Hokkaido Mathematical Journal Vol. 47 (2018) p. 25–32

The influence of order and conjugacy class length on the structure of finite groups

Alireza Khalili Asboei, Mohammad Reza Darafsheh and Reza Mohammadyari

(Received March 19, 2015; Revised September 25, 2015)

Abstract. Let $2^n+1 > 5$ be a prime number. In this article, we will show $G \cong C_n(2)$ if and only if $|G| = |C_n(2)|$ and G has a conjugacy class length $|C_n(2)|/(2^n+1)$. Furthermore, we will show Thompson's conjecture is valid under a weak condition for the symplectic groups $C_n(2)$.

Key words: Finite simple group, conjugacy class length, Thompson's conjecture.

1. Introduction

In this article, we investigate the possibility of characterizing $C_n(2)$ by simple conditions when $2^n + 1 > 5$ is a prime number. In fact, the main theorem of this paper is as follows:

Main Theorem *Let G be a group. Then $G \cong C_n(2)$ if and only if $|G| = |C_n(2)|$ and G has a conjugacy class length $|C_n(2)|/(2^n + 1)$, where $2^n + 1 = p > 5$ is a prime number.*

For related results, Chen et al. in [6] showed that the projective special linear groups $A_1(p)$ are recognizable by their order and one conjugacy class length, where p is a prime number. As a consequence of their result, they showed that Thompson's conjecture is valid for $A_1(p)$.

Put $N(G) = \{n : G \text{ has a conjugacy class of size } n\}$. The well-known Thompson's conjecture states that if L is a finite non-abelian simple group, G is a finite group with a trivial center, and $N(G) = N(L)$, then $L \cong G$. This conjecture is stated in [4], [5] in which the conjecture is verified for a few finite simple groups.

Similar characterizations have been found in [2] and [11] for the groups: sporadic simple groups, and simple K_3-groups (a finite simple group is called a simple K_n-group if its order is divisible by exactly n distinct primes) and

---

2010 Mathematics Subject Classification : 20D08, 20D60.

alternating group of prime degree.

The *prime graph* of a finite group G that is denoted by $\Gamma(G)$ is the graph whose vertices are the prime divisors of G and where prime p is defined to be adjacent to prime q ($\neq p$) if and only if G contains an element of order pq.

We denote by $\pi(G)$ the set of prime divisors of $|G|$. Let $t(G)$ be the number of connected components of $\Gamma(G)$ and let $\pi_1, \pi_2, \ldots, \pi_{t(G)}$ be the connected components of $\Gamma(G)$. If $2 \in \pi(G)$, then we always suppose $2 \in \pi_1$.

We can express $|G|$ as a product of integers $m_1, m_2, \ldots, m_{t(G)}$, where $\pi(m_i) = \pi_i$ for each i. The numbers m_i are called the order components of G. In particular, if m_i is odd, then we call it an odd component of G. Write $OC(G)$ for the set $\{m_1, m_2, \ldots, m_{t(G)}\}$ of order components of G and $T(G)$ for the set of connected components of G. According to the classification theorem of finite simple groups and [10], [13], [8], we can list the order components of finite simple groups with disconnected prime graphs as in Tables 1–4 in [5].

If n is an integer, then denote the r-part of n by $n_r = r^a$ or by $r^a \parallel n$, namely, $r^a \mid n$ but $r^{a+1} \nmid n$. If q is a prime, then we denote by $S_q(G)$ a Sylow q-subgroup of G, by $\mathrm{Syl}_q(G)$ the set of Sylow q-subgroups of G. The other notation and terminology in this paper are standard, and the reader is referred to [7] if necessary.

2. Preliminary Results

Definition 2.1 Let a and n be integers greater than 1. Then a Zsigmondy prime of $a^n - 1$ is a prime l such that $l \mid (a^n - 1)$ but $l \nmid (a^i - 1)$ for $1 \leq i < n$.

