Lemma 3.3 (i), $p^k \mid r(r-1)$. If $t \geq 1$, since $|H/N|$ does not divide $\Pi_{i=0}^{k-1}(p^k - p^i)$ and $\prod_{i=k-t}^{k-1}(p^k - p^i) = p^{t(k-t)} \prod_{j=0}^{t-1}(p^t - p^j)$, we have that $|H/N|$ does not divide $\prod_{j=0}^{t-1}(p^t - p^j)$. By Lemma 3.3 (ii), $p^t|N_{G/N}(Q)| \mid r(r-1)$, where $Q \in Syl_r(G/N)$. By Lemma 3.3 (i), $|N_{G/N}(Q)| = |N_{H/N}(Q)||G/H|$, so we have $p^t|G/H| \mid r(r-1)$. Since $|N|_p|G/H|_p = p^k$ and $|N|_p = p^k$, we obtain $|G/H|_p = p^{k-t}$. Thus $p^k \mid r(r-1)$. Since $r \mid |H/N|$, it is easy to know $p \neq r$. Therefore, $p^k \mid (r-1)$. $\square$

Lemma 3.5. *Let $r \geq 5$ and let $1 \leq N < H \leq G$ be a normal series of G with H/N simple. If $r \mid |H/N|$, then $t_r(1) \mid |H/N|$ and H/N is a non-ablian simple group and G is not solvable group.*

Proof. We first prove that $t_r(1) \mid |H/N|$. If $t_r(1) \nmid |H/N|$, then there exists a prime p satisfying $r/2 < p < r$ such that $p \mid |N||G/H|$. Since $r \mid |H/N|$, $|H/N| \nmid (p-1)$. Hence $p \mid (r-1)$ by Lemma 3.4. But $(r-1)/2 < r/2$, contrary to $r/2 < p$. Since the number of prime factors of $t_r(1)$ is greater that 1, then H/N is a non-ablian simple group. Clearly G is not solvable group. $\square$

Lemma 3.6. *If $r \geq 59$ and let $1 \leq N < H \leq G$ be a normal series of G with H/N simple and $r \mid |H/N|$,*
(i) If $\gcd(t_r(6), r-1) = 1$, then $t_r(6) \mid |H/N|$.
(ii) If $\gcd(t_r(6), r-1)$ is a prime p, then $(t_r(6)/p) \mid |H/N|$.

Proof. By Lemma 3.5, $t_r(1) \mid |H/N|$. Suppose $t_r(6) \nmid |H/N|$. There exists a prime q with $r/7 < q \leq r/2$ such that $q \mid |N||G/H|$. Let $|N|_q|G/H|_q = q^k$. If $|H/N| \mid \prod_{i=0}^{k-1}(q^k - q^i)$ with $1 \leq k \leq 6$, then $t_r(1) \mid \prod_{i=1}^{k}(q^i - 1)$. By Lemma 2.1, the number of prime factors of $t_r(1)$ is greater than 6. But the number of primes p with $p \mid \prod_{i=1}^{6}(q^i - 1)$ and $r/2 < p$ is less than or equal to 6, a contradiction. By Lemma 3.4, $q^k \mid (r-1)$. If $\gcd(t_r(6), r-1) = 1$, then $k = 0$, contrary to $q \mid |N||G/H|$. Hence, (i) is true. If $\gcd(t_r(6), r-1) = p$, then $k = 1$ and $q = p$. It follows that $(t_r(6)/p) \mid |H/N|$. This proves (ii). $\square$

Lemma 3.7. *Let $r \geq 5$. If $1 \leq N < H \leq G$ is a normal series of G, $t_r(1) \mid |H/N|$, and H/N is a non-abelian simple group, then $H/N \cong A_r$.*

Proof. We consider the following cases:

Case 1. $r = 5$. In this case, we have $|H/N| = 2^a 3 \cdot 5$ with $a \leq 3$. It is clear that $H/N \cong A_5$.

Case 2. $r = 7$. In this case, we have $|H/N| = 2^a 3^b 5 \cdot 7$ with $a \leq 4$ and $b \leq 2$. It is clear that $H/N \cong A_7$.

