ON THE MAXIMAL NUMBER OF ELEMENTS PAIRWISE GENERATING THE FINITE ALTERNATING GROUP

FRANCESCO FUMAGALLI, MARTINO GARONZI, AND PIETRO GHERI

Abstract. Let $G$ be the alternating group of degree $n$. Let $\omega(G)$ be the maximal size of a subset $S$ of $G$ such that $\langle x, y \rangle = G$ whenever $x, y \in S$ and $x \neq y$ and let $\sigma(G)$ be the minimal size of a family of proper subgroups of $G$ whose union is $G$. We prove that, when $n$ varies in the family of composite numbers, $\sigma(G)/\omega(G)$ tends to 1 as $n \to \infty$. Moreover, we explicitly calculate $\sigma(A_n)$ for $n \geq 21$ congruent to 3 modulo 18.

1. Introduction

Given a finite group $G$ that can be generated by 2 elements but not by 1 element, set $\omega(G)$ to be the largest size of a pairwise generating set $S \subseteq G$, that is, a subset $S$ of $G$ with the property that $\langle x, y \rangle = G$ for any two distinct elements $x, y$ of $S$. Also, set $\sigma(G)$ to be the covering number of $G$, that is the minimal number of proper subgroups of $G$ whose union is $G$. We will reserve the term “covering” of $G$ for any family of proper subgroups of $G$ whose union is $G$.

Since any proper subgroup of $G$ contains at most one element of any pairwise generating set, $\omega(G) \leq \sigma(G)$ always.

S. Blackburn [2] and L. Stringer [15] proved that if $n$ is odd and $n \neq 9, 15$ then $\sigma(S_n) = \omega(S_n)$ and that if $n \equiv 2 \pmod{4}$ then $\sigma(A_n) = \omega(A_n)$. Stringer also proved that $\omega(S_9) < \sigma(S_9)$. In [2] it is conjectured that, if $S$ is a finite non abelian simple group, then $\sigma(S)/\omega(S)$ tends to 1 as the order of $S$ goes to infinity. We remark that, apart from the above, the only cases in which the precise value of $\omega(G)$ is known are for groups $G$ of Fitting height at most 2 ([13]) and for certain linear groups (see [3]).

In this paper, we prove the following results.

Theorem 1. Let $n$ vary in the set of composite positive integers. Then

$$\lim_{n \to \infty} \frac{\sigma(A_n)}{\omega(A_n)} = 1.$$
Note that Stringer’s result implies our theorem when \( n \equiv 2 \pmod{4} \), so we will only prove it when \( n \) is divisible by 4 or an odd composite integer.

Our second result concerns the precise value of \( \sigma(A_n) \) when \( n \equiv 3 \pmod{18} \).

**Theorem 2.** Let \( n > 3 \) be an integer with \( n \equiv 3 \pmod{18} \) and let \( q := n/3 \). Then

\[
\sigma(A_n) = \sum_{i=1}^{q-2} \binom{n}{i} + \frac{1}{6} \frac{n!}{q!^3}.
\]

A minimal covering of \( A_n \) consists of the intransitive maximal subgroups of type \((S_i \times S_{n-i}) \cap A_n\), for \( i = 1, \ldots, q-2 \), and the imprimitive maximal subgroups with 3 blocks, which are isomorphic to \((S_q \wr S_3) \cap A_n\).

2. **Technical lemmas**

In this section we will collect some technical results we will need throughout the paper.

**Lemma 1** (Lemma 10.3.3 in [15]). Let \( n \) be an odd integer which is the product of at least three primes (not necessarily distinct). Then if \( n \) is sufficiently large we have

\[
\frac{|S_{n/p} \wr S_p|}{|S_{n/m} \wr S_m|} \geq 2^{\sqrt{n}-3}
\]

where \( m \) is any nontrivial proper divisor of \( n \) different from \( p \).

The following lemma is a generalization of [2] Lemma 4] and its proof uses the same ideas. We need to apply it for \( k \leq 3 \).

**Lemma 2.** Let \( a_1, \ldots, a_k \) be positive integers with \( \sum_{i=1}^{k} a_i = n \). Let \( M \) be a subgroup of \( S_n \). The number of conjugates of \( M \) in \( S_n \) containing a fixed element of type \((a_1, \ldots, a_k)\) is at most \( n^k \).