Lemma 2.1 ([14]) *If a and n are integers greater than* 1*, then there exists a Zsigmondy prime of $a^n - 1$, unless $(a, n) = (2, 6)$ or $n = 2$ and $a = 2^s - 1$ for some natural number s.*

Remark 2.1 If l is a Zsigmondy prime of $a^n - 1$, then Fermat's little theorem shows that $n \mid (l - 1)$. Put $Z_n(a) = \{l : l$ 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 2.2 ([12]) *The equation $p^m - q^n = 1$, where p and q are primes and m, $n > 1$ has only solution, namely, $3^2 - 2^3 = 1$.*

Lemma 2.3 ([9]) *Let q be a prime power which is not of the form $3^r 2^s \pm 1$,* *where* $r = 0,\ 1$ *and* $s \geq 1$. *Let* $M = C_n(q)$, *where* $n = 2^m (m \geq 2)$ *and* $OC_2 = (q^n+1)/(2, q+1)$. *If* $x \in \pi_1(M)$, $x^\alpha \mid |M|$ *and* $x^\alpha - 1 \equiv 0 \bmod OC_2$, *then* $x^\alpha = q^{2kn}$, *where* $1 \leq k \leq n/2$.

Corollary 2.1 *If* $x \in \pi(C_n(2)) - \{p\}$ *and* $x^\alpha - 1 \equiv 0$ *mod* p, *then either* $x^\alpha \nmid |C_n(2)|$ *or* $x = 2$.

Proof. It follows from Lemma 2.3. □

3. Proof of the Main Theorem

By [1, Corollary 2.3], $C_n(2)$ has one conjugacy class length $|C_n(2)|/(2^n+1)$. Note that since $2^n+1 > 5$ is prime, we deduce that n is a power of 2. Since the necessity of the theorem can be checked easily, we only need to prove the sufficiency.

By hypothesis, there exists an element x of order p in G such that $C_G(x) = \langle x \rangle$ and $C_G(x)$ is a Sylow p-subgroup of G. By the Sylow theorem, we have that $C_G(y) = \langle y \rangle$ for any element y in G of order p. So, $\{p\}$ is a prime graph component of G and $t(G) \geq 2$. In addition, p is the maximal prime divisor of $|G|$ and an odd order component of G.

We are going to prove the main theorem in the following steps:

Step 1. G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H and G/K are π_1-groups, K/H is a non-abelian simple group and H is a nilpotent group.

Let $g \in G$ be an element of order p, then $C_G(g) = \langle g \rangle$. Set $H = O_{p'}(G)$ (the largest normal p'-subgroup of G). Then H is a nilpotent group since g acts on H fixed point freely. Let K be a normal subgroup of G such that K/H is a minimal normal subgroup of G/H. Then K/H is a direct product of copies of some simple group. Since $p \mid |K/H|$ and $p^2 \nmid |K/H|$, K/H is a simple group. Since $\langle g \rangle$ is a Sylow p-subgroup of K, $G = N_G(\langle g \rangle)K$ by the Frattini argument and so $|G/K|$ divides $p-1$.

If $|K/H| = p$, then by Lemma 2.1, there is a prime $r \in Z_{n-1}(2) \cap \pi(G)$ and so $|C_n(2)|_r = |2^{n-1} - 1|_r \leq |G|_r$. Since $\pi(G) = \pi(K) \cup \pi(H) = \pi_1(G) \cup \pi_2(G)$, then $r \in (H)$. Since H is nilpotent, a Sylow r-subgroup is normal in G. It follows that the Sylow p-subgroup of G acts fixed point freely on the set of elements of order r and so $p \mid |C_n(2)|_r - 1$. Thus $p \leq |C_n(2)|_r \leq 2^{n-1} - 1 < p$, a contradiction. Therefore G has normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that K/H is a non-abelian simple group and p is an odd order component of K/H.

Step 2. $\pi(H) \subseteq \{2\}$.