Case 3. $11 \leq r \leq 19$. Note that $|G| < 10^{25}$ for $11 \leq r \leq 19$. If H/N is not isomorphic to any alternating group, since $t_r(1) \mid |H/N|$, by [1, pp. 239–241], H/N is isomorphic to one of the following groups:

M_{22} (for $r = 11$),	$L_2(q)$ of order $\geq 10^6$,	$G_2(q)$ of order $\geq 10^{20}$,
Suz (for $r = 13$),	$L_3(q)$ of order $\geq 10^{12}$,	
HS (for $r = 11$),	$U_3(q)$ of order $\geq 10^{12}$,	
McL (for $r = 11$),	$L_4(q)$ of order $\geq 10^{16}$,	
Fi_{22} (for $r = 13$),	$U_4(q)$ of order $\geq 10^{16}$,	
$U_6(2)$ (for $r = 11$),	$S_4(q)$ of order $\geq 10^{16}$,	

If H/N is isomorphic to one of the six groups on the left side, by $|H/N| \mid |G|$, we have $H/N \cong M_{22}$ and $r = 11$. So $|N|_3|G/H|_3 = 3$ by $|S_r|_3/|M_{22}|_3 = 3$. Since $|M_{22}| \nmid (3^2 - 3)(3^2 - 1)$, we have $3 \mid 10$ by Lemma 3.4, a contradiction. Suppose H/N is isomorphic to a simple group of Lie type in characteristic p. Let $|H/N|_p = p^t$. If H/N is isomorphic to $L_4(q)$, $U_4(q)$, $S_4(q)$, or $G_2(q)$ of order $\geq 10^{16}$, then $p^t \geq 10^6$ by Lemma 4 in [10]. When $p \geq 3$, by Lemma 2.3, $10^6 \leq p^t \leq p^{(r-1)/(p-1)} \leq 3^{(r-1)/2} < 3^{11}$, a contradiction. When $p = 2$, since $2^{19} \nmid |G|$, we have $10^6 \leq p^t \leq 2^{18}$, a contradiction. If $H/N \cong U_3(q)$ $(q = p^k)$, then $p \neq 11$ by $p^{3k} \mid |U_3(q)|$ and $11^3 \nmid |G|$. Thus $11 \mid p^{2k} - 1$ or $11 \mid p^{3k} + 1$. Since $11 \nmid p^2 - 1$, we have $\exp_{11}(p) = 5$ or 10. Therefore, $5 \mid k$. Thus $p^{3k} + 1$ has a prime factor ≥ 31 (see Lemma 2 in [11]), contrary to $r \leq 19$. Similarly, we derive a contradiction if $H/N \cong L_2(q)$ or $L_3(q)$.

Case 4. $23 \leq r \leq 43$. Since $t_r(1) \mid |H/N|$, it is easy to prove that H/N is not isomorphic to any sporadic simple group. If H/N is isomorphic to a simple group of Lie type in characteristic 23, we have $H/N \cong L_2(23)$ or $L_2(23^2)$. If $H/N \cong L_2(23)$, we have $r = 23$, since $29 \nmid |L_2(23)|$. But $19 \nmid |L_2(23)|$, contrary to $t_r(1) \mid |H/N|$. If $H/N \cong L_2(23^2)$, then $r = 43$. But $43 \nmid |L_2(23^2)|$, again contrary to $r \mid |H/N|$. If $H/N \cong^3 D_4(p^k)$ with $p \neq 23$, then $23 \mid p^{8k} + p^{4k} + 1$ or $23 \mid p^{6k} - 1$. Moreover, $23 \mid p^{12k} - 1$. We have $\exp_{23}(p) = 11$ or 22 since $23 \nmid p^2 - 1$. Thus, $11 \mid k$. Then $p^{132} \mid |^3D_4(p^k)|$, contrary to $p^{132} \nmid |G|$. If H/N is isomorphic to a simple group of Lie type in characteristic p except $^3D_4(p^k)$ with $p \neq 23$, let $|H/N|_p = p^s$. By examining the orders of simple groups of Lie type, we know that there exists a positive integer $t \leq s$ such that $23 \mid p^t + 1$ and $(p^t + 1) \mid |H/N|$, or $23 \mid p^t - 1$ and $(p^t - 1) \mid |H/N|$. As above, we can prove $11 \mid t$. Thus, $s \geq t \geq 11$. Since $p^{11} \nmid |G|$ for $r \leq 43$ and $p \geq 5$, we have $p = 2$ or 3. Since 2 and 3 are not primitive roots, we have $(2^{11} - 1) \mid |H/N|$ or $(3^{11} - 1) \mid |H/N|$. But $2^{11} - 1$ and $3^{11} - 1$ have a prime factor > 43, contrary to $r \leq 43$.