**Proof.** Let \( N \) be the number of elements of \( S_n \) of type \((a_1, \ldots, a_k)\) and let \( g \) be an element of this type. We want to show that \( N \geq n!/n^k \). Assume that \( a_1, \ldots, a_k \) are organized so that \( k_i \) of them equal \( a_i \) for \( i = 1, \ldots, t \), so that \( k_1 + \cdots + k_t = k \) and \( a_1k_1 + \cdots + a_tk_t = n \). Since the centralizer of \( g \) in \( S_n \) is isomorphic to \( \prod_{i=1}^{t} C_{a_i} \wr S_{k_i} \), we deduce that

\[
N = \frac{n!}{a_1^{k_1}k_1! \cdots a_t^{k_t}k_t!} \geq \frac{n!}{(a_1k_1)^{k_1} \cdots (a_tk_t)^{k_t}} \geq \frac{n!}{n^k},
\]

being \( n^k = (a_1k_1 + \cdots + a_tk_t)^{k_1+\cdots+k_t} \).

Let us double-count the size of the set \( X \) of pairs \((h, H)\) such that \( H \) is a subgroup of \( S_n \) conjugate to \( M \) and \( h \in H \) is of type \((a_1, \ldots, a_k)\). We have \( |X| = N \cdot a(M) \) where \( a(M) \) is the number of conjugates of \( M \) containing a fixed \( h \in G \) of this type and \( |X| = |S_n : NS_n(M)| \cdot b(M) \leq |S_n| \) where \( b(M) \leq |M| \) is the number of elements of \( M \) of type \((a_1, \ldots, a_k)\). We obtain

\[
n! \geq |X| = N \cdot a(M) \geq (n!/n^k)a(M).
\]

It follows that \( a(M) \leq n^k \). \( \square \)
In the following we make frequent use of Stirling’s inequalities, which holds for every integer \( t \geq 2 \),
\[
\sqrt{2\pi t} \cdot (t/e)^t < t! < e\sqrt{t} \cdot (t/e)^t.
\]

**Lemma 3.** Let \( X := \{(x, y) \in \mathbb{N}^2 : 2 \leq x \leq y - 2\} \). Then
\[
\lim_{\|(x, y)\| \to \infty \atop (x, y) \in X} \frac{y!^{x-1}}{x!^{y-1}} = +\infty.
\]

**Proof.** Set
\[
f(x, y) := \frac{y!^{x-1}}{x!^{y-1}}.
\]
Note that \( f(x, y) \leq f(x, y + 1) \) whenever \( (x, y) \in X \). This is because the claimed inequality is equivalent to \( x! \leq (y + 1)^{x-1} \) for \( (x, y) \in X \), which is a consequence of the inequality \( x! \leq x^{x-1} \), which can be easily proved by induction.

We are left to check that \( f(x, x+2) \) tends to \( +\infty \) when \( x \) tends to \( +\infty \). This can be proved directly using calculus techniques and again the fact that \( x! \leq x^{x-1} \). □

**Lemma 4.** Let \( d \geq 2 \), \( k \geq 5 \) be integers such that and \( n = dk \geq 26 \). Then
\[
|S_d \setminus S_k| = d^k k! \leq (n/5e)^n(5n)^{5/2}e\sqrt{n}.
\]

**Proof.** Set \( f(x) := (nx)^{x/2}/e^n \) for any real \( x \geq 5 \). The derivative of \( f \) is \( f'(x) = (1/(2x))f(x)g(x) \) where \( g(x) = x \log(nx) - 2n + x \), so \( f'(5) < 0 \) being \( n \geq 14 \), and \( f \) is decreasing in \( x = 5 \). Since \( g'(x) = \log(nx) + 2 \) is positive (being \( x \geq 5 \)) and the sign of \( f' \) equals the sign of \( g \), we deduce that in the interval \([5, n/5]\) we have \( f(x) \leq \max\{f(5), f(n/5)\} \) and this equals \( f(5) \) being \( n \geq 25 \). Therefore, using the bound \( m! \leq (m/e)^m e\sqrt{m} \), if \( k \leq n/5 \) we obtain
\[
d^k k! \leq (d/e)^{dk} e^{k/2} (k/e)^k k!^{1/2} = f(k) \cdot (n/e)^n e\sqrt{k} \leq (n/5e)^n(5n)^{5/2} e\sqrt{n}.
\]
The case \( k > n/5 \) corresponds to \( d < 5 \) and can be done case by case. For \( d = 4 \) we need \( n \geq 18 \), for \( d = 3 \) we need \( n \geq 2 \) and for \( d = 2 \) we need \( n \geq 26 \). □

