RECOGNIZING CHEVALLEY GROUPS $G_2(q)$ BY nse

Shitian Liu

School of Science
Sichuan University of Science and Engineering
Zigong Sichuan, 643000
China
e-mail: liust@suse.edu.cn

Zhanghua Zhang

Sichuan Water Conservancy Vocational College
Chongzhou Chengdu, 611231
China
e-mail: 243512561@qq.com

Abstract. Let $G_2(q)$ be a Chevalley group over a finite field $K = F_q$ of characteristic p. For a group G, let $\text{nse}(G) = \{s_k \big| k \in \omega(G)\}$ where $\omega(G)$ is the set of element orders of G and s_k is the number of elements of order k in G. In this note, we give a new characterization of some special Chevalley groups $G_2(q)$ by nse.

Keywords and Phrases: Element order, Alternating group, Thompson's conjecture, Conjugacy classes, Simple group.

AMS Subject Classification: 20D05, 20D06, 20D20.

1. Introduction

For a finite group G, let $\omega(G)$ be the set of element orders of G. If $k \in \omega(G)$ and s_k be the number of elements of order k in G, then let $\text{nse}(G) = \{s_k \big| k \in \omega(G)\}$. J. G. Thompson put forward a very interesting problem related to algebraic number fields as follows (see [22], for instance).

Thompson's Problem. *Let $T(G) = \{(n, s_n) \big| n \in \omega(G)$ and $s_n \in \text{nse}(G)\}$, where s_n is the number of elements with order n. Suppose that $T(G) = T(H)$. If G is a finite solvable group, is it true that H is also necessarily solvable?*

So, some authors consider these cases (see [14], [19], and [20]).

If we consider only $\text{nse}(G)$, then whether can it characterize finite simple groups? Some groups $PSL(2, r)$ and S_r, where r is a prime and S_r is a symmetric group of degree r, are proved valid by nse (see [2], [3]). Recently, alternating groups A_p of special class under condition that $p \mid |G|$ but $p^2 \nmid |G|$, are characterized by nse only (see [1]). In this note, we give a new characterization of Chevalley groups $G_2(q)$ where $q \equiv -1 \mod 3$ and q is odd. In fact, we have the following.

Main theorem. *Let p be a prime and $p = q^2 + q + 1$ such that q is odd and $q \equiv -1 \mod 3$. Assume that $p||G|$. If $\mathrm{nse}(G) = \mathrm{nse}(G_2(q))$, then G is isomorphic to $G_2(q)$.*

Some notations are introduced. All groups considered are finite and p is a prime. For a natural number n, let $\pi(n)$ be the set of prime divisors of n. We denote by $\pi(G)$ the set of prime divisors of $|G|$ and by $\omega(G)$ the set of element orders of G. We also denote the number of elements of order k in G by s_k and let $\mathrm{nse}(G) := \{s_k : s_k \in \omega(G)\}$. If there is no ambiguity, we write s_k instead of $s_k(G)$. Let $GK(G)$ be a graph with vertex set $\pi(G)$ such that two primes p and q in $\pi(G)$ are joined by an edge if G has an element of order $p \cdot q$. We set $s(G)$ denote the number of connected components of the prime graph $GK(G)$ and let $m_1, m_2, \cdots, m_{s(G)}$ be the connected components of $GK(G)$. If $2 \in \pi(G)$, we assume that $2 \in m_1(G)$. $|G|$ can be expressed as a product of co-prime positive integers $OC_i, i = 1, 2, \cdots, s(G)$. The sets of order components of finite simple groups with disconnected prime graph can be obtained by [12] and [26]. Let r be a prime. Then we denote the number of the Sylow r-subgroup G_r of G by $n_r(G)$ or n_r. Also, $|x^G|$ denotes the order of conjugacy class of x in G. The other notations are standard (see [7], for instance).

2. Some preliminary results

In this section, we give some lemmas which will be used to prove the main theorem.

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

Proof. See [8]. ∎

Lemma 2. *Let G be a group containing more than two elements. If the maximal numbers of elements of the same order in G is finite, then G is finite and $|G| \leq s(s^2 - 1)$.*

Proof. See [21]. ∎

Lemma 3. *Let G be a group and P be a cyclic Sylow p-subgroup of G of order p^a. If there is a prime r such that $p^a r \in \omega(G)$, then $s_{p^a r} = s_r(C_G(P))s_{p^a}$. In particular, $\phi(r)s_{p^a} \mid s_{p^a r}$, where $\phi(r)$ is the Euler function of r.*

Proof. See [18]. ∎

Lemma 4. *Let $q > 1$ be an integer, m be a nature number, and p be an odd prime. If p divides $q - 1$, then $(q^m - 1)_p = m_p \cdot (q - 1)_p$.*

Proof. See Lemma 8(1) of [9]. ■

Lemma 5. *Let G be a finite group and $p \in \pi(G)$ be odd. Suppose that P is a Sylow p-subgroup of G and $n = p^s m$ with $(p, m) = 1$. If P is not cyclic and $s > 1$, then the number of elements of order n is always a multiple of p^s.*

Proof. See [15]. ■

Lemma 6. *Let a, b and n be positive integers such that $(a, b) = 1$. Then there exists a prime p with the following properties:*

- *p divides $a^n - b^n$,*
- *p does not divide $a^k - b^k$ for all $k < n$,*

with the following exceptions: $a = 2, b = 1$; $n = 6$ and $a + b = 2^k$; $n = 2$.