Let $r \in \pi(H)$. Then $r \neq p$ and since H is nilpotent, we deduce that $S_r(H) \trianglelefteq G$ and hence, $S_p(G)$ acts fixed point freely on $S_r(H) - \{1\}$. Thus $p \mid |S_r(H)| - 1$. If $r \neq 2$, then $|S_r(H)| \mid |C_n(2)|_r$ and hence, Corollary 2.1 leads us to get a contradiction. Thus $r = 2$, as claimed.

According to the classification theorem of finite simple groups and the results in Tables 1–4 in [5], K/H is an alternating group, sporadic group or simple group of Lie type.

Step 3. K/H is not a sporadic simple group.

Suppose that K/H is a sporadic simple group. Since one of the odd order components of K/H is $p = 2^n + 1$, we get a contradiction by considering the odd order components of sporadic simple groups.

Step 4. K/H can not be an alternating group A_m, where $m \geq 5$.

If $K/H \cong A_m$ with $m \geq 5$, then since $p \in \pi(K/H)$, $m \geq 2^n + 1$. Thus there is a prime $u \in \pi(A_m) \subseteq \pi(G)$ such that $(p-1)/2 < u < p$. Since $|G| = |C_n(2)|$, there exists $t \in \{2i, i : 1 < i < n-1\} \cup \{n\}$ such that $u \in Z_t(2)$. But $u > (2^n - 1 + 1)/2 = 2^{n-1}$ and so $u = 2^{n-1} + 1$ or $2^n - 1$. But n is a power of 2 and hence, $3 \mid 2^{n-1} + 1$ and $2^n - 1$. Thus $3 \mid u$. This implies that $u = 3$ ad hence, $n = 2$, which is a contradiction.

Step 5. $K/H \cong C_n(2)$.

By Steps 3 and 4, and the classification theorem of finite simple groups, K/H is a simple group of Lie type such that $t(K/H) \geq 2$ and $p \in OC(K/H)$. Thus K/H is isomorphic to one of the group of Lie type (in the following cases, r is an odd prime number):

Case 1. Let $t(K/H) = 2$. Then $OC_2(K/H) = 2^n + 1$. Then we have:

1.1. If $K/H \cong C_{n'}(q)$, where $n' = 2^u > 2$, then $(q^{n'} + 1)/(2, q-1) = 2^n + 1$. If q is odd, then $q^{n'} = 2^{n+1} + 1$, which contradicts Lemma 2.2. Thus $q = 2^t$ and hence, $q^{n'} = 2^n$. But $p \in Z_{2n}(2)$ and $p \in Z_{2n't}(2)$. Thus Remark 2.1 forces $n't = n$. We claim that $t = 1$. If not, then $Z_{n-1}(2) \cap \pi(K/H) = \emptyset$. But Lemma 2.1 forces $Z_{n-1}(2) \neq \emptyset$ and hence since $|G| = |C_n(2)|$, $\pi(G)$ contains a prime $r \in Z_{n-1}(2)$. Since $r \nmid |\mathrm{Out}(K/H)|$ and $G/K \lesssim \mathrm{Out}(K/H)$, we deduce that $r \mid |H|$. Thus Step 2 shows that $r = 2$, which is a contradiction. Thus $t = 1$ and hence, $K/H \cong C_n(2)$.

Arguing as above if $K/H \cong B_{n'}(q)$, where $n' = 2^u \geq 4$, then $n' = n$ and $q = 2$. Thus $K/H \cong B_n(2) = C_n(2)$.

1.2. If $K/H \cong C_r(3)$ or $B_r(3)$, then $(3^r - 1)/2 = 2^{n+1}$. Thus $2^n + 1 = 3^r - 3$, which is a contradiction. The same reasoning rules out the case when $K/H \cong D_r(3)$ or $D_{r+1}(3)$.

1.3. If $K/H \cong C_r(2)$, then $2^r - 1 = 2^n + 1$ and hence, $2^r = 2^n + 2$, which is a contradiction. The same reasoning rules out the case when $K/H \cong D_r(2)$ or $D_{r+1}(2)$.