**Lemma 5.** Let \( n \) be an even positive integer, \( r \) an odd divisor of \( n \) such that \( 3 \leq r \leq n/3 \) and set \( g(n, r) = (r!)^{n/3} (n/r)! + r \cdot r! \cdot ((n/r)!)^3 \). Then there exists a positive constant \( C \) such that \( g(n, r) \leq C((n/3)!)^3 \) for every \( n \) large enough.

**Proof.** Let \( n \) and \( r \) as in the statement and note that since \( n \) is even and \( r \) is odd we have \( 3 \leq r \leq n/4 \). If \( r = 3 \) then \( g(n, r) = 6^{n/3}(n/3)! + 18((n/3)!)^3 < 19((n/3)!)^3 \) for large enough \( n \). Using Stirling’s inequalities (1), it is easy to prove that \( (n/4)^n \leq n \cdot (3/4)^n \) for large enough \( n \), and this easily implies the result when \( r = n/4 \).

Assume therefore that \( 5 \leq r \leq n/5 \). We apply Lemma 4 and deduce that
\[
g(n, r) \leq (r + 1) \left( \frac{n}{5e} \right)^n (5n)^{5/2} e\sqrt{n} \leq \left( \frac{n}{5e} \right)^n (5n)^{5/2} n^{3/2} e.
\]
By another application of (1), we get that there exists a positive constant \( D \) such that
\[
\frac{g(n, r)}{((n/3)!)^3} \leq (3/5)^n n^{5/2} \cdot D,
\]
which tends to zero as \( n \) tends to infinity. □
3. Proof of Theorem 1

Let $\Gamma$ be an (undirected) graph. Recall that the degree of a vertex of $\Gamma$ is defined as the number of vertices of $\Gamma$ that are adjacent to it. Also, a set of vertices is called independent if no two of its elements are connected by an edge. We prove Theorem 1 as an application of following result due to P.E. Haxell.

**Theorem 3** (Theorem 2 in [7]). Let $k$ be a positive integer, let $\Gamma$ be a graph of maximum degree at most $k$, and let $V(\Gamma) = V_1 \cup \cdots \cup V_n$ be a partition of the vertex set of $\Gamma$. Suppose that $|V_i| \geq 2k$ for each $i$. Then $\Gamma$ has an independent set \{ $v_1, \ldots, v_n$ \} where $v_i \in V_i$ for each $i$.

We will apply Theorem 3 to prove Theorem 1, first for $n$ odd and composite, then for $n$ divisible by 4. This will correspond to two different graphs.

3.1. Case $n$ odd. We first consider the case $n$ is an odd composite number. In this section, $p$ will always be the smallest prime divisor of $n$. For each proper nontrivial divisor $m$ of $n$, let $P_m$ be the set of partitions of the set \{ $1, \ldots, n$ \} into $m$ blocks each of cardinality $n/m$. We want to find a maximal set of $n$-cycles in $A_n$ pairwise generating $A_n$ and in particular we will prove the following.

**Proposition 1.** If $n$ is a sufficiently large odd composite number and $p$ denotes the smallest prime divisor of $n$, then $\omega(A_n) \geq |P_p|$.

Since the imprimitive maximal subgroups of $A_n$ preserving a partition with $p$ blocks cover all the $n$-cycles in $A_n$, and since the elements of $A_n$ which are not $n$-cycles are covered by the maximal intransitive subgroups of type $(S_i \times S_{n-i}) \cap A_n$ with $1 \leq i \leq n/3$, we deduce from Proposition 1 that

$$|P_p| \leq \omega(A_n) \leq \sigma(A_n) \leq |P_p| + \sum_{i=1}^{\lfloor n/3 \rfloor} \binom{n}{i}.$$

This proves Theorem 1 since the sum on the right-hand side is less than $2^n$, so it is asymptotically irrelevant compared to

$$|P_p| = \frac{n!}{(n/p)!p!} \geq \frac{(n/e)^{n(e/p)^{p/2}}}{(n/e)^{n(p/e)^p e^{\sqrt{p}}}} = \frac{p^n}{e^{\sqrt{p}}} \cdot \left( e^{2 \sqrt{n/p^3}} \right)^p \geq 3^n$$

where the last inequality holds for sufficiently large $n$.