Proof. See [24]. ■

Remark 7. *If $b = 1$, the prime p is called the Zsigmondy prime. If p is a Zsigmnody of $a^n - 1$, then Fermat's little theorem shows that $n \mid p - 1$. Put $Z_n(a) = \{p : p$ is a Zsigmondy prime of $a^n - 1\}$. If $r \in Z_n(a)$ and $r \mid a^m - 1$, then $n \mid m$.*

Lemma 8. *If G is a finite group such that $t(G) \geq 2$, then G has one of the following structures:*

(1) *G is a Frobenius group or 2-Frobenius group;*

(2) *G has a normal series $1 \leq H \leq K \leq G$ such that $\pi(G/K) \cup \pi(H) \subseteq \pi_1$ and K/H is a non-abelian simple group. In particular, H is nilpotent, $G/K \lesssim \mathrm{Out}(K/H)$ and the odd order components of G are the odd order components of K/H.*

Proof. See [23]. ■

Lemma 9. *Let G be a Frobenius group of even order with kernel K and complement H. Then $s(G) = 2$, the prime graph components of G are $\pi(H)$ and $\pi(K)$ and the following assertions hold:*

(1) *K is nilpotent;*

(2) *$|K| \equiv 1 (mod \quad |H|)$.*

Proof. See [6]. ■

Lemma 10. *Let G be a 2-Frobenius group, i.e., G is a finite group and has a normal series $1 \leq H \leq K \leq G$ such that K and G/H are Frobenius groups with kernels H and K/H, respectively. Then:*

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

(2) *G/K and K/H are cyclic, $|G/K| \mid (|K/H| - 1)$ and $G/K \leq \mathrm{Aut}(K/H)$.*

Proof. See [6]. ∎

Lemma 11. *Let G be a finite non-abelian simple group and p is the largest prime divisor of $|G|$ with $p \mid |G|$. Then $p \nmid |\mathrm{Out}(G)|$.*

Proof. See [13]. ∎

3. Some information for $G_2(q)$

Let $\sum = \{\pm\xi_i, \xi_i - \xi_j \mid 1 \le i,\ j \le 3,\ i \ne j\}$ (where $\xi_1 + \xi_2 + \xi_3 = 0$) be the root system of type G_2, and choose $a = \xi_2, b = \xi_1 - \xi_2$ for a fundamental system of roots. Let χ be a homomorphism of the root module P_0 (i. e. P_0 is the additive group generated by the roots) into the multiplicative group K^*. Put $\chi(\xi) = z_i, i = 1, 2, 3$. Then the element $h(\chi_1)$ of Cartan subgroup H associated with $\mathfrak{H}$ will be denoted by $h(z_1, z_2, z_3)$. For each $r \in \sum$, there exists uniquely a homomorphism ϕ_r of $SL(2, K)$ into G such that $\phi_r\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_r(t), \phi_r\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-r}(t)$ for every $t \in K$. Let ω be an element of order 3 in K and $y_i \in P$ where P is a parabolic subgroup of G. Let $2 < q \equiv \epsilon \mod 3$ and assume that q is odd.

We know that $m_1(G_2(q)) = q^6(q^3-\epsilon)(q^2-1)(q+\epsilon)$ and $m_2(G_2(q)) = q^2-\epsilon q+1$.

Lemma 1. *In case $p \ne 2, 3$, the representatives and the orders of the centralizers in $G_2(q)$ are given by Table 1.*

Proof. See [5]. ∎

Lemma 2. *Let $L = G_2(q)$ with that q is odd and $q \equiv -1 \mod 3$. Let $p = q^2+q+1$ be a prime. Then*

$$s_p(L) = \sum_{|x|=p, x\ne 1} |x^L| = \frac{q^2+q}{6(q^2+q+1)}|L|.$$

Proof. Let $p = q^2 + q + 1$. Then from Lemma 1, we know that the order of the centralizers of an p-element in L is of order p and the number of the conjugacy classes of p-elements in L is $\frac{1}{6}(q^2 + q - 1 - \epsilon)$. Let $q \equiv -1 \mod 3$. Since $s_p(L) = \sum_{|x|=p, x\ne 1} |x^L|$, and $\epsilon = -1$, then

$$s_p(L) = \frac{q^2+q}{6(q^2+q+1)}|L|.$$ ∎

Lemma 3. *For $u \ne p$, then for every $u \in \omega(L)$, $p \mid s_u(L)$.*

Proof. It is easy to get from Lemma 1, that $p \mid s_u(L)$ for all $u \in \omega(L)$ such that $u \ne p$. ∎

Let n denote the number of conjugacy classes and Z the order of centralizers of elements of G, respectively.

