Quasigroups and Related Systems 27 (2019), 15 − 24

NSE characterization of some Suzuki groups

Azam Babai and Maryam Khatami

Abstract. Let G be a group, and $\pi_e(G)$ be the set of element orders of G. For $k \in \pi_e(G)$, the number of elements of G of order k is denoted by $m_k(G)$. Set $nse(G) = \{m_k(G) \mid k \in \pi_e(G)\}$. Let $q = 2^{2n+1}$, and $p = q - 1$ be a Mersenne prime. In this paper, we show that if G is a group such that $nse(G) = nse(Sz(q))$ and $p \in \pi_e(G)$ but $p^2 \notin \pi_e(G)$, then $G \cong Sz(q)$ or $G \cong Sz(q) \rtimes \mathbb{Z}_{2n+1}$.

1. Introduction

Let G be a group. Denote by $\pi_e(G)$, the set of orders of elements of G. Let $k \in \pi_e(G)$, and $m_k(G)$ be the number of elements of order k in G. Put $nse(G) = \{m_k(G) \mid k \in \pi_e(G)\}$, the set of number of elements of the same order in G. For each finite group G, and each positive integer t, let $M_t(G) = \{g \in G \mid g^t = 1\}$. The finite groups G and H are called of the same order type if $|M_t(G)| = |M_t(H)|$, for $t = 1, 2, \ldots$ The most important problem related to the set $nse(G)$ is Thompson's problem:

Thompson's Problem. *Suppose that G and H are finite groups of the same order type. If G is solvable, is it true that H is necessarily solvable?*

Nobody has been solved this problem completely until now. Obviously, if G and H are groups of the same order type, then $|G| = |H|$ and $nse(G) = nse(H)$. So, if a group G is characterizable by its order and $nse(G)$, then G satisfies Thompson's problem. Note that, in 1987 Thompson gave an example, which shows that not all groups G are characterizable by $|G|$ and $nse(G)$. In [7], it was proved that if G is a finite group and M is a simple K_4-group, then $G \cong M$ if and only if $|G| = |M|$ and $nse(G) = nse(M)$ (A simple K_n-group is a simple group G such that $|G|$ has n distinct prime divisors).

Let G be a finite group, and $\pi(G)$ be the set of prime divisors of $|G|$. The prime graph of a group G, which is denoted by $\Gamma(G)$, is a graph with vertex set $\pi(G)$, and two distinct vertices p and q are adjacent if and only if $pq \in \pi_e(G)$. Let $t(G)$ be the number of connected components of $\Gamma(G)$, and $\pi_1(G), \ldots, \pi_{t(G)}(G)$ be the set of vertices of the connected components of $\Gamma(G)$. If there is no ambiguity, we use the notation π_i instead of $\pi_i(G)$. If $2 \in \pi(G)$, we always assume that $2 \in \pi_1$, and π_1 is called the *even component* of $\Gamma(G)$ and $\pi_2, \ldots, \pi_{t(G)}$ are called the *odd*

2010 Mathematics Subject Classification: 20D06, 20D60, 20D15.
Keywords: Suzuki groups, set of number of elements of the same order, prime graph.

components of $\Gamma(G)$. Note that $|G|$ can be expressed as a product of coprime integers k_i, for $i = 1, \ldots, t(G)$, such that $\pi(k_i) = \pi_i$. We call $k_1, \ldots, k_{t(G)}$ the order components of G.

In [5], it is proved that the simple group $Sz(2^{2n+1})$, where $2^{2n+1} - 1$ is a prime number, is uniquely determined by $nse(Sz(2^{2n+1}))$ and $|Sz(2^{2n+1})|$.

In this paper, we improve their result and show that if G is a group such that $nse(G) = nse(Sz(q))$, where $q = 2^{2n+1}$, and $p = q - 1$ is a prime, and $p \in \pi_e(G)$ and $p^2 \notin \pi_e(G)$, then $G \cong Sz(q)$ or $G \cong Sz(q) \rtimes \mathbb{Z}_{2n+1}$. To prove the theorem, we show that the prime graph of the group G is disconnected, and then by using William's theorem and the classification of finite simple groups we get the result.

Let n be an integer, by $\pi(n)$ we mean the set of prime divisors of n. Note that $\pi(G) = \pi(|G|)$. For every $r \in \pi(G)$, denote by P_r, a Sylow r-subgroup of G, and by $n_r(G)$, the number of Sylow r-subgroups of G. Also, the Euler's totient function is denoted by $\phi(n)$, which is the number of positive integers less that n that are relatively prime to n.

2. Main results

The following preliminary results are needed to prove our main theorem:

Theorem 2.1. (cf. [8]) *Let G be a group containing more that two elements. If the maximal number s of elements of the same order in G is finite, then G is finite and $|G| \leqslant s(s^2 - 1)$.*

Theorem 2.2. (cf. [4]) *Let G be a finite group and t be a positive integer dividing $|G|$. Then $t \mid |M_t(G)|$.*

It is easy to obtain the following corollary:

Corollary 2.3. *Let G be a finite group. Then the following hold:*

(1) *For every divisor n of $|G|$, $n \mid \sum_{d|n} m_d(G)$.*

(2) *For every $n \in \pi_e(G)$, $m_n(G) = k\phi(n)$ where k is the number of cyclic subgroups of order n.*

Theorem 2.4. (cf. [2]) *Let G be a Frobenius group of even order with kernel K and complement H. Then $t(G) = 2$, and the prime graph components of G are $\pi(K)$ and $\pi(H)$, and the following hold:*

(i) *K is nilpotent;*

(ii) $|K| \equiv 1 \pmod{|H|}$.

