DOI: 10.28919/ejma.2023.3.25

Eur. J. Math. Appl. (2023)3:25
URL: http://ejma.euap.org

ALMOST SIMPLE GROUPS WITH MORE THAN ONE HALF OF THE NUMBER OF CYCLIC SUBGROUPS

WEIDONG XU, RULIN SHEN*

Abstract. Let G be a finite group, $c(G)$ the number of cyclic subgroups of G, and $\alpha(G)$ the ratio of the number of cyclic subgroups of G to the order of the group, i.e.$\alpha(G) = c(G)/|G|$. A group G called an almost simple group if there exists a finite non-abelian simple group such that $S \leq G \leq Aut(S)$. In this paper, we prove that if G is an almost simple group, then $\alpha(G) \geq 1/2$ if and only if $G \cong A_5, S_5, S_6$.

1. Introduction

In this paper all groups are finite. Define $c(G)$ be the number of cyclic subgroups of G and let $\alpha(G)$ be the ratio of the number of cyclic subgroups of G to the order of the group, i.e.$\alpha(G) = c(G)/|G|$. In recent years, numerous academics have explored the correlation between $\alpha(G)$ and finite group structure, and many results have been achieved. In 2018, Garonzi and Lima have classified the groups with $\alpha(G) > 3/4$ (see [1]). In 2020, Gao and Shen have classified the groups with $\alpha(G) = 3/4$ (see [2]). More recently, Cayley continued to study the classification of groups for a given value of $\alpha(G)$ (see [3]). In this paper, we restrict G to an almost simple group, that is $S \leq G \leq Aut(S)$, where S is a finite non-abelian simple group. Our focus is the classification of almost simple groups G, satisfying property $\alpha(G) > 1/2$.

Theorem 1.1. *Let G be an almost simple group. Then $\alpha(G) > 1/2$ if and only if $G \cong A_5, S_5, S_6$.*

2. Some Lemmas

We define $I(G) = \{x \in G \mid x^2 = 1\}$, $J(G) = \{x \in G \mid o(x) \neq 1, 2, 3, 4, 6\}$ and denote $k(G)$ the number of conjugacy classes of the group G. For the proof of the theorem, we also give the following necessary lemmas.

Lemma 2.1. *([1]) Let G be a finite group, then $c(G) = \sum_{x \in G} \frac{1}{\varphi(o(x))}$, where $o(x)$ is the order of the element x and $\varphi(o(x))$ is Euler function of $o(x)$.*

Department of Mathematics, Hubei Minzu University, Enshi, Hubei Province, 445000, P. R. China

*Corresponding author

E-mail address: oshenrulin@hotmail.com.
Key words and phrases. finite groups; r-singular elements; simple groups.

Received 18/10/2023.

Project supported by the NSF of China (Grant No. 12161035).

Lemma 2.2. *Let G be a finite group. If $|I(G)| < \frac{1}{2}|J(G)|$, then $\alpha(G) < \frac{1}{2}$.*

Proof. For any element y of $I(G)$, we have $\varphi(o(y)) = 1$. Let t is any element of $J(G)$, then $\varphi(o(t)) \geq 4$. But for any remaining element z, we have $\varphi(o(z)) = 2$. Hence $c(G) = \sum\limits_{x\in G} \frac{1}{\varphi(o(x))} = \sum\limits_{y\in I(G)} \frac{1}{\varphi(o(y))} + \sum\limits_{t\in J(G)} \frac{1}{\varphi(o(t))} + \sum\limits_{z\in G-I(G)-J(G)} \frac{1}{\varphi(o(z))} \leq |I(G)| + \frac{1}{4}|J(G)| + \frac{1}{2}(|G| - |I(G)| - |J(G)|) = \frac{1}{2}|I(G)| - \frac{1}{4}|J(G)| + \frac{1}{2}|G| < \frac{1}{2}|G|$. thus $\alpha(G) = \frac{c(G)}{|G|} < \frac{1}{2}$. □

Lemma 2.3. *([1, Lemma 1]) Let G be a finite group. Then $|I(G)|^2 \leq k(G) \cdot |G|$.*