Table 1. The representatives and the orders of the centralizers in case $p \neq 2, 3$

Representatives	n	Z
1	1	$q^6(q^2-1)(q^6-1)$
$h(-1,-1,1)$	1	$q^2(q^2-1)^2$
$h(\omega,\omega,\omega)$	1	$q^3(q^2-1)(q^3+\epsilon)$
$h(z,z^{-1},1), z^{q-1}=1, z^2\neq 1$	$\frac{q-3}{2}$	$q(q-1)^2(q+1)$
$h(z^{-1},z^{-1},z^2), z^{q-1}=1, z^2\neq 1, z^3\neq 1$	$\frac{q-4-\epsilon}{2}$	$q(q-1)^2(q+1)$
$h(z_1,z_2,z_3), z_i^{q-1}=1, z_iZ_j^{\pm 1}$	$\frac{q^2-8q+17+2\epsilon}{12}$	$(q-1)^2$
$h(z^{-1},z^{-1},z^2), z^{q+1}=1, z^2\neq 1, z^3\neq 1$	$\frac{q-2+\epsilon}{2}$	$q(q-1)(q+1)^2$
$h(z,z^{-1},1), z^{q+1}=1, z^2\neq 1$	$\frac{q-1}{2}$	$q(q-1)(q+1)^2$
$h(z_1,z_2,z_3), z_i^{q+1}=1, z_iZ_j^{\pm 1}$	$\frac{q^2-4q+5-2\epsilon}{12}$	$(q+1)^2$
$h(z,z^q,z^{-q-1}), z^{q^2-1}=1, z^{q\pm 1}\neq 1$	$\frac{(q-1)^2}{4}$	q^2-1
$h(z,z^{-q},z^{q-1}), z^{q^2-1}=1, z^{q\pm 1}\neq 1$	$\frac{(q-1)^2}{4}$	q^2-1
$h(z,z^q,z^{q^2}), z^{q^2+q+1}=1, z^3\neq 1$	$\frac{q^2+q-1-\epsilon}{6}$	q^2+q+1
$h(z,z^{-q},z^{q^2}), z^{q^2-q+1}=1, z^3\neq 1$	$\frac{q^2-q-1-\epsilon}{6}$	q^2-q+1
$h(-1,-1,-1)x_b(1)$	1	$q^2(q^2-1)$
$h(-1,-1,-1)x_c(1)$	1	$q^2(q^2-1)$
$h(-1,-1,-1)x_b(1)x_c(1)$	1	$2q^2$
$h(-1,-1,-1)x_b(1)x_c(\lambda)$	1	$2q^2$
$h(\omega,\omega,\omega)y, y\in\Phi_b \text{ or } \Phi_b^*$	1	$q^3(q-\epsilon)$
$h(\omega,\omega,\omega)y, y\in\Psi \text{ or } \Psi_2\cap\Gamma(\omega_2)$	3	$3q^3$
$h(z,z^{-1},1)x_c(1), z^{q-1}=1, z^2\neq 1$	$\frac{q-3}{2}$	$q(q-1)$
$h(z^{-1},z^2,z^{-1})x_b(1), z^{q-1}=1, z^2\neq 1, z^3\neq 1$	$\frac{q-1-\epsilon}{2}$	$q(q-1)$
$h(z,z^{-1},1)x_{2a+b}(1), z^{q+1}=1, z\neq 1$	$\frac{q-1}{2}$	$q(q+1)$
$h(z^{-1},z^2,z^{-1})x_{3a+2b}(1), z^{q+1}=1, z^3\neq 1$	$\frac{q-1+\epsilon}{2}$	$q(q+1)$

Lemma 4. *Assume that $L = G_2(q)$ where q is odd and $q \equiv -1 \mod 3$. Let $p = q^2+q+1$ be a prime. Then $s_2 = \frac{1}{q^2(q^2-1)}|L|$, in particular, $p \mid s_2$.*

Proof. It is known that L has one class of involutions (see [12, 17]). By Lemma 1, the order of the centralizers and the numbers of conjugacy classes of the elements x of order 2 in L are $q^2(q^2-1)$ and 1, respectively. Since $s_2 = \sum_{|x|=2, x\neq 1} |x^L|$, then $s_2 = \frac{|L|}{q^2(q^2-1)}$ In particular, $p \mid s_2$. ■

We also need the following due to Nosratpur and Darafsheh.

Lemma 5. *Let $L = G_2(q)$, where q is odd and $q \equiv -1 \mod 3$, and $d(q) = q^2+q+1$.*

(1) *If $p \in \pi(L)$, then $|L_p| \leq q^6$, where $L_p \in \mathrm{Syl}_p(L)$.*

(2) *If $p \in \pi_1(L)$, $p^\alpha \mid |L|$, and $p^\alpha - 1 \equiv 0 \mid d(q)$, then $p^\alpha = q^3$ or $p^\alpha = q^6$.*

Proof. See Lemma 3.2 of [16]. ■

4. Proof of the main theorem

In the proof of main theorem, we use the order components of finite simple groups that are listed as in Tables 1, 2 and 3 (see [10] and [23]).

Let G be a group such that $\mathrm{nse}(G) = \mathrm{nse}(G_2(q))$, and s_n be the number of elements of order n. By Lemma 2 We note that $s_n = k\phi(n)$, where k is the number of cyclic subgroups of order n. Also we note that if $n > 2$, then $\phi(n)$ is even. If $m \in \omega(G)$, then by Lemma 1 and the above discussion, we have

$$(4.1)\qquad \begin{cases} \phi(m) \mid s_m \\ m \mid \sum_{d\,|\,m} s_d. \end{cases}$$

Proof of the main theorem **Proof.** In the proof of the main theorem, we always assume that $\mathrm{nse}(G) = \mathrm{nse}(G_2(q))$ and $L = G_2(q)$ where q is odd and $q \equiv -1 \mod 3$. We divide the proof into the following series of Lemmas.