A finite group G is called 2-*Frobenius*, if it has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$, such that K is a Frobenius group with kernel H, and G/H is a Frobenius group with kernel K/H.

Theorem 2.5. (cf. [2]) *Let G be a 2-Frobenius group with normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$, such that K and G/H are Frobenius groups with kernels H, and K/H, respectively. Then*

(*i*) $t(G) = 2$, $\pi_1 = \pi(G/K) \cup \pi(H)$ *and* $\pi_2 = \pi(K/H)$;

(*ii*) G/K *and* K/H *are cyclic,* $|G/K|$ *is a divisor of* $(|K/H| - 1)$ *and* $G/K \leqslant Aut(K/H)$.

Theorem 2.6. (cf. [10]) *Let G be a finite group with $t(G) \geqslant 2$. Then G has one of the following structures:*

(*i*) *G is a Frobenius or 2-Frobenius group.*

(*ii*) *G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that $\pi(H) \cup \pi(G/K) \subseteq \pi_1$ and K/H is a nonabelian simple group. In particular, H is nilpotent, $G/K \leqslant Out(K/H)$, and the odd order components of G are the odd order components of K/H.*

Theorem 2.7. (cf. [3]) *The equation $p^m - q^n = 1$, where p and q are primes and $m, n > 1$ has only one solution, namely $3^2 - 2^3 = 1$.*

Theorem 2.8. (Zsigmondy Theorem) (cf. [11]) *Let p be a prime and n be a positive integer. Then one of the following holds:*

(*i*) *There is a primitive prime p' for $p^n - 1$, that is, $p' \mid (p^n - 1)$ but $p' \nmid (p^m - 1)$, for every $1 \leqslant m < n$,*

(*ii*) $p = 2$, $n = 1$ *or* 6,

(*iii*) *p is a Mersenne prime and $n = 2$.*

Remark 2.9. Let k and n be coprime integers. If there is an integer x such that $x^2 \equiv k \pmod n$, then k is called a *quadratic residue modulo* n, otherwise k is called a *quadratic nonresidue* modulo n. For a prime p, the symbol (a/p) is defined as follows: $(a/p) = 1$ if a is a quadratic residue modulo p, $(a/p) = -1$ if a is a quadratic nonresidue modulo p, and $(a/p) = 0$ if $p \mid a$. It is a well known result that $(-1/p) = (-1)^{(p-1)/2}$.

Let p be a prime and a be an integer such that $(a,p) = 1$. The smallest positive integer $k \geqslant 1$ such that $a^k \equiv 1 \pmod p$ is called the order of a with respect to p, and is denoted by $ord_p(a)$. Obviously, if $a^n \equiv 1 \pmod p$, then $ord_p(a) \mid n$.

In [9], Suzuki showed that $Sz(q)$ has a partition as follows:

(1) $q^2 + 1$ Sylow 2-subgroups of order q^2 and exponent 4.

(2) $q^2(q^2 + 1)/2$ cyclic subgroups of order $q - 1$.

(3) $\frac{q^2(q-1)(q+\sqrt{2q}+1)}{4}$ cyclic subgroups of order $q - \sqrt{2q} + 1$.

(4) $\frac{q^2(q-1)(q-\sqrt{2q}+1)}{4}$ cyclic subgroups of order $q + \sqrt{2q} + 1$.

So, it is easy to see that $nse(Sz(q)) = \{(q-1)(q^2+1), q(q-1)(q^2+1), \phi(r)q^2(q^2+1)/2, \phi(s)q^2(q-1)(q+\sqrt{2q}+1)/4, \phi(t)q^2(q-1)(q-\sqrt{2q}+1)/4\}$, where $r > 1$ is a divisor of $q-1$, $s > 1$ is a divisor of $q - \sqrt{2q} + 1$ and $t > 1$ is a divisor of $q + \sqrt{2q} + 1$.

Theorem 2.10. *Let G be a group such that $nse(G) = nse(Sz(q))$, where $q = 2^{2n+1}$ and $p = q-1$ is a prime. If $p \in \pi_e(G)$ and $p^2 \notin \pi_e(G)$, then $G \cong Sz(q)$ or $G \cong Sz(q) \rtimes \mathbb{Z}_{2n+1}$.*

Proof. It is obvious by Theorem 2.1 that G is a finite group. By Corollary 2.3, $m_2(G)$ is the only odd number in $nse(G)$, so $m_2(G) = (q-1)(q^2+1)$. Note that $p \mid 1+m_p(G)$, so $m_p(G) = \phi(r)q^2(q^2+1)/2$, where $r > 1$ is a divisor of $q-1 = p$. Therefore $m_p(G) = q^2(q^2+1)(q-2)/2$.

Let P be a Sylow p-subgroup of G. By assumption we have $exp(P) = p$. We claim that $|P| = p$.

Let $|P| = p^b$, for some $b \geqslant 2$. So, $|P| \mid 1+m_p(G)$, which implies that $(q-1)^b$ is a divisor of

$$q^5 - 2q^4 + q^3 - 2q^2 + 2 = (q-1)(q^4 - q^3 - 2q - 2).$$

Then we have $q-1$ is a divisor of $q^4 - q^3 - 2q - 2 = (q-1)(q^3-2) - 4$, and consequently $q-1 \mid 4$, which is impossible. So $b = 1$, and P is a cyclic group of order p, as we claimed. Hence it is easy to see that $m_p(G) = n_p(G)(p-1)$, where $n_p(G)$ is the number of Sylow p-subgroups of G. Therefore $n_p(G) = q^2(q^2+1)/2$.

• Step 1. $t(G) \geqslant 2$.