Case 5. $47 \leq r \leq 79$. In this case, $47 \mid |H/N|$. It can be proved that H/N is isomorphic to an alternating group as above.

Case 6. $r \geq 83$. Clearly, H/N is not isomorphic to any sporadic simple group for $r \geq 83$. If H/N is isomorphic to a simple group of Lie type in characteristic p and $|H/N|_p = p^t$, then $|H/N| < p^{3t}$ by Lemma 4 in [10]. In particular, if H/N is not isomorphic to $L_2(p^t)$, then $|H/N| < p^{8t/3}$. We first prove $p \leq r/7$. If $r/2 < p \leq r$, then we have $H/N \cong L_2(p)$. Since $|L_2(p)| = p(p^2 - 1)/2$, the number of prime factors of $t_r(1)$ is not greater than 2, contrary to Lemma 2.1. If $r/(s+1) < p \leq r/s$ with $s = 2$ or 3, then $t_r(1) < |H/N|/p^t < p^{2t} \leq p^{2s} \leq p^6 \leq (r/2)^6$. But $t_r(1) > (r/2)^7$ by Lemma 2.1, a contradiction. If $r/(s+1) < p \leq r/s$ with $4 \leq s \leq 6$, by Lemma 3.6, we have $(2/r)t_r(3) < |H/N|/p^t < p^{2t} \leq p^{2s} \leq p^{12} \leq (r/4)^{12}$. By

Lemma 2.1, we have $(2/r)t_r(3) > (2/r)(r/4)^{12}t_{[r/2]}(1) > (r/4)^{12}$, a contradiction. Now we prove that $p \leq r/7$ is impossible.

(i) If $r \geq 409$ and $p \geq 3$, by Lemmas 2.2, 2.3, and 3.6, we have $e^{1.201r} < (2/r)t_r(6) < |H/N|/p^t < p^{2t} \leq p^{2(r-1)/(p-1)} < (p^{2/(p-1)})^r \leq 3^r$. But $e^{1.201} > 3$, a contradiction.

(ii) For the case where $r \geq 409$ and $p = 2$, if H/N is not isomorphic to $L_2(2^t)$, we have $e^{1.201r} < (2/r)t_r(6) < |H/N|/2^t < 2^{5t/3} < 2^{5r/3}$. But $e^{1.201} > 2^{5/3}$, a contradiction.

Suppose $H/N \cong L_2(2^t)$. Since $(2^{2t}-1) \mid |L_2(2^t)|$ and $2^{2t}-1$ has a prime factor q satisfying $\exp_q(2) = 2t$ (see Lemma 2 in [11]), we have $2t+1 \leq q \leq r$. Hence, $e^{1.201r} < (r/2)t_r(6) \leq 2^{2t} - 1 < 2^r$, a contradiction.

(iii) If $83 \leq r \leq 401$ and $p \geq 7$, we can deduce $e^{0.775r} < 7^{r/3}$ as above, a contradiction.

(iv) If $83 \leq r \leq 401$ and $p \leq 5$, we have $83 \mid |H/N|$ by Lemma 3.6. Similar to the argument used in the case where $23 \leq r \leq 43$, we can deduce $p^{41} - 1 \mid |H/N|$ or $p^{41} + 1 \mid |H/N|$. But $p^{41} - 1$ and $p^{41} + 1$ have a prime factor > 401 for $p \leq 5$, contrary to $r \leq 401$.