Lemma 2.4. *([4, Theorem 2]) If G is any subgroup of S_n, then $k(G) \leq 2^{n-1}$, where n is a positive integer.*

Lemma 2.5. *([5, Page 314 Theorem 1.1]) Suppose that G is A_n with $n \geq 5$. If $n = 6$, then $Aut(A_6)$ is isomorphic to an extension of S_6 by the cyclic of order 2. If $n \neq 6$, then $Aut(A_n)$ is isomorphic to S_n.*

Lemma 2.6. *([4, Lemma 2.1]) If G is a simple group of Lie type in characteristic p, then either*

(1) $k(G) < |G|_p$, that is the order of Sylow p-subgroup of G, or

(2) $G = L_2(q)$, q even (in which case $k(G) = q+1$), or $G = L_2(5)$ (in which case $k(G) = 5$).

Lemma 2.7. *([4, Theorem 1]) Let S be a finite simple group of Lie type over $\mathbb{F}_q$. If the Lie rank of group S is equal to l, then $k(S) \leq (6q)^l$.*

Lemma 2.8. *([6, Lemma 1]) Let G be a finite group, for every normal subgroup N of G, we have $k(G) \leq k(G/N) \cdot k(N)$.*

Lemma 2.9. *Let S be a finite Lie type simple group, then there exist self-centred cyclic subgroups T(see Table 1), satisfying $|T| \geq 5$, $|T| \neq 6$ and $|S| > 4 \cdot |T|^2 \cdot (6q)^l \cdot |Out(S)|^2$, except for the following cases.*

(i) $A_1(q), (q \geq 4)$.

(ii) $A_2(q), q = 2^f, 1 \leq f \leq 8, f = 10; q = 3^f, 1 \leq f \leq 4; q = 5^f, 1 \leq f \leq 2; q = 7^f, 1 \leq f \leq 3; q = 11^f, 1 \leq f \leq 2; q = 13^f, 1 \leq f \leq 2; q = 17, 19, 23, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109$.

(iii) $A_3(q), q = 2, 3, 4, 5, 9; A_4(2); {}^2A_2(q), q = 3, 4, 5, 7, 8, 11, 32; {}^2A_3(q), q = 2, 3;$
$C_2(q), q = 3, 4, 5, 8; D_4(2); {}^2F_4(2)'; {}^2B_2(8)$.

Table 1. **Related Lie type simple groups**

S	$Lie\, rank\, l$	$\lvert Out(S)\rvert$	$\lvert T\rvert\,(\geq 5\; and \neq 6)$
$A_n(q), n \geq 2$	n	$2(n+1, q-1)f$	$(q^{n+1}-1)(q-1)^{-1}$
$^2A_n(q), n \geq 2$	$\left[\frac{n+1}{2}\right]$	$2(n+1, q+1)f$	$(q^{n+1}+(-1)^n)(q+1)^{-1}$
$B_n(q), n \geq 2, q\; odd$	n	$2f$	q^n+1
$C_n(q), n \geq 2$	n	$2f, n=2$ $(2, q-1)f, n \geq 3$	q^n+1
$D_n(q), n \geq 4$	n	$6(4, q^n-1)f, n=4$ $2(4, q^n-1)f, n \neq 4$	q^n-1
$^2D_n(q), n \geq 4$	$n-1$	$2(4, q^n+1)f$	q^n+1
$^2F_4(q), q=2^{2n+1}$	2	f	$q^2+(q+1)(\sqrt{2q}+1)$
$F_4(q)$	4	$(2, p)f$	q^4+1
$^3D_4(q)$	2	$3f$	$(q^3-1)(q+1)$
$^2G_2(q), q=3^{2n+1}$	1	f	$q+\sqrt{3q}+1$
$E_6(q)$	6	$2(3, q-1)f$	$\Phi_{12}(q)\Phi_3(q)$
$^2E_6(q)$	4	$2(3, q+1)f$	$\Phi_{12}(q)\Phi_6(q)$
$E_7(q)$	7	$(2, q-1)f$	$\Phi_{12}(q)(q^3+1)$
$E_8(q)$	8	f	$\Phi_{30}(q)$
$G_2(q)$	2	$2f, p=3$ $f, p \neq 3$	$\Phi_3(q)$
$^2B_2(q)$, $q=2^{2n+1}, n \geq 2$	1	f	$q+\sqrt{2q}+1$

where $q=p^f$, $f \in N$, p is prime, $\Phi_n(q)$ denotes the cyclotomic polynomial(see [5] and [7]).