We claim that for every $t \in \pi(G)$ distinct from p, $tp \notin \pi_e(G)$. Let $t \in \pi(G) \setminus \{p\}$ such that G has an element of order tp. Therefore

$$m_{tp}(G) = \phi(tp)n_p(G)k = n_p(G)(p-1)(t-1)k = m_p(G)(t-1)k,$$

where k is the number of cyclic subgroups of order t in $C_G(P)$. By considering $nse(G)$, the only possibility for $m_{tp}(G)$ is $q^2(q^2+1)(q-2)/2$. So, $m_{tp}(G) = m_p(G)$, and $(t-1)k = 1$, which implies that $t = 2$. Therefore $2p \mid (1 + m_2(G) + m_p(G) + m_{2p}(G))$, which implies that $p \mid m_{2p}(G) = m_p(G)$, a contradiction. So our claim is proved, and p is an isolated vertex in $\Gamma(G)$. Therefore $t(G) \geqslant 2$, as required.

• Step 2. $q^2(q^2+1)(q-1)/2 \mid |G|$ and $|G| \mid q^2(q^2+1)(q-1)(q-2)/2$.

Since $n_p(G) = q^2(q^2+1)/2 \mid |G|$, and $p = q-1 \in \pi(G)$, it is obvious that $q^2(q^2+1)(q-1)/2 \mid |G|$.

Let $r \in \pi(G)$ be distinct from p, and R be a Sylow r-subgroup of G. Since $rp \notin \pi_e(G)$, it follows that R acts fixed point freely on the set of elements of order p in G. Therefore, $|R| \mid m_p(G) = q^2(q^2+1)(q-2)/2$. Therefore, $|G| \mid q^2(q^2+1)(q-1)(q-2)/2$, and so the result follows.

• Step 3. G is neither a Frobenius group nor a 2-Frobenius group.

Let G be a Frobenius group with kernel K and complement H. By Theorem 2.4, we have the prime graph components of G are $\pi(K)$ and $\pi(H)$. Note that $\pi(q(q^2+1)) \subseteq \pi_1(G)$ and $\pi_2(G) = \{p\}$. By the fact that $|H|$ is a divisor of $|K|-1$, we have $|H| < |K|$. On the other hand $|G| = |H||K|$, so by Step 2 we conclude that $|H| = p = q-1$, and $q^2(q^2+1)/2 \mid |K|$. Take $r \in \pi(q - \sqrt{2q} + 1)$. Suppose that R is a Sylow r-subgroup of K. Since K is nilpotent, it follows that R is a normal subgroup of G, and $R \rtimes H$ is a Frobenius group. So we conclude that $|H| = q-1 \mid |R|-1$. Therefore $q-1 \leqslant |R|-1 \leqslant q - \sqrt{2q}$, which is impossible.

Let G be a 2-Frobenius group, with normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$, such that K and G/H are Frobenius groups with Frobenius kernels H and K/H, respectively. So, $\pi(q(q^2+1)) \subseteq \pi_1(G) = \pi(G/K) \cup \pi(H)$, and $\pi_2(G) = \{p\} = \pi(K/H)$. Also, $|G/K|$ is a divisor of $|K/H| - 1 = p - 1 = q - 2$. Let $r \in \pi(q^2+1)$. If $r \in \pi(G/K)$, then r is a divisor of $|G/K|$, and consequently a divisor of $q-2$. So $r \mid q^2 - 4$, which implies that $r \mid 5$. Therefore $\pi(q^2+1) \setminus \{5\} \subseteq \pi(H)$. By Theorem 2.7, it is easy to see that $\pi(q^2+1) \neq \{5\}$. Therefore, there exists $r \in \pi(q^2+1) \setminus \{5\}$, and so $r \in \pi(H)$.

If $\pi(q^2+1) \neq \{5, r\}$, then there exists $s \in \pi(q^2+1) \cap \pi(H)$, such that $s < q$. Let S be a Sylow s-subgroup of H. Since H is nilpotent, it follows that S is a normal subgroup of K. Note that S is a cyclic subgroup, and so it has a unique subgroup S_1 of order s. Therefore $S_1 \trianglelefteq K$. Let P be a Sylow p-subgroup of K. So $S_1 \rtimes P$ is a Frobenius group, which implies that $p \mid s-1$. So $p = q-1 \leqslant s-1$, which is a contradiction.

Now let $\pi(q^2+1) = \{5, r\}$. Since $q^2+1 = (q+\sqrt{2q}+1)(q-\sqrt{2q}+1)$ and $q \pm \sqrt{2q}+1 > 1$ and $(q-\sqrt{2q}+1, q+\sqrt{2q}+1) = 1$, it follows that $\pi(q+\sqrt{2q}+1) = \{5\}$, or $\pi(q-\sqrt{2q}+1) = \{5\}$.

First suppose that $\pi(q+\sqrt{2q}+1) = \{5\}$. So $2^{n+1}(2^n+1) = 5^a - 1$, for some integer a.