1.4. If $K/H \cong D_r(5)$, where $r \geq 5$, then $(5^r - 1)/4 = (2^n + 1)$. Thus $5^r - 5 = 2^{n+2}$, which is contradiction.

1.5. If $K/H \cong^2 D_{n'}(3)$, where $9 \leq n' = 2^m + 1$ and n' is not prime, then $(3^{n'} - 1)/2 = 2^{n+1}$ and hence, $3^{n'} - 1 = 2^{n+1} + 1$. Thus Lemma 2.2 forces $n + 1 = 3$, which is a contradiction.

1.6. If $K/H \cong^2 D_{n'}(2)$, where $n' = 2^m + 1 \geq 5$, then $2^{n'-1} + 1 = 2^n + 1$ and hence, $n' - 1 = n$. Thus $K/H \cong^2 D_{n+1}(2)$. Then $Z_{n+1}(2) \subseteq \pi(K/H)$ and hence, $Z_{n+1}(2) \subseteq \pi(G) = \pi(C_n(2))$, which is a contradiction.
If $K/H \cong^2 D_{n'}(q)$, where $n' = 2^u \geq 4$, then $n' = n$ and $q = 2$. Similarly we can rules out this case.

1.7. If $K/H \cong^2 D_r(3)$, where $5 \leq r \neq 2^m + 1$, then $(3^r + 1)/4 = 2^n + 1$ and hence, $3^r = 2^{n+2} + 3$, which is a contradiction.

1.8. If $K/H \cong G_2(q)$, where $2 < q \equiv \varepsilon \bmod 3$ and $\varepsilon = \pm 1$, then $q^2 - \varepsilon q + 1 = 2^n + 1$. Thus $q(q - \varepsilon) = 2^n$, which is impossible. The same reasoning rules out the case when $K/H \cong F_4(q)$, where q is odd.

1.9. If $K/H \cong^2 F_4(2)'$, then since $|^2F_4(2)| = 2^{11}.3^3.5^2.13$, $2^n + 1 = 13$, a contradiction. Also we can rule out $K/H \cong {}^2A_3(2)$.

1.10. Let $K/H \cong A_{r-1}(q)$, where $(r, q) \neq (3, 2)$, $(3, 4)$. Since $(q^r - 1)/((r, q - 1)(q - 1)) = p$, $p \in Z_r(q)$ and hence, Remark 2.1 shows that $r \mid p - 1 = 2^n$. Thus $r = 2$, which is a contradiction. The same reasoning rules out the case when $K/H \cong^2 A_{r-1}(q)$.

1.11. Let $K/H \cong A_r(q)$, where $(q-1) \mid (r+1)$. Since $(q^r - 1)/(r, q - 1) = p$, $p \in Z_r(q)$ and hence, Remark 2.1 shows that $r \mid p - 1 = 2^n$. Thus $r = 2$, which is a contradiction. The same reasoning rules out the case when $(q + 1) \mid (r + 1)$, $(r, q) \neq (3, 3)$, $(5, 2)$ and $K/H \cong^2 A_r(q)$.

1.12. If $K/H \cong E_6(q)$, where $q = u^\alpha$, then $(q^6 + q^3 + 1)/(3, q - 1) = p$. Thus $p \in Z_6(q)$ and hence, Remark 2.1 shows that $6 \mid p - 1 = 2^n$, which is a contradiction. The same reasoning rules out the case when $K/H \cong^2 E_6(q)$, where $q > 2$.

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

2.1. If $K/H \cong A_1(q)$, where $4 \mid q+1$, then $(q-1)/2 = 2^n+1$ or $q = 2^n+1$. If $q = 2^n + 1$, then $q + 1 = 2^n + 2$ and hence, $4 \nmid q + 1$, which is a contradiction. If $(q-1)/2 = p$, then $q \equiv -1 \bmod 4$. Let $q = u^\alpha$, where u is a prime. Thus $p \in Z_\alpha(u)$ and hence, Remark 2.1 shows that $\alpha \mid p - 1 = 2^n$. So $\alpha = 2^t$ and hence, $q = u^\alpha \equiv 1 \bmod 4$, which is a contradiction.