Lemma 1. *Let $p \neq u \in \pi(L)$. Then $p \mid s_u(L)$.*

Proof. It is easy to see that $p \mid s_u$ by Lemma 1. In fact, we can show this by the following.

By [4, Proposition 7], the maximal torus T of $G_2(q)$ has the order $(q \pm 1)^2$, $q^2 - 1$, $q^2 \pm q + 1$. Then there is an element $x \in L$ and some torus T such that $p \neq |x| = u$ and $T \leq C_L(x)$. It follows that $|x^L|$ is the multiple of $\frac{|L|}{|T|}$ for some T. But $s_u(L) = \sum\limits_{|x|=u, x\neq 1} |x^L|$. Hence $p \mid s_u(L)$. ∎

Lemma 2. *$s_2(G) = s_2(L)$. In particular, $p \mid s_2$.*

Proof. We know that if $2 < n \in \omega(G)$, then s_n is even. By Lemma 1, $2 \mid 1+s_2(L)$. On the other hand, in G, the only odd number in $\mathrm{nse}(G)\backslash\{1\}$ is $s_2(G)$. Hence we have $s_2(G) = s_2(L)$. By Lemma 1, $p \mid s_2$. ∎

Lemma 3. *For $u \in \omega(G)$, $p \nmid s_u(G)$ if and only if $s_u(G) = s_p(G)$. In particular $s_p(G) = s_p(L)$, in particular, $p \nmid s_p$.*

Proof. By Lemmas 2 and 3, $s_u(G) = s_p(L)$ if and only if $p \nmid s_u(G)$. By Lemma 1, $p \mid 1 + s_p(G)$ and so $p \nmid s_p(G)$. Therefore, we have $s_p(G) = s_p(L)$, in particular, $p \nmid s_p$. ∎

Lemma 4. *The Sylow p-subgroup of G is of order p.*

Proof. Let $G_p \in \mathrm{Syl}_p(G)$. Then by Lemma 1, $|G_p| \mid 1 + s_p + \cdots + s_{p^i}$ for some integer i. If $\exp(G_p) \geq p^3$, then by (4.1), $\phi(p^3) \mid s_{p^3}$ and hence, $p^2 \mid s_{p^3}$. But there is no number from $\mathrm{nse}(G)$ which is divisible by p^2. Thus $\exp(G_p) = p$ or p^2.

Let $\exp(G_p) = p^2$. Then there is an element of order p^2 with $\phi(p^2) \mid s_{p^2}$. Hence $p(p-1) \mid s_{p^2}$.

If $|G| = p^2$, then G_p is cyclic and so $n_p = \frac{s_{p^2}}{p(p-1)} = t$ for some integer t. We know that the intersection of any two Sylow p-subgroups of G may lie in a subgroup of order p. Therefore the number of cyclic subgroups of order p is something between 1 and the number of Sylow p-subgroups of G. It follows that $\frac{q^2+q}{6(q^2+q+1)}|L| = s_p \leq (p-1)n_p(G) = (p-1)t$ and so $n_p \geq \frac{|L|}{6(q^2+q+1)}$. Thus $s_{p^2} \geq \frac{p-1}{6}|L| > |L|$ since q is odd, $p = q^2+q+1$ with $q \equiv -1 \mod 3$.

If $|G_p| \geq p^3$, then by Lemma 5, $p^2 \mid s_{p^2}$ and so $s_{p^2} = p^2 t$ for some integer t. But the equation $s_{p^2} = p^2 t$ has no solution in nse(G), a contradiction.

Let $\exp(G_p) = p$. Then by Lemmas 2 and 3, $s_p = \frac{q^2+q}{6(q^2+q+1)}|L|$. Since

$$1+s_p = \frac{1}{6}p^2[(q^{10}-2q^9-q^8+7q^7-7q^6-5q^5+13q^4-8q^3-6q^2+15q-9)+\frac{13q+10}{q^2+q+1}],$$

then $|G_p| = p$. ∎

Lemma 5. *The prime divisor of* $|G|$ *is the same as* $|L|$.

Proof. By Lemma 3, $s_p = \frac{q^2+q}{6(q^2+q+1)}|L|$. Also by Lemma 4, $|G_p| = p = q^2+q+1$. It follows from Sylow's theorem, that $n_p = \frac{s_p}{\phi(p)} = \frac{|L|}{6p}$. Therefore, $\pi(G) = \pi(L)$. ∎

Lemma 6. *Let* $r \in \pi(G) - \{p\}$. *Then* $r \cdot p \notin \omega(G)$.

Proof. If $2 \cdot p \in \omega(G)$, then by Lemma 1, $2\cdot p \mid 1+s_2+s_p+s_{2\cdot p}$ and also $p \mid 1+s_p$.

By Lemma 2, $p \mid s_2$. It follows that $p \mid s_{2\cdot p}$.