If a is even, then $2^{n+1}(2^n+1) = (5^{a/2}-1)(5^{a/2}+1)$. Since $(5^{a/2}-1, 5^{a/2}+1) = 2$, it follows that $2^n \mid 5^{a/2}-1$, or $2^n \mid 5^{a/2}+1$. If $2^n \mid 5^{a/2}-1$, then $5^{a/2}-1 = 2^n B$, and $2(2^n+1) = (5^{a/2}+1)B$, for some odd integer B. If $B \geqslant 3$, then $5^{a/2}-1 > 2^{n+1}$ and $2^n+1 > 5^{a/2}+1$, therefore $2^n > 5^{a/2} > 2^{n+1}+1$, a contradiction. So $B = 1$, and $5^{a/2} = 2^n+1 = 2^{n+1}+1$, which is impossible. If $2^n \mid 5^{a/2}+1$, then $5^{a/2}+1 = 2^n B$, and $2(2^n+1) = (5^{a/2}-1)B$, for some odd integer B. If $B \geqslant 3$, then $5^{a/2}+1 > 2^{n+1}$, and $2^n+1 > 5^{a/2}-1$, hence $2^n+2 > 5^{a/2} > 2^{n+1}-1$. Therefore $n = 1$, and the equation $2^{n+1}(2^n+1) = 5^a - 1$ does not have any solution. Now let $B = 1$, so $5^{a/2} = 2^n - 1 = 2^{n+1}+3$, which is impossible.

If a is odd, then $2^{n+1}(2^n+1) = 4(1+5+\ldots+5^{a-1})$. Then $2^{n+1} = 4$, therefore $n = 1$, which is impossible as we said above.

Now suppose that $\pi(q-\sqrt{2q}+1) = \{5\}$. So $2^{n+1}(2^n-1) = 5^a - 1$, for some integer a.

Let a be even. Therefore $2^{n+1}(2^n-1) = (5^{a/2}-1)(5^{a/2}+1)$, which implies that either $2^n \mid 5^{a/2}-1$, or $2^n \mid 5^{a/2}+1$. Let $2^n \mid 5^{a/2}-1$. So $5^{a/2}-1 = 2^n B$, and $2(2^n-1) = (5^{a/2}+1)B$, for some odd integer B. If $B \geqslant 3$, then $2^n - 2 > 5^{a/2} > 2^{n+1}+1$, which is a contradiction. So $B = 1$, and hence $5^{a/2} = 2^n+1 = 2^{n+1}-3$, which implies that $n = 2$. Therefore, $nse(G) = nse(Sz(32))$ and by the main theorem of [6], $G \cong Sz(32)$, which is not a 2-Frobenius group, a contradiction. Now let $2^n \mid 5^{a/2}+1$. So $5^{a/2}+1 = 2^n B$, and $2(2^n-1) = (5^{a/2}-1)B$, for some odd integer B. If $B \geqslant 3$, then $2^n > 5^{a/2} > 2^{n+1}-1$, which is impossible. So $B = 1$, and $5^{a/2} = 2^n - 1 = 2^{n+1}-1$, a contradiction.

So we may assume that a is odd. Hence $2^{n+1}(2^n-1) = 4(1+5+\ldots+5^{a-1})$, implies that $2^{n+1} = 4$. Therefore $n = 1$, and $q = 8$. So $|G/K| \mid 6$, which implies that $\pi(q^2+1) = \{5, 13\} \subseteq \pi(H)$, so there exists $s \in \pi(q^2+1) \cap \pi(H)$, such that

$s < q$ and by a similar argument as above we get a contradiction.

• STEP 4. G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that $\pi(H) \cup \pi(G/K) \subseteq \pi_1$, and K/H is a Suzuki simple group.

Since $t(G) \geqslant 2$, and G is not a Frobenius and 2-Frobenius group, Theorem 2.6 implies that G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that $\pi(H) \cup \pi(G/K) \subseteq \pi_1$, and K/H is a nonabelian simple group, and the odd order components of G are the odd order components of K/H. In particular $t(K/H) \geqslant 2$. Now by the classification of finite simple groups and the results in Tables 1-3 in [1], we show that K/H is isomorphic to a Suzuki simple group:

(i) K/H is not isomorphic to a sporadic simple group, or ${}^2A_3(2)$, ${}^2F_4(2)'$, ${}^2A_5(2)$, $E_7(2)$, $E_7(3)$, $A_2(4)$ and ${}^2E_6(2)$.

If K/H is isomorphic to one of the mentioned groups, it is obvious that one of the odd order components of that group must be the Mersenne prime p. But in every case it is easy to get a contradiction by the fact that $|K/H|$ is a divisor of $|G|$. For example, let $K/H \cong J_4$, then $p = 2^{2n+1} - 1 = 31$, which implies that $n = 2$ and $q = 32$. But $|J_4| \nmid q^2(q^2+1)(q-1)(q-2)/2$, which is a contradiction by Step 2.

(ii) K/H is not isomorphic to alternating groups.

Let $K/H \cong A_{p'}$, where $p' > 6$ and $p'-2$ are primes. Then either $p' = 2^{2n+1}-1$ or $p'-2 = 2^{2n+1}-1$. First let $p' = 2^{2n+1}-1$. So since $p'-2$ is an odd order component of K/H, we have $q-3 = 2^{2n+1}-3$ is a divisor of $q^2(q^2+1)(q-2)/2$. It is obvious that $(q-3, q^2(q-2)/2) = 1$, so $q-3 \mid q^2+1$, which implies that $q-3 \mid 10$. The only possibility is $q = 8$ and $p' = 7$, but $|A_7| \nmid q^2(q^2+1)(q-1)(q-2)/2$, a contradiciton.

Now let $p'-2 = 2^{2n+1}-1$. Therefore $p' = q+1$ which is an odd order component of K/H divides $q^2(q^2+1)(q-2)/2$. By the fact that $(q+1, q^2(q^2+1)/2) = 1$, it follows that $q+1 \mid q-2$, a contradiction.

By a similar argument one can get that K/H can not be isomorphic to A_m, such that $6 < m = p', p'+1, p'+2$ where p' is a prime and not both m and $m-2$ are primes.

(iii) K/H is not isomorphic to simple groups of Lie type except Suzuki groups.