Proof. The order of the outer automorphism group of simple groups of Lie type is given by [5], and the order of the self-centralized cyclic subgroup T is given in [7]. We list in Table 1. It is easy to compute that if S is not in (i),(ii),(iii), then S satisfies $|S| > 4 \cdot |T|^2 \cdot (6q)^l \cdot |Out(S)|^2$, $|T| \geq 5$ and $|T| \neq 6$. □

3. Proof of Theorem

Proof. Suppose G is an almost simple group, that is $S \leq G \leq Aut(S)$, where S is a finite non-abelian simple group. If $G \cong A_5, S_5, S_6$, then $\alpha(A_5) = \frac{8}{15}, \alpha(S_5) = \frac{67}{120}, \alpha(S_6) = \frac{181}{360}$, all of which have $\alpha(G) \geq \frac{1}{2}$. conversely we assume $\alpha(G) \geq \frac{1}{2}$, we need to prove $G \cong A_5, S_5, S_6$.

Firstly, suppose S is an Alternating group A_n with $n \geq 5$. According to the Atlas group table (see [8]), G is isomorphic to A_5, S_5 or S_6 if n=5,6,7 and $\alpha(G) \geq \frac{1}{2}$. When $n \geq 8$, it follows from Lemma 2.5 that $Aut(A_n)$ is isomorphic to S_n, and hence G is isomorphic to A_n or S_n. Then, by Lemma 2.3 and Lemma 2.4, we obtain $|I(S_n)| \leq \sqrt{2^{n-1} \cdot (n!)}$. Next, if n is even, then $J(A_n) \supseteq \{x \in A_n \mid x \text{ is a } (n-1)\text{-cycle } \}$, and hence $|J(A_n)| \geq \frac{n!}{n-1}$. But $\sqrt{2^{n-1} \cdot (n!)} < \frac{1}{2} \cdot \frac{n!}{n-1}$, and hence $|I(S_n)| < \frac{1}{2} |J(A_n)|$. If n is odd, then $J(A_n) \supseteq \{x \in A_n \mid x \text{ is a } n\text{-cycle } \}$, and hence $|J(A_n)| \geq \frac{n!}{n}$. But $\sqrt{2^{n-1} \cdot (n!)} < \frac{1}{2} \cdot \frac{n!}{n}$, and hence $|I(S_n)| < \frac{1}{2} |J(A_n)|$. Both result in $|I(G)| < \frac{1}{2} |J(G)|$. Thus, if the group S is an Alternating group, it follows from Lemma 2.2 that the group G is isomorphic to A_5, S_5 *or* S_6.

Secondly, suppose S is a simple group of Lie type. When S is not a group of items (i),(ii),(iii) in Lemma 2.9, there exists a self-centred cyclic subgroup T, satisfying $|T| \geq 5$, $|T| \neq 6$ and $|S| > 4 \cdot |T|^2 \cdot (6q)^l \cdot |Out(S)|^2$. We assume that $T = \langle t \rangle$, of course, has $C_S(t) = T$. Since f $\left|t^S\right| = |S : C_S(t)| = |S| / |T|$, we have $|J(S)| \geq |S| / |T|$. By Lemmas 2.3, 2.7 and 2.8 we get

$$\begin{aligned}\frac{|S|}{2|T|} &> \sqrt{(6q)^l \cdot |S| \cdot |Out(S)|^2} \\ &\geq \sqrt{k(S) \cdot |S| \cdot k(Out(S)) \cdot |Out(S)|} \\ &\geq \sqrt{k(Aut(S)) \cdot |Aut(S)|} \\ &\geq |I(Aut(S))| .\end{aligned}$$

Thus S satisfies $|I(Aut(S))| < \frac{1}{2} |J(S)|$, and because $S \leq G \leq Aut(S)$, and hence $|I(G)| \leq |I(Aut(S))| < \frac{1}{2} |J(S)| \leq \frac{1}{2} |J(G)|$. Again, by Lemma 2.2, it follows that $\alpha(G) < \frac{1}{2}$. Below, when S is a group in Lemma 2.9(i),(ii),(iii), we discuss three cases.

