Czechoslovak Mathematical Journal

Azam Babai; Ali Mahmoudifar

Thompson's conjecture for the alternating group of degree $2p$ and $2p+1$

Czechoslovak Mathematical Journal, Vol. 67 (2017), No. 4, 1049–1058

Persistent URL: `http://dml.cz/dmlcz/146966`

Czechoslovak Mathematical Journal, 67 (142) (2017), 1049–1058

THOMPSON'S CONJECTURE FOR THE ALTERNATING GROUP OF DEGREE $2p$ AND $2p+1$

Azam Babai, Qom, Ali Mahmoudifar, Tehran

Received July 25, 2016. First published October 5, 2017.

Abstract. For a finite group G denote by $N(G)$ the set of conjugacy class sizes of G. In 1980s, J. G. Thompson posed the following conjecture: If L is a finite nonabelian simple group, G is a finite group with trivial center and $N(G)=N(L)$, then $G\cong L$. We prove this conjecture for an infinite class of simple groups. Let p be an odd prime. We show that every finite group G with the property $Z(G)=1$ and $N(G)=N(A_i)$ is necessarily isomorphic to A_i, where $i\in\{2p,2p+1\}$.

Keywords: finite group; conjugacy class size; simple group

MSC 2010: 20D05, 20D60

1. Introduction

Let G be a finite group. The set of conjugacy class sizes of G is denoted by $N(G)$. Let n be a natural number. We denote by $\pi(n)$ the set of all prime divisors of n. For a finite group G, the set $\pi(|G|)$ is denoted by $\pi(G)$. Let $\Gamma(G)$ be a simple graph with vertex set $\pi(G)$ such that two distinct prime numbers p and q are adjacent whenever G has an element of order pq. This graph is called the prime graph of G. The number of connected components of $\Gamma(G)$ is denoted by $s(G)$. Also we may define another simple graph on $\pi(G)$, which is called the solvable graph of G and is denoted by $\Gamma_{\rm sol}(G)$. In $\Gamma_{\rm sol}(G)$, two distinct prime numbers p and q are adjacent whenever G has a solvable subgroup H such that $\{p,q\}\subseteq\pi(H)$. In these two graphs, a subset T of $\pi(G)$ is called an independent subset if for every two elements p and q from T there is no edge.

If $p\in\pi(n)$, then by n_p we mean the p-part of n, i.e. $n_p=p^k$ if $p^k\mid n$ but $p^{k+1}\nmid n$. Also from $p^\alpha\parallel n$ we get that $n_p=p^\alpha$. The set of all prime numbers p with $n/2<p\leqslant n$ is denoted by $\Pi(n)$.

A famous conjecture of J. G. Thompson about the characterization of finite nonabelian simple groups is expressed as follows:

Thompson's conjecture. If L is a finite nonabelian simple group, G is a finite group with trivial center and $N(G) = N(L)$, then L and G are isomorphic.

This conjecture, which is Problem 12.38 in the Kourovka notebook [11], was posed in 1988. Chen in [5] proved that this conjecture is valid for simple groups G with $s(G) \geqslant 3$. In [13], it is proved that Thompson's conjecture holds for A_{10} and $L_4(4)$. Also Ahanjideh in [2] and [3] proved that Thompson's conjecture is true for $L_n(q)$ and $D_n(q)$, respectively. The set of all groups G, which have the property $\pi(G) \subseteq \{2, 3, 5, 7, 11, 13, 17\}$, is denoted by ζ_{17}. In [6], it is proved that Thompson's conjecture is valid for those ζ_{17}, whose prime graph is connected. Also the simple groups A_n, where $n = p$, $p + 1$, $p + 2$ and $p \geqslant 3$ is a prime, satisfy Thompson's conjecture (see [4]). Moreover, this conjecture is valid for the alternating simple group A_{22} (see [14]). Also in [7] it is proved that Thompson's conjecture is true for A_n, where $n > 1361$ and at least one of numbers n or $n - 1$ are decomposed into a sum of two primes; we use this article for proving Lemmas 3.10 and 3.11.