CASE 1. Let $K/H \cong A_{p'-1}(q')$, where p' is an odd prime, and $(p', q') \neq (3,2), (3,4)$. Therefore $\frac{q'^{p'}-1}{(q'-1)(p',q'-1)} = p = q-1$. It is easy to see that

$$q - 1 \leqslant 1 + \ldots + q'^{p'-2} + q'^{p'-1} < 2q'^{p'-1} - 1.$$

So $q < 2q'^{p'-1}$, and consequently $q^2+1 \leqslant 4q'^{2(p'-1)}$. Therefore, $|G| \leqslant q^2(q^2+1)(q-1)(q-2)/2 < 32q'^{6(p'-1)}$. On the other hand,

$$|K/H| = \frac{q'^{\frac{1}{2}p'(p'-1)}}{(p', q'-1)}(q'^2-1)\cdots(q'^{p'}-1) > \frac{q'^{\frac{1}{2}p'(p'-1)}}{(p', q'-1)}q'\cdots q'^{p'-1} = \frac{q'^{p'(p'-1)}}{(p', q'-1)}.$$

By the fact $|K/H| \leqslant |G|$, we have $\frac{q'^{p'(p'-1)}}{(p',q'-1)} < 32q'^{6(p'-1)}$, and so $q'^{p'(p'-1)} < q'^{6p'}$, since $(p', q'-1) < q'$ and $32 \leqslant q'^5$. Therefore $p'(p'-1) < 6p'$, which implies that $p' \in \{3, 5\}$.

First let $p' = 3$. Then $\frac{q'^2+q'+1}{(3,q'-1)} = p$. If $3 \mid q'-1$, then $q'(q'+1) = 3p-1 = 3.2^{2n+1} - 4$ is a divisor of $q^2(q^2+1)(q-2)/2$. It is easy to see that $(3.2^{2n+1} - 4, (q-2)/2) = 1$, so $3.2^{2n+1} - 4 \mid q^2(q^2+1)$. Suppose that $(3.2^{2n+1} - 4, q^2+1) = d$. So d is a divisor of $9.2^{4n+2} - 16$, and $9.2^{4n+2} + 9$, which implies that $d \mid 25$. Also $(3.2^{2n+1} - 4)/d$ is a divisor of q^2, and hence $(3.2^{2n+1} - 4)/d \mid 4$. The only possibility is $n = 1$, $q = 7$ and $q' = 4$. But $|A_2(4)| \nmid q^2(q^2+1)(q-1)(q-2)/2$, a contradiction. If $3 \nmid q'-1$, then $q'(q'+1) = p-1 = 2(2^{2n}-1)$. Since $q' \neq 2$, it follows that q' is odd and consequently $q' \mid 2^n - 1$ or $q' \mid 2^n + 1$. If $q' \mid 2^n - 1$, then $2^n - 1 = q'B$ and $q'+1 = 2(2^n+1)B$, for some integer B. Therefore $2^{n+1} + 1 \leqslant q' \leqslant 2^n - 1$, which is impossible. If $q' \mid 2^n + 1$, then $2^n + 1 = q'B$ and $q'+1 = 2(2^n-1)B$, for some integer B. Therefore $2^{n+1} - 3 \leqslant q' \leqslant 2^n + 1$, and so $2^n \leqslant 4$, which implies that $n = 1$ or 2. If $n = 1$, then $q' = 2$ which is impossible by assumption. If $n = 2$, then $q = 32$ and $q' = 5$. Since $41 \in \pi(G) \setminus \pi(K/H)$, it follows that $41 \in \pi(H) \cup \pi(G/K)$. If $41 \in \pi(H)$, then take R a Sylow 41-subgroup of H, and P a Sylow 31-subgroup of K. Since $R \trianglelefteq K$, P acts fixed point freely on R, and so $R \rtimes P$ is a Frobenius group, and consequently, $|P| = 31 \mid |R| - 1 = 40$, a contradiction. So $41 \in \pi(G/K)$, which is a contradiction since $G/K \leqslant Out(K/H)$.

Now let $p' = 5$. Then $\frac{q'^5-1}{(q'-1)(5,q'-1)} = p$. If $5 \mid q'-1$, then $q'(q'+1)(q'^2+1) = 5.2^{2n+1} - 6$ is a divisor of $q^2(q^2+1)(q-2)/2$. It is easy to see that $(5.2^{2n+1} - 6, (q-2)/2) = 1$, therefore $5.2^{2n+1} - 6 \mid q^2(q^2+1)$. Put $d = (5.2^{2n+1} - 6, q^2+1)$. So d is a divisor of $25.2^{4n+2} - 36$ and $25.2^{4n+2} + 25$. Therefore $d \mid 61$, and $(5.2^{2n+1} - 6)/d \mid q^2$, which implies that $(5.2^{2n+1} - 6)/d = 1$ or 2, that both of them are impossible. If $5 \nmid q'-1$, then $q'(q'+1)(q'^2+1) = p-1 = 2(2^{2n}-1)$. If q' is even, then $q' = 2$, and $q = 32$. But $|A_4(2)| \nmid q^2(q^2+1)(q-1)(q-2)/2$, a contradiction. So q' is odd and $q'+1$ and q'^2+1 are even, which implies that $4 \mid q'(q'+1)(q'^2+1) = 2(2^{2n}-1)$, a contradiction.

If K/H is isomorphic to $A_{p'}(q')$, where p' is an odd prime and $(q'-1) \mid (p'+1)$, or ${}^2A_{p'-1}(q')$, for an odd prime p', or ${}^2A_{p'}(q')$, where p' is an odd prime, $(q'+1) \mid (p'+1)$ and $(p', q') \neq (3,3), (5,2)$, then by a similar argument one can get a contradiction.