By Lemma 4, we have that $|G_p| = |G|_p = p$. Then by Lemma 3, $s_{2\cdot p} = s_p \cdot t$ for some integer t and so $p \mid t$.

Let $t = pk$. Then $(k,p) = 1$ and hence $s_{2\cdot p} = s_p \cdot pk = \frac{q(q+1)|L|}{6}k$. We know that $|L| = \sum_{n \in \text{nse}(G)} n$ and so $s_{2\cdot p} > 2|L|$, a contradiction. It follows that $s_{2\cdot p} = s_p \cdot pk \notin \text{nse}(G)$. Therefore $s_{2\cdot p} = s_p$, also a contradiction since $p \nmid s_p$.

Therefore $2 \cdot p \notin \omega(G)$. Similarly we can prove that $r \cdot p \notin \omega(G)$ for $r \in \pi(G)\backslash\{2,p\}$. ∎

Lemma 7. $|G| \mid \frac{q^2+q}{6}|L|$.

Proof. By Lemma 6, $r \cdot p \notin \omega(G)$ for any prime $r \in \pi(G) - \{p\}$. It follows that the Sylow r-subgroup G_r of G acts fixed freely on the set of elements of order p and so $|G_r| \mid s_p$. Therefore $|G| \mid \frac{q^2+q}{6}|L|$. ∎

Lemma 8. *There is a normal series* $1 \leq H \leq K \leq G$ *such that* K/H *is isomorphic to* $G_2(q)$.

Proof. By Lemma 6, $s(G) \geq 2$. Then by Lemma 8, we have the following:

(1) G is a Frobenius group or 2-Frobenius group;

(2) G has a normal series $1 \leq H \leq K \leq G$ such that $\pi(G/K) \cup \pi(H) \subseteq \pi_1$ and K/H is a non-abelian simple group. In particular, H is nilpotent, $G/K \lesssim Out(K/H)$ and the odd order components of G are the odd order components of K/H.

First we prove that G is neither a Frobenius group nor a 2-Frobenius group.

Let G be a Frobenius group of even order with kernel H and complement K. Then by Lemma 9, $s(G)=2$, $\pi(G)=\{\pi(H),\pi(K)\}$. By Lemma 3, $\pi(H)=\{p\}$ or $\pi(K)=\{p\}$. If $\pi(H)=\{p\}$, then since H is nilpotent, H_p is characteristic in H. By hypothesis, we have that $H_p^g=G_p$ for some g and hence, G_p is normal in G. It follows that $s_p(G)=p-1$, contradicting Lemma 3. Now let $\pi(K)=\{p\}$. By Lemmas 4 and 3, $n_p \mid |G|$ and by Lemma 7, $|G| \mid \frac{(q^2+q)|L|}{6}$. So by Lemma 6, there is a prime $r\in Z_{n-1}(2)\cap\pi(G)$ and so $|L_r|=|L|_r=|q^2-1|_r=|q+1|_r$. Since $GK(G)=\{\pi(K),\pi(H)\}$, then $r\in\pi(H)$. Since K is nilpotent, G_r is normal in G. It follows from Lemma 6, that the Sylow p-subgroup of G acts fixed point freely on the set of elements of order r and so $p\le|G_r|\le q+1<q^2+q+1=p$, a contradiction.

Let G be a 2-Frobenius group. Then G has a normal series $1\le H\le K\le G$ such that $\pi(G/K)\cup\pi(H)\subseteq\pi_1$ and K/H is a cyclic group of order p and $|G/K| \mid (p-1)$. Similarly as the argument for the Frobenius group, we get a contradiction.

Therefore G has a normal series $1\le H\le K\le G$ such that $\pi(G/K)\cup\pi(H)\subseteq\pi_1$ and K/H is a non-abelian simple group. In particular, H is nilpotent, $G/K\lesssim Out(K/H)$ and the odd order components of G are the odd order components of K/H.

According to classification theorem of finite simple groups, K/H is an alternating group, sporadic group or simple group of Lie type. By Lemma 6, $s(K/H)\ge 2$.

Let $K/H\cong A_m$ with $m\ge 5$, then $m\ge p$. On the other hand, by Lemma 1 of [11] there is a prime $r\in\pi(A_m)\cap\pi(G)$ such that $q^2-1\le\frac{q^6-1}{2}<r<q^6-1$ and $r\in\pi(A_m)$ but $r\nmid|G|$ by Lemma 5, a contradiction.

Let K/H be sporadic simple groups, we can rule out this case by considering their odd order component since the odd components of K/H is $p=q^2+q+1$ with q odd and $q\equiv -1 \mod 3$.

Therefore K/H is isomorphic to a simple group of Lie type. We consider the following cases.

Case 1: Let $s(K/H)=2$. Then we have that $OC_2(K/H)=p=q^2+q+1$ with q odd and $q\equiv -1 \mod 3$.

1.1. Let $K/H\cong A_{p'-1}(q')$ with $(p',q')\ne(3,2),(3,4)$.

Then $\frac{q'^{p'-1}-1}{(q'-1)(p',q'-1)}=q^2+q+1$ and so $p'-1=2$, $q'=q$. Then by Lemma 7, $(q^4-1)(q^3-1)(q^2-1) \mid \frac{q^2+q}{6}|L|=\frac{q^2+q}{6}\cdot q^6(q^2-1)(q^6-1)$, a contradiction. Similarly, we can rule out these cases "$K/H\cong^2 A_{p'-1}(q')$ and $K/H\cong^2 A_{p'}(q')$".