In this paper, we prove that this conjecture holds for the simple group A_{2p} and A_{2p+1}, where p is an odd prime number. Indeed, we have the following theorem:

Main theorem. *Let p be an odd prime number and $i \in \{2p, 2p+1\}$. If G is a finite group with trivial center and $N(G) = N(A_i)$, then $G \cong A_i$. In particular, Thompson's conjecture holds for the simple group A_{2p} and A_{2p+1}.*

2. Preliminary results

Lemma 2.1 ([12], Lemma 3). *If $n \geqslant 21$, then $|\Pi(n)| \geqslant 0.366n/\ln(n)$. In particular, $|\Pi(n)| \geqslant 3$.*

Lemma 2.2 ([1], Lemma 2.2). *Let $g \in A_n$ and suppose the cycle decomposition of g contains exactly $c_i = c_i(g)$ cycles of length i for each $i \in \{1, \ldots, n\}$ so that $n = \sum\limits_{i=1}^{n} ic_i$. Let $z = n!\Bigl(\prod\limits_{i=1}^{k} i^{c_i} \prod\limits_{i=1}^{k} c_i!\Bigr)^{-1}$. Then for the size of the conjugacy class g^{A_n} of g in A_n we have:*

(1) *If for all even i, $c_i = 0$ and for all odd i, $c_i \in \{0, 1\}$, then $|g^{A_n}| = z/2$.*
(2) *In all other cases, $|g^{A_n}| = z$.*

Lemma 2.3 ([13], Lemma 4). *Suppose that G is a finite group with trivial center and p is a prime from $\pi(G)$ such that p^2 does not divide $|x^G|$ for all x in G. Then a Sylow p-subgroup of G is elementary abelian.*

Lemma 2.4 ([13], Lemma 5)**.** *Let K be a normal subgroup of G and $\overline{G} = G/K$.*
(1) *If $\bar{x}$ is the image of an element x of G in $\overline{G}$, then $|\bar{x}^{\overline{G}}|$ divides $|x^G|$.*
(2) *If $(|x|, |K|) = 1$, then $C_{\overline{G}}(\bar{x}) = C_G(x)K/K$.*
(3) *If $y \in K$, then $|y^K|$ divides $|y^G|$.*

Lemma 2.5 ([6], Lemma 1.4)**.** *Let $x, y \in G$, $(|x|, |y|) = 1$, and $xy = yx$. Then $C_G(xy) = C_G(x) \cap C_G(y)$.*

Lemma 2.6 ([14], Lemma 7)**.** *Let L be a finite simple group, let G be a finite group, and let $p \in \pi(L)$.*
(1) *Then there exists an element $x \in L$ such that $|L|_p = |x^L|_p$.*
(2) *If $N(G) = N(L)$, then $|L|$ divides $|G|$.*

Lemma 2.7 ([10], Lemma 2.2)**.** *Let G be a finite group and $p, q \in \pi(G)$ such that $p \neq q$. Also let $|G|_p = p$, $|G|_q = q$, $p \nmid q - 1$ and $q \nmid p - 1$. Then $p \sim q$ in $\Gamma(G)$ if and only if $p \sim q$ in $\Gamma_{\mathrm{sol}}(G)$.*

Lemma 2.8 ([10], Theorem 2.1)**.** *Let G be a finite group and T be an independent subset of $\Gamma_{\mathrm{sol}}(G)$ with $|T| \geqslant 2$. Then there exists a nonabelian simple group S such that*
$$S \leqslant \overline{G} := \frac{G}{N} \leqslant \mathrm{Aut}(S),$$
where $N = O_{T'}(G)$. Also we have $T \subseteq \pi(S)$ and $\pi(\overline{G}/S) \cap T = \emptyset$. Moreover, $C_G(N) \leqslant N$ or $S \leqslant C_G(N)N/N$.

Lemma 2.9 ([10], Theorem 2.4)**.** *Let $n \geqslant 13$ be a natural number and p be the greatest prime number less than or equal to n. Also let G be a finite group such that $|G| \mid n!$. If $\Pi(n)$ is an independent subset of $\Gamma_{\mathrm{sol}}(G)$, then there exists a natural number m such that*
$$A_m \leqslant G/N \leqslant S_m,$$
where $N = O_{\Pi(n)'}(G)$ and $p \leqslant m$.