Case 2. Let $K/H \cong A_1(q')$, where $2 < q' \equiv \epsilon \pmod 4$ and $\epsilon = \pm 1$. Then either $(q'+\epsilon)/2 = p$, or $q' = p$.

First let $(q'+\epsilon)/2 = p = 2^{2n+1} - 1$. If $\epsilon = -1$, then $q' - 1 = 2^{2n+2} - 2$, and so $q' = 2^{2n+2} - 1$ is a divisor of $(q^2+1)(q-2)/2$. Put $d = (2^{2n+2} - 1, q^2+1)$. It is easy to see that $d \mid 5$ and so $(2^{2n+2} - 1)/d \mid (q-2)/2$. Therefore $(2^{2n+2} - 1)/d$ is a divisor of $2^{2n+2} - 1$ and $2^{2n+2} - 4$, which implies that $(2^{2n+2} - 1)/d = 1$ or 3. Therefore $n = 1$ and $q' = 15$, which is impossible. If $\epsilon = 1$, then $q' + 1 = 2^{2n+2} - 2$. Therefore $q' = 2^{2n+2} - 3$ is a divisor of $(q^2+1)(q-2)/2$. It is easy to see that $(2^{2n+2} - 3, (q-2)/2) = 1$, and so $2^{2n+2} - 3 \mid q^2 + 1$. Therefore $2^{2n+2} - 3$ is a divisor of $2^{4n+4} - 9$ and $2^{4n+4} + 4$, which implies that $2^{2n+2} - 3 \mid 13$. Therefore $n = 1$. Since $nse(Sz(8)) = \{455, 3640, 5824, 6720, 12480\}$, by the fact $p \mid 1 + m_p(G)$, it is easy to see that $3 \notin \pi(G)$. Therefore this case is impossible.

Now let $q' = p = 2^{2n+1} - 1$ be a Mersenne prime. Therefore $|K/H| = q(q-1)(q-2)/2$. There exists $r \in \pi(q - \sqrt{2q} + 1)$ such that $r \notin \pi(K/H)$. Therefore $r \in \pi(H)$ or $r \in \pi(G/K)$. If $r \in \pi(H)$, then take R a Sylow r-subgroup of H and P a Sylow p-subgroup of K. Obviously, $R \rtimes P$ is a Frobenius group and so $|P|$ is a divisor of $|R| - 1$. Therefore $|P| = q - 1 \leqslant |R| - 1 \leqslant q - \sqrt{2q}$, a contradiction. So $r \in \pi(G/K)$, which is a contradiction since $G/K \leqslant Out(A_1(p))$.

Case 3. Let K/H be isomorphic to $A_1(q')$, where $q' > 2$ is even. Then either $q' + 1 = p$ or $q' - 1 = p$. If $q' + 1 = p = 2^{2n+1} - 1$, then $2^{2n+1} - q' = 2$, which is impossible since $4 \mid 2^{2n+1} - q'$. If $q' - 1 = p = 2^{2n+1} - 1$, then $q' + 1 = 2^{2n+1} + 1$ is a divisor of $q^2(q^2+1)(q-1)(q-2)/2$, which is impossible.

Case 4. Let $K/H \cong C_m(q')$, where $m = 2^l \geqslant 2$. Therefore $(q'^m + 1)/(2, q' - 1) = p$, which implies that $q'^m \equiv -1 \pmod p$, and hence $(-1/p) = 1$. So $p \equiv 1 \pmod 4$, a contradiction.

If K/H is isomorphic to $B_m(q')$, for odd q' and $m = 2^l \geqslant 4$, ${}^2D_m(q')$, for $m = 2^l \geqslant 4$, ${}^2D_m(2)$, for $m = 2^l + 1 \geqslant 5$, ${}^2D_m(3)$, for $m = 2^l + 1 \geqslant 9$ which is not a prime number, we can get a contradiction by a similar argument.

Case 5. Let K/H be isomorphic to $D_{p'}(q')$, where $p' \geqslant 5$ is a prime and $q' = 2, 3, 5$. Note that $k_2 = (q'^{p'} - 1)/(q' - 1)$. If $q' = 2$, then $2^{p'} - 1 = 2^{2n+1} - 1$, and hence $p' = 2n+1$. Therefore $2^{p'-1}+1 = 2^{2n}+1$ is a divisor of $q^2(q^2+1)(q-2)/2$. Since $2^{2n} + 1$ and $q^2/2$ are relatively prime we have $2^{2n} + 1 \mid (q^2+1)(q-2)$. Let $d = (2^{2n}+1, q^2+1)$. Therefore $d \mid 2^{2(2n+1)}+1$ and $d \mid 4(2^{4n}-1)$, which implies that $d \mid 5$. Obviously $(2^{2n}+1)/d$ is a divisor of $q-2 = 2(2^{2n}-1)$, and so $(2^{2n}+1)/d = 1$. Therefore $n = 1$, and $p' = 3$, which is a contradiction by assumption. Let $q' = 3$. Then $(3^{p'}-1)/2 = 2^{2n+1}-1$, and hence $2^{2n+2} - 3^{p'} = 1$, and we get a contradiction by Theorem 2.7. Now let $q' = 5$, and $(5^{p'}-1)/4 = 2^{2n+1}-1$. Therefore $5^{p'-1}+1 = 2(2^{2n+2}+1)/5$ is a divisor of $q^2(q^2+1)(q-2)/2$. So $(2^{2n+2}+1)/5 \mid (q^2+1)(q-2)$. It is easy to see that $d = ((2^{2n+2}+1)/5, q^2+1) \mid 5$. Hence $(2^{2n+2}+1)/5d \mid q-2$, which implies that $(2^{2n+2}+1)/5d \mid 5$. So this case is also impossible.