We have proved that $H/N \cong A_r$. Now set $\overline{H} := H/N \cong A_r$ and $\overline{G} := G/N$. On the other hand, we have:

$$A_r \cong \overline{H} \cong \overline{H}C_{\overline{G}}(\overline{H})/C_{\overline{G}}(\overline{H}) \leq \overline{G}/C_{\overline{G}}(\overline{H}) = N_{\overline{G}}(\overline{H})/C_{\overline{G}}(\overline{H}) \leq Aut(\overline{H}).$$

Let $K = \{x \in G \mid xN \in C_{\overline{G}}(\overline{H})\}$, then $G/K \cong \overline{G}/C_{\overline{G}}(\overline{H})$. Hence $A_r \leq G/K \leq Aut(A_r)$, and hence $G/K \cong A_r$ or $G/K \cong S_r$. If $G/K \cong A_r$, then $|K| = 2$. We have $N \leq K$, and N is a maximal solvable normal subgroup of G, then $N = K$. Hence $H/N \cong A_r = G/N$, then $|N| = 2$. So G has a normal subgroup N of order 2, generated by a central involution z. Therefore G has an element of order $2r$. Now we prove that G does not any element of order $2r$, a contradiction. At first we show that $r \parallel m_2(S_r) = m_2(G)$. We have $m_2(S_r) = \sum |cl_{S_r}(x_k)|$ such that $|x_k| = 2$. Since $2 \neq 1, r$, the cyclic structure of x_k for any k is $1^{t_1}2^{t_2}\ldots l^{t_l}$, where $t_1, t_2, \ldots, t_l, 1, 2, \ldots, l$ are not equal to r. On the other hand, we have $|cl_{S_r}(x_k)| = r!/1^{t_1}2^{t_2}\ldots l^{t_l}t_1!t_2!\ldots t_l!$. Hence $m_2(S_r) = r!h$, where h is a real number. Since $m_2(S_r) \lneqq r!$, then $0 < h < 1$. Therefore $r \parallel m_2(S_r)$. We know that if P and Q are Sylow r-subgroups of G, then they are conjugate, which implies that $C_G(P)$ and $C_G(Q)$ are conjugate. Since $2r \in \pi_e(G)$, we have $m_{2r}(G) = \phi(2r)n_r(G)k = (r-1)!k$, where k is the number of cyclic subgroups of order 2 in $C_G(P_r)$. Hence $m_r(G) \mid m_{2r}(G)$. On the other hand, $2r \mid (1 + m_2(G) + m_r(G) + m_{2r}(G))$, by (2.1). Since $r \mid (1 + m_r(G))$ and $r \mid m_2(G)$, then $r \mid m_{2r}(G)$. Therefore by $(r-1)! \mid m_{2r}(G)$ and $r \mid m_{2r}(G)$, we can conclude that $r! \mid m_{2r}(G)$, a contradiction. Hence G/K is not isomorphic to A_r, and hence $G/K \cong S_r$, then $|K| = 1$ and $G \cong S_r$. Thus the proof is completed. □

Corollary 3.8. *Let G be a finite group. If $|G| = |S_r|$, where r is a prime number and $|N_G(R)| = |N_{S_r}(S)|$, where $R \in Syl_r(G)$ and $S \in Syl_r(S_r)$, then $G \cong S_r$.*

Proof. It follows at once from Theorem 1. □

Corollary 3.9. *Let G be a finite group. If $|N_G(P_1)| = |N_{S_r}(P_2)|$ for every prime p, where $P_1 \in Syl_p(G)$, $P_2 \in Syl_p(S_r)$ and r is a prime number, then $G \cong S_r$.*

Proof. Since $|N_G(P_1)| = |N_{S_r}(P_2)|$ for every prime p, where $P_1 \in Syl_p(G)$, $P_2 \in Syl_p(S_r)$, we have $|P_1| = |P_2|$. Thus, $|G|_p = |S_r|_p$ for every prime p. Hence, $|G| = |S_r|$. It follows that $G \cong S_r$. □

4. Proof of the Main Theorem 2

We now prove the theorem 2 stated in the Introduction. Let G be a group such that $\mathrm{nse}(G) = \mathrm{nse}(S_r)$, where $r < 5 \times 10^8$ and $r - 2$ are prime numbers and $r \in \pi(G)$. By Lemma 2.7, we can assume that G is finite. The following lemmas reduce the problem to a study of groups with the same order with S_r.