Case 1. $S \cong A_1(q), (q \geq 4)$.

When $q = 4, 5$, S is isomorphic to A_5. When $q = 9$, S is isomorphic to A_6. These are discussed and not repeated. For $q = 7, 8, 11, 13, 16$, $|I(G)| < \frac{1}{2} |J(G)|$ is easily calculated from the Atlas table. The case of $q \geq 17$ is discussed below. Since $\varphi(d)$ denotes the value of the Euler function of an element of order d in $A_1(q)$ and $q^2 - 1$ denotes the number of elements of order p in $A_1(q)$ (see Lemma 2.2.9 in [9]), we have $|J(S)| \geq |S| - 4q^2 - 3q$ and $|I(Aut(S))| < \frac{1}{4} q(q^2 - 8q - 7)$ below. In fact, by Lemma 2.2.9 in [9], we know that the number of 2nd order elements is at most $q^2 - 1$, and since $\varphi(d) = 2, d = 3, 4, 6$, it is possible to take that 3rd, 4th, and 6th order elements exist and that the number of elements is taken to be $q(q + 1)$, and thus that $|J(S)| \geq |S| - 4q^2 - 3q$. By Lemma 2.6, we have $|I(Aut(S))| \leq \sqrt{(q + 1) \cdot (2, q - 1)^2 \cdot f^2 \cdot |S|} < \frac{1}{4} q(q^2 - 8q - 7)$, and because of $\frac{1}{4} q(q^2 - 8q - 7) \leq \frac{1}{2}(|S| - 4q^2 - 3q)$, thus $|I(Aut(S))| < \frac{1}{2} |J(S)|$.

Case 2. $S \cong A_2(q)$, *where* $q = 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^{10}, 3, 3^2, 3^3, 3^4, 5, 5^2, 7, 7^2,$ $7^3, 11, 11^2, 13, 13^2, 17, 19, 23, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109$.

When $q = 2, 3, 4, 5, 7, 8, 9, 11$, it is easy to verify $|I(G)| < \frac{1}{2} |J(G)|$ according to the Atlas group table. When $q = 17$, then there are elements of order 307, and according to lemma 3.1 in [10] the number of elements of order 307 is 2309188608, so $|J(S)| \geq 2309188608$. Substituting Lemma 2.6, it is clear that $|I(Aut(S))| < \frac{1}{2} \cdot 2309188608 \leq \frac{1}{2} |J(S)|$. When $q = 31$, there is an element of order 331, again using Lemma 2.6 and Lemma 3.1 in [10], which proves that there is $|I(Aut(S))| < \frac{1}{2} |J(S)|$. For $q \neq 2, 3, 4, 5, 7, 8, 9, 11, 17, 31$. By Theorem 5.2.14 in [11], there exists a primitive prime divisor $r (r \geq 5)$ in $|S|$, written $|S|_{r'} = |S| / |S|_r$, where $|S|_r$ is Sylow r- subgroup order of the group S. Clearly $\{x \in S \mid r|o(x)\}$ is a non-empty subset of the group S. By Theorem 3 of [12], there exists $|S|_{r'}$ which divides $\{x \in S \mid r|o(x)\}$, so $|J(S)| \geq |\{x \in S \mid r|o(x)\}| \geq |S|_{r'} = |S|/r$. Then by Lemma 2.6 and the order of the group S, it follows that there exists a primitive prime divisor r such that $|I(Aut(S))| < \sqrt{q^3 \cdot 4 \cdot (3, q-1)^2 \cdot f^2 \cdot |S|} < \frac{|S|}{2r} \leq \frac{1}{2}|J(S)|$, where r is in the order of q-values corresponding to the order of $7, 7, 5, 43, 13, 41, 7, 41, 13, 19, 43, 61, 7, 5, 5, 7, 19, 11, 31, 17, 37, 5, 3169, 13, 11$.