We are therefore reduced to prove Proposition 1.

For every $\Delta \in P_m$ let $C(\Delta)$ be the set of $n$-cycles $x \in A_n$ such that $\Delta$ is the set of orbits of the element $x^n$. In other words, $C(\Delta)$ is the set of $n$-cycles contained in the maximal imprimitive subgroup of $A_n$ whose block system is $\Delta$. Using the fact that every $n$-cycle belongs to a unique imprimitive maximal subgroup of $S_n$ with $m$ blocks, it is easy to see that $|C(\Delta)| = |S_{n/m} \wr S_m|/n$ using a double counting argument. With a slight abuse of notation, for any maximal subgroup $H$ of $A_n$, we call $C(H)$ the set of $n$-cycles contained in $H$.

We define a graph $\Gamma$ whose vertex set is $V(\Gamma)$ and whose edge set is $E(\Gamma)$ in the following way. $V(\Gamma)$ is the set of $n$-cycles of $A_n$ and, for distinct $x, y \in V(\Gamma)$, we say that $\{x, y\} \in E(\Gamma)$ if and only if $\{x, y\} \neq A_n$ and the orbits of $x^n$ do not coincide with those of $y^n$, in other words there is no $\Delta \in P_p$ such that both $x$ and $y$ belong to $C(\Delta)$. 


Since the $n$-cycles are pairwise conjugate in $S_n$, the graph $\Gamma$ is vertex-transitive, so it is regular, in other words, every vertex has the same valency $k$. In order to prove Proposition 1, it is enough to prove that $|C(\Delta)| \geq 2k$ for all $\Delta \in P_p$, since then the result will follow from Theorem 3 applied to the partition of the vertex-set of $\Gamma$ given by the $C(\Delta)$ with $\Delta \in P_p$.

If $x$ is any vertex, then

$$k \leq \sum_{H \in \mathcal{H}_x} |C(H)|$$

where $\mathcal{H}_x$ is the set of maximal subgroups of $A_n$ containing $x$, except for the maximal imprimitive subgroup with $p$ blocks. Clearly, no intransitive subgroup contains $x$ so $\mathcal{H}_x$ is made of imprimitive and primitive subgroups. Let $\mathcal{H}_x^{imp}$ be the set of maximal imprimitive subgroups of $A_n$ containing $x$ whose number of blocks is not $p$, and let $\mathcal{H}_x^{prim}$ be the set of maximal primitive subgroups of $A_n$ containing $x$. Then

$$k \leq \sum_{H \in \mathcal{H}_x^{imp}} |C(H)| + \sum_{H \in \mathcal{H}_x^{prim}} |C(H)|.$$

We bound the first term of the above sum. Let $\Delta_m(x)$ be the partition in $P_m$ whose blocks are the orbits of the element $x^m$. Since $n$ has at most $2\sqrt{n}$ positive divisors,

$$\sum_{H \in \mathcal{H}_x^{imp}} |C(H)| = \sum_{m|n, m \neq p} |C(\Delta_m(x))| \leq 2\sqrt{n} \max_{m|n, m \neq p} |S_{n/m} \wr S_m|/n$$

where the second summation and the maximum is on all nontrivial proper divisors $m$ of $n$ that are different from $p$.

Note that, if $n \neq p^2$, the last term in (2) is at least $c^n$ for any given constant $c$, if $n$ is sufficiently large. This can be checked easily using $|S_{n/m} \wr S_m| = (n/m)!^m m!$ and Stirling inequalities (1).

Lemma 1 implies that the last term in (2) is asymptotically irrelevant compared to $|C(\Delta)|$ for $\Delta \in P_p$ when $n$ is the product of at least three primes.