Lemma 4.1. *If $i \in \pi_e(S_r)$, $i \neq 1$ and $i \neq r$, then $r \parallel m_i(S_r)$.*

Proof. We have $m_i(S_r) = \sum |cl_{S_r}(x_k)|$ such that $|x_k| = i$. Since $i \neq 1, r$, the cyclic structure of x_k for any k is $1^{t_1}2^{t_2} \ldots l^{t_l}$, where $t_1, t_2, \ldots, t_l, 1, 2, \ldots, l$ are not equal to r. On the other hand, we have $|cl_{S_r}(x_k)| = r!/1^{t_1}2^{t_2} \ldots l^{t_l}t_1!t_2! \ldots t_l!$. Hence $m_i(S_r) = r!h$, where h is a real number. Since $m_i(S_r) \lneqq r!$, then $0 < h < 1$. Therefore $r \parallel m_i(S_r)$. □

Lemma 4.2. $|P_r| = r$.

Proof. At first we prove that if $r = 5$, then $|P_5| = 5$. We know that, $\mathrm{nse}(G) = \mathrm{nse}(S_5) = \{1, 20, 24, 25, 30\}$. We show that $\pi(G) \subseteq \{2, 3, 5\}$. Since $25 \in \mathrm{nse}(G)$, it follows from (2.1) that $2 \in \pi(G)$ and $m_2 = 25$. Let $2 \neq p \in \pi(G)$. By (2.1), we have $p \in \{3, 5, 31\}$. If $p = 31$, then by (2.1), $m_{31} = 30$. On the other hand, if $62 \in \pi_e(G)$, then by (2.1), we conclude that $m_{62} = 30$ and $62|86$, which is a contradiction. Therefore $62 \notin \pi_e(G)$. So P_{31} acts fixed point freely on the set of elements of order 2, and $|P_{31}| \mid m_2$, which is a contradiction. Thus $\pi(G) \subseteq \{2, 3, 5\}$. It is easy to show that, $m_5 = 24$, by (2.1). Also if $3 \in \pi_e(G)$, then $m_3 = 20$. By (2.1), we conclude that G does not contain any element of order 15, 20 and 25. Also, we get $m_4 = 30$ and $m_8 = 24$ and G does not contain any element of order 16. Since $2, 5 \in \pi(G)$, hence we have $\pi(G) = \{2, 5\}$ or $\{2, 3, 5\}$. Suppose that $\pi(G) = \{2, 5\}$. Then $\pi_e(G) \subseteq \{1, 2, 4, 5, 8, 10\}$. Therefore $|G| = 100 + 20k_1 + 24k_2 + 30k_3 = 2^m \times 5^n$, where $0 \leq k_1 + k_2 + k_3 \leq 1$. Hence $5 \mid k_2$, which implies that $k_2 = 0$, and so $50 + 10k_1 + 15k_3 = 2^{m-1} \times 5^n$. Hence $2 \mid k_3$, which implies that $k_3 = 0$. It is easy to check that the only solution of the equation is $(k_1, k_2, k_3, m, n) = (0, 0, 0, 2, 2)$. Thus $|G| = 2^2 \times 5^2$. It is clear that $\pi_e(G) = \{1, 2, 4, 5, 10\}$, hence $\exp(P_2) = 4$, and P_2 is cyclic. Therefore $n_2 = m_4/\phi(4) = 30/2 = 15$, since every Sylow 2-subgroup has one element of order 2, then $m_2 \leq 15$, which is a contradiction. Hence $\pi(G) = \{2, 3, 5\}$. Since G has no element of order 15, the group P_5 acts fixed point freely on the set of elements of order 3. Therefore $|P_5|$ is a divisor of $m_3 = 20$, which implies that $|P_5| = 5$. Now suppose that $r \neq 5$, by Lemma 4.1, we have $r^2 \nmid m_i(G)$, for any $i \in \pi_e(G)$. On the other hand, if $r^3 \in \pi_e(G)$, then by (2.1) we have $\phi(r^3) \mid m_{r^3}(G)$. Thus $r^2 \mid m_{r^3}(G)$, which is a contradiction. Therefore $r^3 \notin \pi_e(G)$. Hence $\exp(P_r) = r$ or $\exp(P_r) = r^2$. We claim that $\exp(P_r) = r$. Suppose that $\exp(P_r) = r^2$. Hence there exists an element of order r^2 in G such that $\phi(r^2) \mid m_{r^2}(G)$. Thus $r(r-1) \mid m_{r^2}(G)$. And so $m_{r^2}(G) = r(r-1)t$, where $r \nmid t$. If $|P_r| = r^2$, then P_r will be a cyclic group and we have $n_r(G) = m_{r^2}(G)/\phi(r^2) = r(r-1)t/r(r-1) = t$. Since $m_r(G) = (r-1)!$, then $(r-1)! = (r-1)n_r(G) = (r-1)t$. Therefore $t = (r-2)!$ and $m_{r^2}(G) = r(r-1)(r-2)! = r!$, which is a contradiction. If $|P_r| = r^s$, where $s \geq 3$, then by Lemma 2.6, we have $m_{r^2}(G) = r^2 l$ for some natural number l, which is a contradiction by Lemma 4.1. Thus $\exp(P_r) = r$. By Lemma 2.5, $|P_r| \mid (1 + m_r(G)) = 1 + (r-1)!$. By [12], $|P_r| = r$. □