1.2. Let $K/H\cong B_{p'}(3)$. Then $\frac{3^{p'}-1}{2}=q^2+q+1$. But by Lemma 6, the equation has no solution in $\mathbb{N}$.

1.3. Let $K/H\cong C_n(q')$ with $n=2^m\ge 2$, q' odd. Then $\frac{q'^n+1}{(2,q-1)}=q^2+q+1$ and so by Lemma 6, the equation has no solution. Similarly, we can rule out "$K/H\cong C_{p'}(q')$".

1.4. Let $K/H \cong D_{p'}(q')$ with $p' \geq 5, q' = 2, 3, 5$. Then $\frac{q'^{p'}-1}{(2,q'-1)} = q^2 + q + 1$ and so $q \geq 2q'$. By Lemma 7, $q'^{p'} \mid q^7$ and hence, $q'^{p'} < 2^7 q'^7$. If $q' = 2$, then $p' < 14$. It follows that $p' = 5, 6, 7, \cdots, 13$. Thus order consideration rules out these cases. Similarly, we can rule out $K/H \cong D_{p'+1}(q')$ with $q' = 2, 3$.

1.5. Let $K/H \cong^2 D_n(q')$, with $n = 2^m \geq 4$, then $\frac{q'^n+1}{(2,q'+1)} = q^2 + q + 1$. If q' is odd, then by Lemma 6, the equation has no solution. If q' is even, then $q'^n = q(q+1)$, the equation has no solution. Similarly, we can rule out these cases "$K/H \cong^2 D_n(2)$ with $n = 2^m + 1 \geq 5$, $K/H \cong^2 D_p(3)$ with $5 \leq p \neq 2^m + 1$ and $K/H \cong^2 D_n(3)$ with $9 \leq 2^m + 1 \neq p$".

1.6. Let $K/H \cong G_2(q')$, with $2 < q' \equiv \epsilon \mod 3, \epsilon = \pm 1$, then $q'^2 - \epsilon q' + 1 = q^2 + q + 1$ and hence, $q'(q' - \epsilon) = q(q + 1)$. If $\epsilon = -1$, then we have the desired result. If $\epsilon = 1$, then $q' = 3, q = 2$. Order consideration rule out this case.

1.7. Let $K/H \cong^3 D_4(q')$, then $q'^4 + q'^2 + 1 = q^2 + q + 1$ and hence, $q'^2(q'^2 + 1) = q(q + 1)$. Thus $q'^2 = q$, and so $(q^3 - 1)(q^6 - 1) \mid (q^2 - 1)(q^6 - 1)$, a contradiction.

1.8. Let $K/H \cong F_4(q')$ with q' odd, then $q'^4 - q'^2 + 1 = q^2 + q = 1$ and hence, $q'^2(q'^2 - 1) = q(q + 1)$, a contradiction.

1.9. Let $K/H \cong E_6(q')$, then $\frac{q'^6+q'^3+1}{(3,q'-1)} = q^2 + q + 1$. If q' is odd, then $q = q'^3$, and so $q^{12} \mid q^7$, a contradiction. If q' is even and $q' \equiv 1 \mod 3$, then $q'^3(q'^3 + 1) = 3(q^2+q)+2 = 2(1+3\frac{q^2+q}{2})$, the equation has no solution. Similarly, $K/H \ncong^2 E_6(q')$ with $q' > 2$.

Case 2: Let $s(L/K) = 3$. Then $q^2 + q + 1 \in \{OC_2(K/H), OC_3(K/H)\}$.

2.1. Let $K/H \cong L_2(q')$, where $4 \mid q' + 1$. Then $q' = q^2 + q + 1$ or $\frac{q'-1}{2} = q^2 + q + 1$.

> If $q' = q^2 + q + 1$, then $4 \mid q' + 1 = q^2 + q + 2$. So there is a prime r such that $p < r < p^6$ and $r \in \pi(H)$ or $r \in \pi(G) \setminus \pi(L_2(q'))$ contradicting the maximality of p. If $r \in \pi(H)$, then $r \sim p$, a contradiction. If the latter, $r \mid \mathrm{Out}(L_2(q'))$, contradicting Lemma 11.
>
> If $\frac{q'-1}{2} = q^2 + q + 1$, then $q' = 2p + 1$. Similarly, we can rule out this case as above.

Similarly, $K/H \ncong L_2(q)$, with $4 \mid q - 1$ and $K/H \ncong L_2(q)$, with $q > 2$ and q even.

2.2. Let $K/H \cong^2 D_{p'}(3)$ with $5 \leq p' = 2^m + 1$. Then $p = \frac{3^{p'-1}+1}{2}$ or $p = \frac{3^{p'}+1}{4}$. In both cases, by Lemma 6, there is no solution. Similarly, $K/H \ncong^2 D_{p'+1}(2)$ with $n \geq 2, p' = 2^n - 1$.