In the cases that K/H is isomorphic to $B_{p'}(3)$, for odd prime p', $C_{p'}(q')$, where p' is an odd prime and $q' = 2, 3$, or $D_{p'+1}(q')$, where p' is an odd prime and $q' = 2, 3$, we get a contradiction similarly.

Case 6. Let $K/H \cong {}^2D_{p'}(3)$, where $p' = 2^m + 1$. Then $(3^{p'-1}+1)/2 = p$ or $(3^{p'}+1)/4 = p$. If $(3^{p'-1}+1)/2 = p$, then $3^{p'-1} \equiv -1 \pmod p$, and hence $(-1/p) = 1$. Therfore $p \equiv 1 \pmod 4$, a contradiction. Now let $(3^{p'}+1)/4 = p = 2^{2n+1} - 1$. Therefore $3^{p'-1} + 1 = 2(2^{2n+2} - 1)/3$ is a divisor of $q^2(q^2+1)(q-2)/2$. So $(2^{2n+2}-1)/3 \mid (q^2+1)(q-2)$. It is easy to see that $d = ((2^{2n+2}-1)/3, q^2+1) \mid 5$. Therefore $(2^{2n+2}-1)/3d$ is a divisor of $q - 2 = 2^{2n+1} - 2$. Consequently, $(2^{2n+2} - 1)/3d \mid 3$. Thus $n = 1$, $q = 8$ and $p' = 3$. But $|{}^2D_3(3)| \nmid q^2(q^2+1)(q-1)(q-2)/2$, which is a contradiction.

If K/H is isomorphic to ${}^2D_{p'}(3)$, for prime $5 \leqslant p' \neq 2^m+1$, then the argument is similar.

Case 7. Let $K/H \cong F_4(q')$, where q' is even. Then $k_2 = q'^4 + 1$ and $k_3 =$

$q'^4-q'^2+1$. If $q'^4+1=2^{2n+1}-1$, then $q'^4-2^{2n+1}=-2$, which is impossible since the left side is divisible by 4. If $q'^4-q'^2+1=2^{2n+1}-1$, then $q'^2(q'^2-1)=2(2^{2n}-1)$. Again, the left side is divisible by 4, but the right side is not, a contradiction.

In cases that K/H is isomorphic to $F_4(q')$, for odd q', ${}^2F_4(q')$, for $q'=2^{2m+1}>2$, or ${}^3D_4(q')$, in a similar way we can get a contradiction.

Case 8. Let $K/H\cong E_6(q')$. Then $(q'^6+q'^3+1)/(3,q'-1)=2^{2n+1}-1$. First let $3\nmid q'-1$. Therefore $q'^3(q'^3+1)=2(2^{2n}-1)$. Obviously, q' is odd, and so $q'^3\mid 2^{2n}-1$. Since $(2^n-1,2^n+1)=1$, it follows that $q'^3\mid 2^n-1$ or $q'^3\mid 2^n+1$. If $q'^3\mid 2^n-1$, then $2^n-1=q'^3B$, and $q'^3+1=2(2^n+1)B$, for some integer B. So, $2^n+1<q'^3+1\leqslant 2^n$, a contradiction. If $q'^3\mid 2^n+1$, then $2^n+1=q'^3B$ and $q'^3+1=2(2^n-1)B$. Therefore, $2(2^n-1)\leqslant q'^3+1\leqslant 2^n+2$, and so $n=1$ or 2, which both of them are impossible by equation $q'^3(q'^3+1)=2(2^{2n}-1)$. Now let $3\mid q'-1$. So $q'^3(q'^3+1)=3.2^{2n+1}-4=4(3.2^{2n-1}-1)$. Since $q'^3(q'^3+1)$ divides $|K/H|$, it follows that $3.2^{2n-1}-1$ is a divisor of $(q^2+1)(q-2)$. Let $d=(3.2^{2n-1}-1,q^2+1)$. It is easy to see that $d\mid 25$, and consequently $(3.2^{2n-1}-1)/d\mid q-2=2^{2n+1}-2$. So $(3.2^{2n-1}-1)/d=1$, which implies that $n=1$, and $q'^3(q'^3+1)=20$, which is impossible.

If K/H is isomorphic to ${}^2E_6(q')$, for $q'>2$, then the result follows similarly.

Case 9. Let K/H be isomorphic to $G_2(q')$, where $q'>2$ and $q'\equiv\epsilon \pmod 3$, for $\epsilon=\pm1$. Then $q'^2-\epsilon q'+1=2^{2n+1}-1$, and so $q'(q'-\epsilon)=2(2^{2n}-1)$. Obviously q' is odd and $q'\mid 2^n-1$ or $q'\mid 2^n+1$. If $q'\mid 2^n-1$, then $2^n-1=q'B$ and $q'-\epsilon=2(2^n+1)B$ for some integer B. Therefore, $2^n+1<q'-\epsilon\leqslant q'+1\leqslant 2^n$, which is impossible. If $q'\mid 2^n+1$, then $2^n+1=q'B$ and $q'-\epsilon=2(2^n-1)B$, for some integer B. So $2(2^n-1)\leqslant q'-\epsilon\leqslant q'+1\leqslant 2^n+2$, which implies that $n=1$ or 2. If $n=1$, then $q'=3$, which is impossible by assumption. If $n=2$, then $q=32$ and $q'=5$, which is impossible since $|G_2(5)|\nmid q^2(q^2+1)(q-1)(q-2)/2$.