Lemma 4.3. $\pi(G) = \pi(S_r)$.

Proof. By Lemma 4.2, we have $|P_r| = r$. Hence $(r-2)! = m_r(G)/\phi(r) = n_r(G) \mid |G|$. Thus $\pi((r-2)!) \subseteq \pi(G)$. Now we show that $\pi(S_r) = \pi(G)$. Let p be a prime number such that $p > r$. Suppose that $pr \in \pi_e(G)$. We have $m_{pr}(G) = \phi(pr)n_r(G)k$, where k is the number of cyclic subgroups of order p in $C_G(P_r)$. Hence $(p-1)(r-1)! \mid m_{pr}$. On the other hand, since p is prime and $p > r$, then $p-1 > r$. Thus $(p-1)(r-1)! > r!$, then $m_{pr} > r!$, which is a contradiction. Thus $pr \notin \pi_e(G)$. Then P_p acts fixed point freely on the set of elements of order r, and so $|P_p| \mid (r-1)!$, which is a contradiction. Therefore $p \notin \pi(G)$. By the assumption $r \in \pi(G)$, hence $\pi(G) = \pi(S_r)$. □

Lemma 4.4. *G has not any element of order $2r$.*

Proof. Suppose that G has an element of order $2r$. We have

$$m_{2r}(G) = \phi(2r)n_r(G)k = (r-1)!k,$$

where k is the number of cyclic subgroups of order 2 in $C_G(P_r)$. Hence $m_r(G) \mid m_{2r}(G)$. On the other hand, $2r \mid (1 + m_2(G) + m_r(G) + m_{2r}(G))$, by (2.1). Since $r \mid (1 + m_r(G))$ and $r \mid m_2(G)$ by Lemma 4.1, $r \mid m_{2r}(G)$. Therefore by $(r-1)! \mid m_{2r}(G)$ and $r \mid m_{2r}(G)$, we can conclude that $r! \mid m_{2r}(G)$, a contradiction. □

Lemma 4.5. *G has not any element of order $3r, 5r, 7r, \ldots, pr$, where p is the prime number such that $p < r$.*

Proof. The proof of this lemma is completely similar to Lemma 4.4. □

Lemma 4.6. *If $p = r-2$, then $|P_p| = p$ and $n_p(G) = r!/2p(p-1)$.*

Proof. Since $pr \notin \pi_e(G)$, then the group P_p acts fixed point freely on the set of elements of order r, and so $|P_p| \mid m_r(G) = (r-1)!$. Thus $|P_p| = p$. Since Sylow p-subgroups are cyclic, then $n_p(G) = m_p(G)/\phi(p) = r!/2p(p-1)$. □

Lemma 4.7. $|G| = |S_r|$.