Case 3. $S \cong A_3(q), q = 2, 3, 4, 5, 9; A_4(2);\ ^2A_2(q), q = 3, 4, 5, 7, 8, 11, 32;\ ^2A_3(q), q = 2, 3; C_2(q), q = 3, 4, 5, 8;\ D_4(2);\ ^2F_4(2)';\ ^2B_2(8)$.

According to the Atlas group table, if $S \cong A_3(2), A_3(3), A_4(2), ^2A_2(3), ^2A_2(4), ^2A_2(5), ^2A_2(7), ^2A_2(8), ^2A_2(11), ^2A_3(2), ^2A_3(3), C_2(3), C_2(4), C_2(5), D_4(2), ^2F_4(2)', ^2B_2(8)$, then $|I(G)| < \frac{1}{2}|J(G)|$ is obtained. If $S \cong A_3(4), A_3(5), A_3(9), ^2A_2(32), C_2(8)$, according to the order of the group S, there exist r is $7, 13, 7, 5, 31$. Again, by Lemma 2.6 and Theorem 3 of [12], it is verified that there exists $|I(Aut(S))| < \frac{1}{2}|J(S)|$.

For $|I(Aut(S))| < \frac{1}{2}|J(S)|$ appears in the above three cases due to $S \leq G \leq Aut(S)$, and hence $|I(G)| \leq |I(Aut(S))| < \frac{1}{2}|J(S)| \leq \frac{1}{2}|J(G)|$. Thus, if S is a group not isomorphic to A_5, A_6 in (i),(ii),(iii), by Lemma 2.2, both yield $\alpha(G) < \frac{1}{2}$. Thus, if S is a simple group of Lie type, $G \cong A_5, S_5, S_6$.

Finally, if the group S is a sporadic simple group according to the Atlas group table, we check that we have $|I(G)| < \frac{1}{2}|J(G)|$. According to Lemma 2.2, we have $\alpha(G) < \frac{1}{2}$. In summary, we have $G \cong A_5, S_5, S_6$, if $\alpha(G) \geq \frac{1}{2}$. The proof is complete. □

References

[1] M. Garonzi, I. Lima, On the number of cyclic subgroups of a finite group, Bull. Brazil. Math. Soc. 49 (2018), 515–530.

[2] X. Gao, R. Shen, Finite groups with many cyclic subgroups, Indian J. Pure Appl. Math. 54 (2023), 485–498.

[3] J.A. Cayley, Finite groups in which the number of cyclic subgroups is 3/4 the order of the group, MSU Graduate Theses, 3695.

[4] M.W. Liebeck, L. Pyber, Upper bounds for the number of conjugacy classes of a finite group, J. Algebra, 198 (1997), 538–562.

[5] M. Xu Preliminary study of finite groups, Modern Mathematics Fundamentals Series 152, 2014. (In Chinese).

[6] R.M. Guralnick, G.R. Robinson, On the commuting probability in finite groups, J. Algebra. 300 (2006), 509–528.

[7] W. Feit, G.M. Seitz, On finite rational groups and related topics, Illinois J. Math. 33 (1989), 103–131.

[8] J.H. Conway, R.T. Curtis, S.P. Norton, et al. Atlas of finite groups, Oxford: Clarendon Press, 1985.

[9] C. Shao, Using the number of elements of the same order to study finite groups, PhD thesis, Soochow University, 2008. (In Chinese).

[10] S. Asgary, N. Ahanjideh, Characterization of $PSL(3, q)$ by nse, Math. Rep. 19 (2017), 425–438.

[11] P.B. Kleidman, M.W. Liebeck, The subgroup structure of the finite classical groups, Cambridge: Cambridge University Press, 1980.

[12] L. Weisnerm, On the number of elements of a group which have a power in a given conjugate set, Bull. Amer. Math. Soc. 31 (1925), 492–497.