2.3. Let $K/H \cong G_2(q')$ with $q' \equiv 0 \mod 3$. Then $q'^2 - q' + 1 = q^2 + q + 1$ or $q'^2 + q' + 1 = q^2 + q + 1$. If the former, then $q'(q' - 1) = q(q + 1)$ and so $q' = 3, q = 2$. Order consideration rules out this case. If the latter, $q = q'$ and so $(q^2 - 1)^3 \mid (q^2 - 1)^2$, a contradiction. Similarly we can rule out "$K/H \cong^2 G_2(q')$ with $q' = 3^{2m+1} > 3$".

2.4. Let $K/H \cong F_4(q')$, where q' is even. Then $q'^4+1 = q^2+q+1$ or $q'^4 - q'^2+1 = q^2+q+1$. If the former, $q'^4 = q(q+1)$, a contradiction. If the latter, $q'^2(q'^2-1) = q(q+1)$, but the equation has no solution in $\mathbb{N}$. Similarly, $K/H \ncong^2 F_4(q')$, where $q' = 2^{2m+1} > 2$.

Case 3: $s(K/H) \in \{4,5\}$. Then $p = q^2+q+1 \in \{OC_2(K/H), OC_3(K/H), OC_4(K/H), OC_5(K/H)\}$.

3.1. Let $K/H \cong L_3(4)$ or ${}^2E_6(2)$. Then $2^n-1=7$ or $2^n-1=19$. If the former, $n=3$, then order consideration rules out. If the latter, it is impossible.

3.2. Let $K/H \cong^2 B_2(q')$, with $q' = 2^{2m+1}$. Then $p = q^2+q+1 \in \{q'-1, q' \pm \sqrt{2q'}+1\}$. If the former, then $q^2+q+1 = p = q'-1$. Order consideration rules out. If the latter, then $\sqrt{q'}(\sqrt{q'}+\sqrt{2}) = q(q+1)$ or $\sqrt{q'}(\sqrt{q'}-\sqrt{2}) = q(q+1)$, the equation has no solution in $\mathbb{N}$.

3.3. Let $K/H \cong E_8(q')$. If $\frac{q'^{10}-q'^5+1}{q'^2-q'+1} = q^2+q+1$, then $q'^{30} \equiv 1 \mod d(q)$. By Lemma 5, $q'^{30} = q^6$ and so $q'^{120} = q^{24} > q^6$, a contradiction. If $\frac{q'^{10}+q'^5+1}{q'^2+q'+1} = q^2+q+1$, then $q'^{15} \equiv 1 \mod d(q)$. By Lemma 5, $q'^{15} = q^6$ and so $q'^{120} = q^{48} > q^6$, a contradiction. If $q'^8+q'^4+1 = q^2+q+1$, then $q'^4(q'^4+1) = q(q+1)$ and so $q'^4 = q$. But $q'^{120} = q^{30} > q^6$, a contradiction.

Hence $K/H \cong G_2(q)$ with $q \equiv -1 \mod 3$ and q odd. ∎

Lemma 9. $\pi(H) \subsetneqq \pi(q^2+q)$.

Proof. Let $r \in \pi(H)$. Then $r \neq p$ and by Lemma 8, H is nilpotent. It follows that H_r is normal in G. By Lemma 6, $r \cdot p \notin \omega(G)$, and hence, the Sylow p-subgroup of G acts fixed point freely on the set of elements of order r. Thus $p \mid |H_r|-1$. If $r \notin \pi(q(q+1))$, then by Lemma 7, $|H_r| \mid (q^2+q)_r|L|_r$. By the proof of Lemma 8, we know that $r \nmid q(q+1)$ and hence, $|H_r| \mid |L|_r$. On the other hand, $H_r \leq q^t-1$ for some integer $t \in \{2,6\}$ and so $p \leq |H_r| \leq q^2+q+1 = p$, a contradiction. Thus $\pi(H) \subsetneqq \pi(q^2+q)$. ∎

Lemma 10. *G is isomorphic to $G_2(q)$ with $q \equiv -1 \mod 3$ and q odd.*

Proof. By Lemma 8, we have that K/H is isomorphic to $G_2(q)$. We will prove that $H=1$. Assume the contrary, then by Lemma 9, H is a π-group with $\pi = \pi(q^2+q)$. By Lemma 6, $2 \cdot p \notin \omega(G)$ and hence, the Sylow p-subgroup acts fixed point freely on H_2-1 and so $p \mid |H|-1 = (q+1)_2-1 < q+1 < q^2+q+1 = p$, where n_r denotes the number such that $r^m \mid n$ but $r^{m+1} \nmid n$ for some integer m, a contradiction. If $2 \neq r \in \pi(q(q+1))$, then we also have $r \cdot p \in \omega(G)$. It follows that the Sylow p-subgroup acts fixed point freely on H_r-1 and so $p \mid |H|-1 \leq q+1 < q^2+q+1 = p$, a contradiction. It follows that $H=1$ and so $K \cong G_2(q)$. We refine the normal series into $1 < K < G$ and so $K < G < \mathrm{Aut}(K)$. If $G \cong G_2(q)$, it is the desired result. If $G \cong \mathrm{Aut}(G_2(q))$, then there is a prime $r \in \pi(f)$ where $q = r'^f$ (by [7, pp. xvi], $|\mathrm{Out}(G_2(q))| = f$) such that $s_r(Aut(G_2(q))) \notin \mathrm{nse}(G)$, a contradiction. This completes the proof of the Lemma. ∎

This completes the proof. ∎

5. Some applications

On Thompson's conjecture, if G and H are of the same order type, then $\mathrm{nse}(G) = \mathrm{nse}(H)$ and $|G| = |H|$.