Lemma 2.10 ([9], Theorem 4.34)**.** *Let A act via automorphisms on an abelian group G, and suppose that $(|G|, |A|) = 1$. Then $G = C_G(A) \times [G, A]$.*

Lemma 2.11 ([8], Lemma 5)**.** *Let g act via automorphisms on an abelian group G, and suppose that $(|G|, |g|) = 1$. Then $|g|$ divides $|[G, g]| - 1$.*

Lemma 2.12 ([6], Lemma 1.6). *Let G be a finite group, $N \trianglelefteq G$, and $C \leqslant G$. Then $|N : N \cap C|$ divides $|G : C|$.*

3. Proof of the Main theorem

Let G be a finite group with trivial center. First, suppose that $N(G) = N(A_{2p})$. We are going to prove $G \cong A_{2p}$.

According to [6], [14], if $N(G) = N(A_{2p})$, then $G \cong A_{2p}$ for $p \leqslant 11$. So in the following we assume that $\varrho := \Pi(2p)$ and $p > 11$ is a prime number. We will prove the above assertion using the following lemmas:

Lemma 3.1. *There exists $g \in G$ such that the conjugacy class size of g is equal to $(2p)!/2p^2$ and it is a maximal element of $N(G)$ by divisibility.*

Proof. Since $N(G) = N(A_{2p})$, for every $a \in A_{2p}$ there exists $g \in G$ such that $|g^G| = |a^{A_{2p}}|$. Let $a := (1\ 2 \ldots\ p)(p+1\ p+2\ \ldots\ 2p)$ be a permutation in A_{2p}. Hence $|a^{A_{2p}}| = (2p)!/2p^2$ by Lemma 2.2. Since $|a^{A_{2p}}|$ is a maximal element of $N(A_{2p})$, the proof is complete. ☐

Lemma 3.2. *Let $s \in \varrho$. Every s'-number of $N(A_{2p})$ is divisible by p.*

Proof. Let $|b^{A_{2p}}|$ be an s'-number of $N(A_{2p})$. Let the cyclic structure of b be denoted by $1^{t_1}2^{t_2}\ldots l^{t_l}$, where $2p = \sum_{i=1}^{l} it_i$. Hence, we have

$$|b^{A_{2p}}| = \frac{(2p)!}{1^{t_1}\ldots l^{t_l}t_1!\ldots t_l!\,d},$$

where $d \in \{1, 2\}$. Since s does not divide $|b^{A_{2p}}|$ and $s \parallel (2p)!$, so $s \parallel 1^{t_1}\ldots l^{t_l}t_1!\ldots t_l!$. Therefore we have the two following cases:

Case 1. Let $s \mid 1^{t_1}\ldots l^{t_l}$. So there exists a natural number $m \leqslant l$ such that $m = s$.

On the contrary, assume that p does not divide $|b^{A_{2p}}|$. Similarly to the above discussion, we get that $p^2 \parallel 1^{t_1}\ldots l^{t_l}t_1!\ldots t_l!$. We have the following cases:

▷ Let there exist a natural number $m' \leqslant l$ such that $m' = p$ and $t_{m'} = 2$. It follows that

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m + m't_{m'} \geqslant s + 2p > 3p,$$

which is a contradiction.

▷ Let there exist a natural number $m' \leqslant l$ such that $t_{m'} \geqslant 2p$. Consequently,

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m + m't_{m'} \geqslant s + 2p > 3p,$$

which is impossible.

▷ Let there exist a natural number $m', m'' \leqslant l$ such that $p \leqslant t_{m'}, t_{m''} < 2p$. Consequently,

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m + m't_{m'} + m''t_{m''} \geqslant s + p + p > 3p,$$

which is impossible.

▷ Let there exist a natural number $m', m'' \leqslant l$ such that $m' = p$ and $p \leqslant t_{m''} < p^2$. Hence,

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m + m't_{m'} + m''t_{m''} \geqslant s + p + p > 3p,$$

which is a contradiction.

Therefore p divides $|b^{A_{2p}}|$.

Case 2. Let $s \mid t_1! \dots t_l!$. Therefore there exists a natural number $m \leqslant l$ such that $t_m \geqslant s$. By the same discussion, we get that p divides $|b^{A_{2p}}|$. □

Remark 3.1. Let $s \in \varrho$ and $g \in G$. There exists $a \in A_{2p}$ such that $|g^G| = |a^{A_{2p}}|$. Since $|a^{A_{2p}}|_s \leqslant s$, s^2 does not divide $|g^G|$. Now by Lemma 2.3, we conclude that a Sylow s-subgroup of G is elementary abelian.