2.2. If $K/H \cong A_1(q)$, where $4 \mid q + 1$, then $q = 2^n + 1$ or $(q + 1)/2 = p$.
- If $q = 2^n + 1$, then $q = p$ and hence, $|K/H| = p(p^2 - 1)/2 = 2^n p(2^{n-1} + 1)$ and since $G/K \lesssim \mathrm{Out}(K/H) \cong Z_2$, we deduce that $Z_n(2) \subseteq \pi(H)$, which is a contradiction with Step 2.
- If $(q + 1)/2 = p$, then $q = 2^{n-1} + 1$. Thus $3 \mid q$ and hence, $3^\alpha = 2^{n+1} + 1$, which is a contradiction with Lemma 2.2

2.3. If $K/H \cong A_1(q)$, where $q > 2$ and q is even, then $p \in \{q-1, q+1\}$. If $q - 1 = 2^n + 1$, then $q = 2(2^{n-1} + 1)$, which is a contradiction. If $q+1 = 2^n+1$, then $q = 2^n$ and hence, $|K/H| = 2^n(2^n-1)(2^n+1)$. But $G/K \lesssim \mathrm{Out}(K/H) \cong Z_n$, so $Z_{n-1}(2) \subseteq \pi(H)$, which is a contradiction with Step 2.

2.4. If $K/H \cong {}^2A_5(2)$ or $A_2(2)$, then $|K/H| = 2^{15}.3^6.7.11$ or $8.3.7$. Clearly, $2^n + 1 \neq 11$ and $2^n + 1 \neq 7$, which is a contradiction.

2.5. If $K/H \cong {}^2D_r(3)$, where $r = 2^t + 1 \geq 5$, then $(3^r + 1)/4 = 2^n + 1$ or $(3^r - 1)/2 = 2^n + 1$. If $(3^r + 1)/4 = 2^n + 1$, then $3^r = 2^{n+2} + 3$, which is a contradiction. If $(3^r - 1)/2 = 2^n + 1$, then $2^{n+1} + 1 = 3^{r-1}$, which is contradiction with Lemma 2.2.

2.6. If $K/H \cong G_2(q)$, where $q \equiv 0 \bmod 3$. Then $q^2 - q + 1 = 2^n + 1$ or $q^2 + q + 1 = 2^n + 1$ and hence, $q(q \pm 1) = 2^n$, which is impossible. Similarly we can rule out $K/H = {}^2G_2(q)$.

2.7. If $K/H \cong F_4(q)$, where q is even. Then $q^4 + 1 = 2^n + 1$ or $q^4 - q^2 + 1 = 2^n + 1$. If $q^4 - q^2 + 1 = 2^n + 1$, $q^2(q^2 - 1) = 2^n$, which is impossible. If $q^4 + 1 = 2^n + 1$, then $q^4 = 2^n$, so $(q^{12} - 1) = (2^{3n} - 1) \mid |K/H|$ and hence, $Z_{3n}(2) \subseteq \pi(G) = \pi(C_n(2))$, which is a contradiction again.

2.8. If $K/H \cong {}^2F_4(q)$, where $q = 2^{2t} + 1 > 2$. Then $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1 = 2^n + 1$ or $q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1 = 2^n + 1$. Thus $2^n + 1 = 2^{2(2t+1)} + \varepsilon 2^{3t+2} + 2^{2t+2} + \varepsilon 2^{t+1} + 1$, where $\varepsilon = \pm 1$ and hence, $2^n = 2^{t+1}(2^{3t+1} + \varepsilon 2^{2t+1} + 2^t + \varepsilon)$, which is a contradiction.