In cases $K/H\cong G_2(q')$, where $3\mid q'$, and $K/H\cong {}^2G_2(q')$, where $q'=3^{2m+1}>3$, one can get a contradiction by a similar argument.

Case 10. Let $K/H\cong E_8(q')$. Then $p\in\{q'^8+q'^7-q'^5-q'^4-q'^3+q'+1, q'^8-q'^7+q'^5-q'^4+q'^3-q'+1, q'^8-q'^6+q'^4-q'^2+1, q'^8-q'^4+1\}$. Therefore $p=q-1<(q'-1)(q'^8+q'^7+q'^6+q'^5+q'^4+q'^3+q'^2+q'+1)=q'^9-1$, which implies that $q<q'^9$. But $q'^{120}\mid |E_8(q')|$, and consequently $q'^{120}\mid q^2(q^2+1)(q-1)(q-2)/2$, which is impossible.

• Step 5. $G\cong Sz(q)$ or $Sz(q)\rtimes\mathbb{Z}_{2n+1}$.

By the previous step, G has a normal series $1\trianglelefteq H\trianglelefteq K\trianglelefteq G$ such that $\pi(H)\cup\pi(G/K)\subseteq\pi_1$, and $K/H\cong Sz(2^{2m+1})$, for some integer $m\geqslant 1$. If $m>n$, then there exists a primitive prime r of $2^{4(2m+1)}-1$ such that $r\in\pi(K/H)$ but $r\notin\pi(G)$, since $|G|\mid q^2(q^2+1)(q-1)(q-2)/2$. So we have $m\leqslant n$. Let $m<n$. By Step 1, $\{p\}$ is an odd component of $\Gamma(G)$, therefore $p=q-1\in\pi(K/H)=\pi(2^{4(2m+1)}(2^{2(2m+1)}+1)(2^{2m+1}-1))$. On the other hand, p is a primitive prime of $2^{2n+1}-1$. Therefore $p\mid 2^{2(2m+1)}+1$, which implies that $2^{4(2m+1)}\equiv 1 \pmod p$, therefore $ord_p(2)=2n+1\mid 4(2m+1)$. So $2n+1\mid 2m+1$, and hence $n\leqslant m$, a contradiction. Therefore $n=m$, and $K/H\cong Sz(q)$. Since $|K/H|=|Sz(q)|$ is a divisor of $|G|$ and $|G|\mid q^2(q^2+1)(q-1)(q-2)/2$, it follows

that $|H||G/K| \mid (q-2)/2$. We claim that $H = 1$. Otherwise, let $r \in \pi(H)$. Take R, a Sylow r-subgroup of H and P, a Sylow p-subgroup of K. By Step 1, it is easy to see that $R \rtimes P$ is a Frobenius group and hence $|P|$ is a divisor of $|R|-1$. Therefore $|P| = q-1 \leqslant |R|-1 \leqslant (q-2)/2-1$, a contradiction. So, $H = 1$ and $K \cong Sz(q)$. Since $G/K \leqslant Out(K/H) = \mathbb{Z}_{2n+1}$ and $2n+1$ is a prime, it follows that $G \cong Sz(q)$, or $G \cong Sz(q) \rtimes \mathbb{Z}_{2n+1}$. □

At the end we put forward the following questions:

Question 1. *Is it possible to omit the assumption $p^2 \notin \pi_e(G)$ in Theorem 2.10?*

Question 2. *If $q-1$ is not prime, what can be said about characterization of $Sz(q)$ by the set nse?*

References

[1] **Z. Akhlaghi, B. Khosravi, M. Khatami**, *Characterization by prime graph of $PGL(2,p^k)$ where p and $k>1$ are odd*, Int. J. Algebra Comput. **20** (2010), no. 7, 847 − 873.

[2] **G.Y. Chen**, *On the structure of Frobenius and 2-Frobenius groups*, J. Southwest China Normal Univ. **20** (1995), no. 5, 485 − 487.

[3] **P. Crescenzo**, *A diophantine equation which arises in the theory of finite groups*, Adv. Math. **17** (1975), no. 1, 25 − 29.

[4] **G. Frobenius**, *Verallgemeinerung des Sylowschen Satze*, Berliner Sitz. (1985), 981−993.

[5] **A. Iranmanesh, H. Parvizi Mosaed, A Tehranian**, *Characterization of Suzuki group by nse and order of group*, Bull. Korean Math. Soc. **53** (2016), no. 3, 651−656.

[6] **H. Parvizi Mosaedi, A. Iranmanesh, A. Taherian**, *A characterization of the small Suzuki groups by the number of the same element order*, J. Sciences **26** (2015), no. 2, 171 − 177.

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

[8] **R. Shen, C. Shao, Q. Jiang, W. Shi, V. Mazurov**, *A new characterization of A_5*, Monatsh. Math. **160** (2010), no. 3, 337 − 341.

[9] **M. Suzuki**, *A new type of simple groups of finite order*, Proc. Nat. Acad. Sci. USA **46** (1960), 868 − 870.

[10] **J. S. Williams**, *Prime graph components of finite groups*, J. Algebra **69** (1981), no. 2, 487 − 513.

[11] **K. Zsigmondy**, *Zur theorie der potenzreste*, Monatsh. Math. Phys. **3** (1892), 265 − 284.

Received 18 June, 2018

A. Babai
Department of Mathematics, University of Qom, Qom , Iran.
e-mail: a_babai@aut.ac.ir

M. Khatami
Department of Mathematics, University of Isfahan, Isfahan, Iran.
e-mail: m.khatami@sci.ui.ac.ir