Lemma 3.3. *Let $s \in \varrho$. A Sylow s-subgroup S of G has the order s.*

Proof. By Lemma 2.6 we know that s divides $|G|$. Let $|S| \geqslant s^2$, hence s^2 divides $|G|$. Let $g \in G$ such that $|g^G| = (2p)!/2p^2$, which is a maximal element of $N(G)$ by Lemma 3.1. By Remark 3.3 for every $x \in G$ we know that s^2 does not divide $|x^G|$, which implies that s divides $|C_G(x)|$ for every $x \in G$. We consider the following two cases:

Case 1. Assume that s does not divide $|g|$. By the above discussion, we know that there exists $w \in C_G(g)$ such that $|w| = s$, which implies that $C_G(gw) = C_G(g) \cap C_G(w)$. Then $|g^G|$ divides $|(gw)^G|$ and $|w^G|$ divides $|(gw)^G|$. Since $|g^G|$ is maximal, $|g^G| = |(gw)^G|$ and so $|w^G|$ divides $|g^G|$. On the other hand, according to Remark 3.3, S is abelian, so $C_G(w)$ includes S up to conjugacy. Then s does not divide $|w^G|$ which implies that p divides $|w^G|$ by Lemma 3.2. Consequently, p divides $|g^G|$, which is impossible.

Case 2. Suppose that s divides $|g|$. Let $t \in \mathbb{N}$ such that $|g| = st$. Since S is elementary abelian, the numbers s and t are coprime. Put $u = g^s$ and $v = g^t$. Then $g = uv$ and $C_G(g) = C_G(u) \cap C_G(v)$. Therefore $|v^G| \mid |g^G|$. On the other hand, since $|v| = s$, $|v^G|$ is an s'-number. Therefore p divides $|v^G|$ by Lemma 3.2, which implies that p divides $|g^G|$, which is a contradiction. □

Lemma 3.4. *Let $s, t \in \varrho$ and $s < t$. There is no element of order st in G. In particular, ϱ is an independent set in $\Gamma(G)$.*

Proof. On the contrary, let $g \in G$ such that $|g| = st$. Put $u = g^s$ and $v = g^t$. Then $g = uv$ and $C_G(g) = C_G(u) \cap C_G(v)$. Then st divides $|C_G(g)|$. On the other hand, by Lemma 3.4 $|G|_s = s$ and $|G|_t = t$, hence st does not divide $|g^G|$. Consider that $b \in A_{2p}$ such that $|g^G| = |b^{A_{2p}}|$. Suppose that the cyclic structure of b is denoted by $1^{t_1}2^{t_2}\dots l^{t_l}$, where $2p = \sum\limits_{i=1}^{l} it_i$. Hence $|g^G| = (2p)!/(1^{t_1}\dots l^{t_l}t_1!\dots t_l!\,d)$, where $d \in \{1, 2\}$ and so st divides $1^{t_1}\dots l^{t_l}t_1!\dots t_l!$. We consider the following cases:

Case 1. Assume that there exist $m, m' \leqslant l$ such that $m = s$ and $m' = t$. We have

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m + m't_{m'} \geqslant s + t > 2p,$$

which is a contradiction.

Case 2. Suppose that there exist $m, m' \leqslant l$ such that $m = t$ and $s \leqslant t_{m'} < t$. Then

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m + m't_{m'} \geqslant s + t > 2p,$$

which is impossible.

Case 3. Let $m \leqslant l$ such that $t_m \geqslant t$. Let $m \geqslant 2$. Therefore

$$2p = \sum_{i=1}^{l} it_i \geqslant mt_m \geqslant 2t > 2p,$$

which is a contradiction.

Therefore $m = 1$ and so $t_1 \geqslant t$. Recall that

$$|g^G| = \frac{(2p)!}{1^{t_1}\dots l^{t_l}t_1!\dots t_l!\,d},$$

where $d \in \{1, 2\}$, $p < t \leqslant t_1 < 2p$ and for all $i \geqslant 2$ we have $t_i < p$. Consequently, $|g^G|_p = p$.