2.9. If $K/H \cong E_7(2)$, then $2^n + 1 \in \{73, 127\}$, which is impossible.

2.10. If $K/H \cong E_7(3)$, then $2^n + 1 \in \{757, 1093\}$, which is impossible.

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

3.1. If $K/H \cong A_2(4)$ or ${}^2E_6(2)$, then $2^n + 1 = 7$ or $2^n + 1 = 19$, which is impossible.
3.2. If $K/H \cong^2 B_2(q)$, where $q = 2^{2t} + 1$ and $t \geq 1$. Then $2^n + 1 \in \{q - 1, q \pm \sqrt{2q} + 1\}$. If $q - 1 = 2^n + 1$, then $2^{2t} + 1 = 2^n + 2$ and if $q \pm \sqrt{2q} + 1 = 2^n + 1$, then $2^{t+1}(2^t \pm 1) = 2^n$, which are impossible.
3.3. If $K/H \cong E_8(q)$, then $2^n + 1 \in \{q^8 - q^7 + q^5 - q^4 + q^3 - q + 1,\ q^8 + q^7 - q^5 - q^4 - q^3 + q + 1,\ q^8 - q^6 + q^4 - q^2 + 1, q^8 - q^4 + 1\}$. Thus $q^t = 2^n$, where $t > 1$ is a natural number such that $(t, q) = 1$, which is a contradiction.

The above cases show that $K/H \cong C_n(2)$.

Now since $|G| = |C_n(2)|$, $H = 1$ and $K = G \cong C_n(2)$. The main theorem is proved.

Corollary *Thompson's conjecture holds for the simple groups* $C_n(2)$, *where* $2^n + 1 > 5$ *prime is a prime number.*

Proof. Let G be a group with trivial central and $N(G) = N(C_n(2))$. Then it is proved in [3, Lemma 1.4] that $|G| = |C_n(2)|$. Hence, the corollary follows from the main theorem. □

References

[1] Ahanjideh N., *Thompson's conjecture for some finite simple groups with connected prime graph.* Algebra Logic. **6** (2013), 451–478.

[2] Asboei K. A. and Mohammadyari R., *Recognizing alternating groups by their order and one conjugacy class length.* J. Algebra. Appl. **15** (2016), doi:10.1142/S0219498816500213.

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

[4] Chen G. Y., *Further reflections on Thompson's conjecture.* J. Algebra. **218** (1999), 276–285.

[5] Chen G. Y., *A new characterization of sporadic simple groups.* Algebra Colloquium. **3** (1996), 49–58.

[6] Chen Y. and Chen G. Y., *Recognizing* $A_1(p)$ *by its order and one special conjugacy class size.* J. Inequal. Appl. (2012), doi:10.1186/1029-242X-2012-310.

[7] Conway J. H., Curtis R. T., Norton S. P. and Wilson R. A., *Atlas of finite groups*, Clarendon, Oxford, 1985.

[8] Iiyori N. and Yamaki H., *Prime graph components of the simple groups of Lie type over the field of even characteristic.* J. Algebra. **155** (1993), 335–343.

[9] Khosravi A. and Khosravi B., *r-Recognizability of* $B_n(q)$ *and* $C_n(q)$*, where* $n = 2^m \geq 4$. J. Pure Appli. Algebra. **199** (2005), 149–165.

[10] Kondtratev A. S. and Mazurove V. D., *Recognition Of Alternating groups of prime degree from their element orders.* Siberian Mathematical Journal. **41** (2000), 294–302.

[11] Li J. B., *Finite groups with special conjugacy class sizes or generalized permutable subgroups*, PhD thesis, Southwest University, Chongqing, 2012.

[12] Ribenboim R., *Classical Theory of Algebraic Numbers*, Springer, New York, 2001.

[13] Williams J. S., *Prime graph components of finite groups.* J. Algebra. **69** (1981), 487–513.

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

Alireza Khalili Asboei
Department of Mathematics
Farhangian University
Tehran, Iran
E-mail: khaliliasbo@yahoo.com

Mohammad Reza Darafsheh
School of Mathematics
Statistics and Computer Science
University of Tehran
Tehran, Iran

Reza Mohammadyari
Department of Mathematics
Buinzahra Branch
Islamic Azad University
Buin Zahra, Iran