Corollary 1. *Let $p = q^2 + q + 1$ be a prime and $p \| |G|$ with $q \equiv -1 \mod 3$. Then $G \cong G_2(q)$ if and only if $|G| = |G_2(q)|$ and $\mathrm{nse}(G) = \mathrm{nse}(G_2(q))$.*

Shi gave the following conjecture.

Conjecture. [22] *Let G be a group and H a finite simple group. Then $G \cong H$ if and only if (a) $\omega(G) = \omega(H)$ and (b) $|G| = |H|$.*

Then we have the following corollary.

Corollary 2. *Let $p = q^2 + q + 1$ be a prime and $p \| |G|$ with $q \equiv -1 \mod 3$. Then $G \cong G_2(q)$ if and only if $\omega(G) = \omega(G_2(q))$ and $|G| = |G_2(q)|$.*

Acknowledgments. The object was supported by the Opening Project of Sichuan Province University Key Laboratory of Bridge Non-destruction Detecting and Engineering Computing (Grant No: 2013QYJ02 and 2014QYJ04), by the Scientific Research Project of Sichuan University of Science and Engineering (Grant No: 2014RC02) and by the Department of Education of Sichuan Province (Grant No: 15ZA0235). The authors are very grateful for the helpful suggestions of the referee.

References

[1] Ahanjideh, N., Asadian, B., *NSE characterization of some alternating groups*, J. Algebra Appl., 14 (2) (2015).

[2] Asboei, A.K., *A new characterization of PGL(2, p),* J. Algebra Appl., 12 (7) (2013).

[3] Asboei, A.K., Amiri, S.S.S., Iranmanesh, A., Tehranian, A., *A characterization of symmetric group S_r, where r is prime number*, Ann. Math. Inform., 40 (2012), 13–23.

[4] Carter, R.W., *Centralizers of semisimple elements in the finite classical groups*, Proc. London Math. Soc., 42 (3) (1981), 1–41.

[5] Chang, B., *The conjugate classes of Chevalley groups of type* (G_2), J. Algebra, 9 (1968), 190–211.

[6] Chen, G., *On Frobenius and 2-Frobenius group*, J. Southwest China Normal Univ., 20 (5) (1995), 485–487.

[7] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A., *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray.

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

[9] GRECHKOSEEVA, M.A., *Recognition of finite simple linear groups over fields of characteristic 2 by the spectrum*, Algebra Log., 47 (4) (2008), 405–427, 524.

[10] KONDRAT'EV, A.S., *On prime graph components of finite simple groups*, Mat. Sb., 180 (6) (1989), 787–797, 864.

[11] KONDRAT'EV, A.S., MAZUROV, V.D., *Recognition of alternating groups of prime degree from the orders of their elements*, Sibirsk. Mat. Zh., 41 (2) (2000), 359–369, iii.

[12] LANG, S., *Algebraic groups over finite fields*, Amer. J. Math., 78 (1956), 555–563.

[13] LIU, S., *OD-characterization of some alternating groups*, Turkish J. Math., 39 (2015).

[14] LIU, S., ZHANG, R., *A new characterization of* A_{12}, Math. Sci., 6 (6) (2012), 30.

[15] MILLER, G.A., *Addition to a theorem due to Frobenius*, Bull. Amer. Math. Soc., 11 (1) (1904), 6–7.

[16] NOSRATPUR, P., DARAFSHEKH, M.R., *Characterization of the groups* $G_2(q)$ *for* $2 < q \equiv -1 \pmod 3$ *by order components*, Sibirsk. Mat. Zh., 54 (5)(2013), 1102–1114.

[17] REE, R., *Classification of involutions and centralizers of involutions in certain simple groups*. In: Proc. Internat. Conf. Theory of Groups (Canberra, 1965). Gordon and Breach, New York, 1967, 281–301.

[18] SHAO, C., JIANG, Q., *A new characterization of some linear groups by NSE*, J. Algebra Appl., 13 (2) (2014).

[19] SHAO, C., SHI, W., JIANG, Q., *Characterization of simple* K_4*-groups*, Front. Math. China, 3 (3) (2008), 355–370.

[20] SHAO, C.G., SHI, W.J., JIANG, Q.H., *A characterization of simple* K_3*-groups*, Adv. Math. (China), 38 (3) (2009), 327–330.

[21] SHEN, R., SHAO, C., JIANG, Q., SHI, W., MAZUROV, V., *A new characterization of* A_5, Monatsh. Math., 160 (3) (2010), 337–341.

[22] SHI, W.J., *A new characterization of the sporadic simple groups*. In: Group theory (Singapore, 1987). de Gruyter, Berlin, 1989, 531–540.

[23] WILLIAMS, J., *Prime graph components of finite groups*, J. Algebra, 69 (2) (1981), 487–513.

[24] ZSIGMONDY, K., *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., 3 (1) (1892), 265–284.

Accepted: 27.03.2015