So we have

$$p = |g^G|_p = \frac{|G|_p}{|C_G(g)|_p}.$$

Then we can consider Sylow p-subgroup P of G such that $M = P \cap C_G(g)$ has index p in P. It follows that M is normal in P and so there exists a nontrivial element z in $M \cap Z(P)$. Since $z \in Z(P)$, p does not divide $|z^G|$. On the other hand, $z \in C_G(g)$, so $|g|$ divides $|C_G(z)|$, hence st divides $|C_G(z)|$. Consequently, st does not divide $|z^G|$ and so p divides $|z^G|$ by Lemma 3.2, which is a contradiction. Therefore there is no element of order st in G. $\square$

Lemma 3.5. *There exists a nonabelian simple group S such that*

$$S \leqslant \overline{G} := G/N \leqslant \mathrm{Aut}(S),$$

where N is a normal subgroup of G such that $\pi(N) \cap \varrho = \emptyset$. Moreover, $\varrho \subseteq \pi(S)$.

P r o o f. By Lemmas 2.7 and 3.5, we know that ϱ is an independent set in $\Gamma_{\mathrm{sol}}(G)$. On the other hand, since $p > 11$, $|\varrho| \geqslant 2$. Therefore the result follows by Lemma 3.5 and Theorem 2.8. $\square$

In the following, we consider S and N as in the last lemma. Also let $\overline{G} = G/N$ and $\bar{x}$ be the image of an element x of G in S.

Lemma 3.6. *The order of finite nonabelian simple group S divides $(2p)!$.*

P r o o f. Since S is simple, it is normal in $\overline{G}$. Then $|\bar{x}^S|$ divides $|\bar{x}^{\overline{G}}|$ by Lemma 2.4. Also we know that $|\bar{x}^{\overline{G}}|$ divides $|x^G|$ by Lemma 2.4. Hence, for every x in G, $|\bar{x}^S|$ divides $|x^G|$. Since $N(G) = N(A_{2p})$, for every x in G, $|\bar{x}^S|$ divides $(2p)!$. On the other hand, by Lemma 2.6 for every $r \in \pi(S)$ there exists $\overline{y}$ in S such that $|S|_r = |\overline{y}^S|_r$. Consequently, for every $r \in \pi(S)$, $|S|_r$ divides $((2p)!)_r$, which is the desired conclusion and now, the result follows. $\square$

Lemma 3.7. *The prime number p does not divide $|N|$.*

P r o o f. On the contrary, suppose that p divides $|N|$. Put $N_0 = O_{p'}(N)$. We know that N_0 is a normal subgroup of G and we consider $\widetilde{G} = G/N_0$. In the following, if $A \leqslant G$, then $\tilde{A}$ is the image of A in $\widetilde{G}$. Let $\widetilde{T} = O_p(\widetilde{N})$. Then $\widetilde{T}$ is a nontrivial p-group and so $Z(\widetilde{T}) \neq 1$. Since $\widetilde{T}$ is characteristic in $\widetilde{N}$, $\widetilde{T}$ is normal in $\widetilde{G}$ and hence $Z(\widetilde{T})$ is normal in $\widetilde{G}$. Let $y \in G$ be of order l, where l is the greatest prime number in ϱ. Hence, the order of $\tilde{y}$, which is the image of y in $\widetilde{G}$, is equal to l. Since $Z(\widetilde{T})$ is abelian, $Z(\widetilde{T}) = C_{Z(\widetilde{T})}(\tilde{y}) \times [Z(\widetilde{T}), \tilde{y}]$ by Lemma 2.10. Consequently,

$$|[Z(\widetilde{T}), \tilde{y}]| = \frac{|Z(\widetilde{T})|}{|Z(\widetilde{T}) \cap C_{\widetilde{G}}(\tilde{y})|}.$$