We now turn to primitive subgroups. When $n > 23$ (and $n$ is not a prime) the primitive maximal subgroups of $A_n$ containing $n$-cycles are permutational isomorphic to $\text{PTL}(m, s) \cap A_n$, where

$$n = \frac{s^m - 1}{s - 1}$$

for some $m \geq 2$ and some prime power $s$, its action on points (or on hyperplanes) of a projective space of dimension $m$ over the field of $s = p^f$ elements (10 Theorem 3). Therefore in particular we have that if $H$ is such a subgroup of $A_n$ then

$$|C(H)| < |\text{PTL}(s)| < 2^{n-1}.$$

By Lemma 2 there are at most $n$ conjugates of $H$ containing a fixed $n$-cycle $x$. Moreover we show now that $S_n$ has at most $\log_2(n)$ conjugacy classes of such maximal primitive subgroups, and therefore this number is at most $2 \log_2(n)$ for $A_n$. First observe that, being $n$ odd, if $(m, s)$ is a pair satisfying equation (3) then $s$ is the biggest power of $p$ dividing $n - 1$. The possible choices for $s$ are at most the number of primes dividing $n - 1$, that is at most $\pi(n - 1)$ which is trivially smaller than $\log_2(n)$. Once that $s$ is chosen there is at most only one possible value for $m$ such that $(m, s)$ satisfies (3). Thus the number of these pairs is bounded from above.
by $\log_2(n)$. Now, for a fixed pair $(m, s)$ satisfying (3) the group $A_n$ contains at most two conjugacy classes of primitive maximal subgroups isomorphic to $PGL_m(s) \cap A_n$ (it can be proved that the two actions of such a group respectively on the projective points and on the projective hyperplanes are equivalent in $S_n$). Thus the number of conjugacy classes of proper primitive maximal subgroups containing an $n$-cycle is at most $2 \log_2(n)$. It follows that

$$ \sum_{H \in \mathcal{H}_{pr}^{c,m}} |C(H)| \leq n \log_2(n) \cdot 2^n$$

and so it is easy to see that the last term in (2) is an upper bound also for this sum (remember that we are considering $n \neq p^2$).

Assume that $n$ is a product of at least three primes, not necessarily distinct. If $\Delta \in \mathcal{P}_p$, then by Lemma 1 we have

$$ \sum_{H \in \mathcal{H}_{pr}^{c,m}} |C(H)| \leq n \log_2(n) \cdot 2^n$$

and we only have to prove that, for large enough $n$, the right-hand side is larger than 2. This follows from Lemma 3.

3.2. Case $n$ divisible by 4. We now prove Theorem 1 when $n$ is divisible by 4.

In [13], Maróti proved that $\sigma(G) \sim 2^{n-2}$. We want to prove that $\omega(G)$ is also asymptotic to $2^{n-2}$ in this case, so that $\omega(G) \sim \sigma(G)$. Since $\omega(G) \leq \sigma(G)$, it is enough to find a lower bound for $\omega(G)$ which is asymptotic to $2^{n-2}$.

We consider the set

$$ \mathcal{S} = \{ \Delta \subseteq \{1, \ldots, n\}, \ 1 < |\Delta| < n/2, \ |\Delta| \text{ odd} \}.$$ 

Since the number of subsets of $\{1, \ldots, n\}$ of even size is equal to the number of subsets of odd size (this can be seen by expanding the equality $0 = (1 - 1)^n$ with the binomial theorem), we have

$$ |\mathcal{S}| = \sum_{i=2}^{n/4} \binom{n}{2i-1} = 2^{n-2} - n \sim 2^{n-2}.$$
Let \( V \) be the set of elements of \( A_n \) of cycle type \((a, n-a)\) for \( a \) odd and \( 1 < a < n/2 \). We have \( V = \bigcup_{\Delta \in S} C(\Delta) \), where \( C(\Delta) \) is the set of bicycles with orbits \( \Delta \) and \( \Omega \setminus \Delta \).

As in the case \( n \) odd, we define a graph \( \Gamma \) with now vertex set \( V(\Gamma) = V \) and whose edge set \( E(\Gamma) \) is the family of size 2 subsets \( \{x, y\} \subseteq V \) such that \( \langle x, y \rangle \neq A_n \) and \( x \) and \( y \) do not belong to the same \( C(\Delta) \), for all \( \Delta \in S \).