Proof. We can suppose that $|S_r| = 2^{k_2}3^{k_3}5^{k_5}\cdots l^{k_l}pr$, where $k_2, k_3, k_5, \ldots, k_l$ are non-negative integers. By Lemma 4.4, the group P_2 acts fixed point freely on the set of elements of order r, and so $|P_2| \mid m_r(G) = (r-1)!$. Thus $|P_2| \mid 2^{k_2}$. Similarly by Lemma 4.5, we have $|P_3| \mid 3^{k_3}, \ldots, |P_l| \mid l^{k_l}$. Therefore $|G| \mid |S_r|$. On the other hand, we know that $(r-2)! = m_r(G)/\phi(r) = n_r(G)$ and $n_r(G) \mid |G|$ and $n_p(G) = r!/2p(p-1) \mid |G|$, then the least common multiple of $(r-2)!$ and $r!/2p(p-1)$ divide the order of G. Therefore $r!/2 \mid |G|$ and so $|G| = |A_r|$ or $|G| = |S_r|$. If $|G| = |A_r|$, by $m_r(S_r) = m_r(A_r) = (r-1)!$, then $|N_G(R)| = |N_{A_r}(S)|$, where $R \in Syl_r(G)$ and $S \in Syl_r(A_r)$, similarly to main Theorem 1, $G \cong A_r$. But we can prove that $\mathrm{nse}(G) \neq \mathrm{nse}(A_r)$. Suppose that $\mathrm{nse}(G) = \mathrm{nse}(A_r)$, since $\mathrm{nse}(G) = \mathrm{nse}(S_r)$, then $m_2(S_r) = m_2(A_r)$. On the other hand $m_2(S_r) = \sum |cl_{S_r}(x_i)|$ such that $|x_i| = 2$, since cyclic structure $1^{r-2}2$ no exists in A_r, then it is clear that $m_2(S_r) > m_2(A_r)$, a contradiction. Hence $|G| = |S_r|$. $\square$

Now by the main Theorem 1, $G \cong S_r$, and the proof is completed.

Acknowledgment. The authors would like to thank from the referees for the valuable comments.

References

[1] Conway, J. H., Curtis, R. T., Norton, S. P., et al., Atlas of Finite Groups. *Clarendon, Oxford*, 1985.

[2] Shao, C. G., Shi, W., Jiang, Q. H., Characterization of simple K_4-groups. *Front Math, China.* **3**(2008), 355–370.

[3] Shao, C. G., Jiang, Q. H., A new characterization of Mathieu groups. *Archivum Math, (Brno) Tomus.* **46**(2010), 13–23.

[4] Shen, R., Shao, C. G., Jiang, Q. H., Shi, W., Mazuro, V., A New Characterization of A_5. *Monatsh Math.* **160** (2010), 337–341.

[5] Khatami, M., Khosravi, B., Akhlaghi, Z., A new characterization for some linear groups. *Monatsh Math.* **163**(2009), 39–50.

[6] Bi, J., Characteristic of Alternating Groups by Orders of Normalizers of Sylow Subgroups. *Algebra Colloq.* **8**(2001), 249–256.

[7] Zassenhaus, H., The theory of groups. 2nd ed, *Chelsea Publishing Company New York*, 1958.

[8] Frobenius, G., Verallgemeinerung des sylowschen satze. *Berliner sitz.* (1895), 981–993.

[9] Miller, G., Addition to a theorem due to Frobenius. *Bull. Am. Math. Soc.* **11**(1904), 6–7.

[10] Bi, J., A characterization of the symmetric groups. *Acta Math. Sinica.* **33**(1990), 70–77. (in Chinease)

[11] Bi, J., A characterization of $L_n(q)$ by the normalizers' orders of their Sylow subgroups. *Acta Math. Sinica* (New Ser). **11**(1995), 300–306.

[12] Crandal, R., Dilcher, K., Pomerance, C., A search for Wieferich and Wilson primes. *Matematics of Computation.* **66**(1997), 433–449.