Now we have that $|[Z(\widetilde{T}),\tilde{y}]|$ divides $|\widetilde{G} : C_{\widetilde{G}}(\tilde{y})|$ by Lemma 2.12. Therefore $|[Z(\widetilde{T}),\tilde{y}]|$ divides $|y^G|$ by Lemma 2.4. On the other hand, since $|[Z(\widetilde{T}),\tilde{y}]|$ divides $|Z(\widetilde{T})|$, $|[Z(\widetilde{T}),\tilde{y}]| = 1$, p or p^2. Furthermore, by Lemma 2.11, $|\tilde{y}| \mid |[Z(\widetilde{T}),\tilde{y}]| - 1$, which implies that $[Z(\widetilde{T}),\tilde{y}] = 1$. It follows that $Z(\widetilde{T}) = C_{Z(\widetilde{T})}(\tilde{y})$. Let $\widetilde{P}$ be a Sylow p-subgroup of $\widetilde{G}$ such that $Z(\widetilde{T}) \leqslant \widetilde{P}$. Since $Z(\widetilde{T}) \trianglelefteq \widetilde{G}$, $Z(\widetilde{T}) \cap Z(\widetilde{P}) \neq 1$. Let $\tilde{z} \in Z(\widetilde{T}) \cap Z(\widetilde{P})$. Since $\tilde{z} \in Z(\widetilde{P})$, $|\tilde{z}^{\widetilde{G}}|$ is a p'-number. Moreover, we have $\tilde{z} \in Z(\widetilde{T}) = C_{Z(\widetilde{T})}(\tilde{y})$, then $\tilde{y} \in C_{\widetilde{G}}(\tilde{z})$. Consequently, $|\tilde{z}^{\widetilde{G}}|$ is an l'-number. Let $z \in G$ such that $\tilde{z}$ is the image of z in $\widetilde{G}$. We can consider $p \nmid |z|$, hence $(|z|, |N_0|) = 1$, so $C_{\widetilde{G}}(\tilde{z}) = C_G(z)N_0/N_0$ by Lemma 2.4, which implies that

$$|z^G| = |\tilde{z}^{\widetilde{G}}| \times \frac{|N_0|}{|N_0 \cap C_G(z)|}.$$

Therefore $|z^G|$ is an l' and p'-number, which is a contradiction by Lemma 3.2. Consequently, p does not divide $|N|$. □

Lemma 3.8. *The simple group S is isomorphic to A_{2p}.*

P r o o f. By Lemmas 3.6, 3.7 and Theorem 2.9, we have $S = A_m$, where $l \leqslant m$ and l is the greatest prime number in ϱ. Therefore $A_m \leqslant \overline{G} \leqslant S_m$. So it is sufficient to show $m = 2p$. By Lemma 3.8, p does not divide $|N|$, so p^2 divides $|A_m|$, which implies that $m \geqslant 2p$. On the other hand, we know that $|A_m|$ divides $(2p)!$ by Lemma 3.7, so $m \leqslant 2p$. Consequently, $m = 2p$ as we desire. □

Lemma 3.9. *G/N is isomorphic with A_{2p}.*

P r o o f. We have $A_{2p} \leqslant \overline{G} = G/N \leqslant S_{2p}$ by Lemma 3.9. On the contrary, let $\overline{G} \cong S_{2p}$. In this case, $N(\overline{G}) = N(S_{2p})$. Let $a = (1\ 2\ \ldots\ p)(p{+}1\ p{+}2\ \ldots\ 2p) \in A_{2p}$. So $\alpha := |a^{A_{2p}}| = (2p)!/2p^2$ is a maximal number of $N(A_{2p})$. On the other hand, we have $b = (1\ 2\ \ldots\ 2p) \in S_{2p}$ and $|b^{S_{2p}}| = (2p)!/2p = p\alpha$. By Lemma 2.4, for every $c \in N(S_{2p})$ there exists $d \in N(A_{2p})$ such that c divides d. It follows that there exists $\beta \in N(A_{2p})$ such that $p\alpha$ divides β, which is a contradiction, since α is maximal in $N(A_{2p})$. □

Lemma 3.10. *N is trivial.*

P r o o f. We know that $p \in \pi(G) \setminus \pi(N)$ by Lemmas 2.6 and 3.8. Let $\overline{g}$ be the image of g in $\overline{G}$. Consider that $|g| = p$, then $|\overline{g}| = p$. We know that there exists an isomorphism from $\overline{G}$ to A_{2p}, say φ, by Lemma 3.10. Let $a = (1\ 2\ \ldots\ p)$ $(p+1\ p+2\ \ldots\ 2p)$ and $\varphi(\overline{g}) = a$. We have

$$\alpha := |\overline{g}^{\overline{G}}| = |a^{A_2 p}| = (2p)!/2p^2,$$

and α is the maximal number in $N(A_{2p})$ by Lemma 3.1, then α is maximal number in $N(G)$. In other words, $|\overline{g}^{\overline{G}}|$ is the maximal number in $N(G)$. On the other hand, $|\overline{g}^{\overline{G}}|$ divides $|g^G|$ by Lemma 2.4, so $|\overline{g}^{\overline{G}}| = |g^G|$. Hence, $|g^G|$ is the maximal number in $N(G)$. Since $(|N|, |g|) = 1$, $N \leqslant C_G(g)$ by Lemma 2.4. Let n be an arbitrary element in N, hence $(|n|, |g|) = 1$, then $C_G(ng) = C_G(n) \cap C_G(g)$, and so $|g^G|$ divides $|(ng)^G|$. Since $|g^G|$ is maximal, $|g^G| = |(ng)^G|$. Consequently, $C_G(g) \leqslant C_G(n)$, which implies that $n \in Z(C_G(g))$. Therefore $N \leqslant Z(C_G(g))$. On the other hand, since $\overline{G}$ is simple, $\overline{G} = \langle \overline{g}^{\overline{G}} \rangle$. Consequently, $G = \langle g^G \rangle N$, which implies that $N \leqslant Z(G)$. Therefore $N = 1$ as we desire. □

The proof of the assertion is an immediate consequence of above lemmas.

Similarly, if G is a finite group with trivial center such that $N(G) = N(A_{2p+1})$, then $G \cong A_{2p+1}$.

References

[1] *A. Abdollahi, H. Shahverdi*: Characterization of the alternating group by its non-commuting graph. J. Algebra *357* (2012), 203–207.

[2] *N. Ahanjideh*: On Thompson's conjecture for some finite simple groups. J. Algebra *344* (2011), 205–228.

[3] *N. Ahanjideh*: On the Thompson's conjecture on conjugacy classes sizes. Int. J. Algebra Comput. *23* (2013), 37–68.

[4] *S. H. Alavi, A. Daneshkhah*: A new characterization of alternating and symmetric groups. J. Appl. Math. Comput. *17* (2005), 245–258.

[5] *G. Chen*: On Thompson's conjecture. J. Algebra *185* (1996), 184–193.

[6] *I. B. Gorshkov*: Thompson's conjecture for simple groups with connected prime graph. Algebra Logic *51* (2012), 111–127; translated from Algebra Logika *51* (2012), 168–192. (In Russian.)

[7] *I. B. Gorshkov*: On Thompson's conjecture for alternating and symmetric groups of degree greater than 1361. Proc. Steklov Inst. Math. *293* (2016), S58–S65; translated from Tr. Inst. Mat. Mekh. (Ekaterinburg) *22* (2016), 44–51. (In Russian.)

[8] *I. B. Gorshkov*: Towards Thompson's conjecture for alternating and symmetric groups. J. Group Theory *19* (2016), 331–336.

[9] *I. M. Isaacs*: Finite Group Theory. Graduate Studies in Mathematics 92, American Mathematical Society, Providence, 2008.

[10] *A. Mahmoudifar, B. Khosravi*: On the characterizability of alternating groups by order and prime graph. Sib. Math. J. *56* (2015), 125–131; translated from Sib. Mat. Zh. *56* (2015), 149–157. (In Russian.)

[11] *V. D. Mazurov, E. I. Khukhro* eds.: The Kourovka Notebook. Unsolved Problems in Group Theory. Institute of Mathematics, Russian Academy of Sciences Siberian Division, Novosibirsk, 2010.

[12] *I. A. Vakula*: On the structure of finite groups isospectral to an alternating group. Proc. Steklov Inst. Math. *272* (2011), 271–286; translated from Tr. Inst. Mat. Mekh. (Ekaterinburg) *16* (2010), 45–60. (In Russian.)

[13] *A. V. Vasil'ev*: On Thompson's conjecture. Sib. Elektron. Mat. Izv. *6* (2009), 457–464.

[14] *M. Xu*: Thompson's conjecture for alternating group of degree 22. Front. Math. China *8* (2013), 1227–1236.

Authors' addresses: Azam Babai, Department of Mathematics, University of Qom, Alghadir Blvd., 37185-3766 Qom, Iran, e-mail: a_babai@aut.ac.ir; Ali Mahmoudifar, Department of Mathematics, Tehran-North Branch, Islamic Azad University, South Makran Street, 1651153311 Tehran, Iran, e-mail: a_mahmoodifar@iau-tnb.ac.ir.