The sets \( C(\Delta) \) determine a partition of \( V(\Gamma) \) and by Theorem 3 we are done if we can prove that, for all \( \Delta \in S \),

\[ |C(\Delta)| \geq 2k, \]

where \( k \) is the maximum degree of a vertex in \( \Gamma \).

In [17, Theorem 1.5] and [18, Theorem 1.1] a careful and detailed description of the primitive permutation groups containing a permutation with at most four cycles is given. From that analysis it follows that, when \( n \) is divisible by 4 and sufficiently large there are only two cases in which a product of two disjoint cycles of odd length in \( S_n \) can be contained in a primitive permutation group \( H \leq S_n \) not containing the alternating group \( A_n \), and in both cases the cycles have lengths 1 and \( n-1 \). By our choice of \( S \), \( |\Delta| \neq 1 \), therefore, since by the definition of \( V \) the intransitive subgroups of \( A_n \) cannot contain subsets of the form \( \{x, y\} \in E(\Gamma) \), the only maximal subgroups of \( A_n \) containing such sets are the imprimitive ones.

We now evaluate the maximum degree \( k \) of our graph. Namely, for any fixed \( x \in C(\Delta) \) we bound the number of elements \( y \in V \setminus C(\Delta) \) such that \( \langle x, y \rangle \neq A_n \).

Let \( \mathcal{H}^{\text{imp}}_x \) be the set of maximal imprimitive subgroups of \( A_n \) containing \( x \). The above discussion implies that

\[ k \leq \sum_{H \in \mathcal{H}^{\text{imp}}_x} |H| \]

Assume that \( x \in C(\Delta) \) with \( |\Delta| = a \), so that \( x \) is a product of two disjoint cycles of lengths \( a \) and \( n-a \). Moreover assume that \( x \) belongs to an imprimitive maximal subgroup \( W \), say \( W \simeq S_d \ltimes S_m \), with \( d, m > 1 \) and \( dm = n \).

Then there are two possibilities.

- \( \Delta \) is the union of some of the blocks of \( W \). In this case \( d \mid a \) and \( W \) is uniquely determined by \( x \), since its blocks are exactly the orbits of \( x^m \).
- \( m \mid a \) and \( \Delta \) (and \( \Omega \setminus \Delta \)) intersects each block of \( W \) in exactly \( a/m \) (resp. \( (n-a)/m \)) elements. In this case there are exactly \( m \) conjugates of \( W \) containing \( x \); they can be obtained by pairing cyclically each orbit of \( x_1^m \) with an orbit of \( x_2^m \), where \( x_1 \) and \( x_2 \) are respectively the restrictions of \( x \) to \( \Delta \) and to \( \Omega \setminus \Delta \).

It follows that

\[
(4) \quad \sum_{H \in \mathcal{H}^{\text{imp}}_x} |H| \leq \sum_{r \mid \gcd(a, n)} \left( |S_r \ltimes S_{n/r}| + r \cdot |S_{n/r} \ltimes S_r| \right) \]

\[
= \sum_{r \mid \gcd(a, n)} \left( (r!)^{n/r} (n/r)! + r \cdot r! \cdot ((n/r)!)^r \right). \]
Since $|C(\Delta)| = (|\Delta| - 1)!(n - |\Delta| - 1)! \geq (2/n)^2(n/2)!^2$, inequality (1) together with Lemma 5 gives, for large enough $n$, 
\[
\frac{k}{|C(\Delta)|} \leq \frac{\sum_{H \in \mathcal{H}_r^{\text{imp}}} |H|}{(2/n)^2(n/2)!^2} \leq \frac{Cn(n/3)!^3}{(2/n)^2(n/2)!^2} \leq c_2(2/3)^nn^3
\]
for some constant $c_2$. The last inequality can be proved easily using Stirling’s inequalities (1). This proves that $k/|C(\Delta)|$ tends to zero as $n \to \infty$, hence it is smaller than 1/2 for sufficiently large $n$, which is what we wanted to prove.

4. Proof of Theorem 2

The following argument is a slight generalization of [10] Section 3.

Let $G$ be any finite non-cyclic group and let $T$ be a finite group containing $G$ as a normal subgroup. Let $\mathcal{M}$ be a family of maximal subgroups of $G$ and let $\Pi$ be a subset of $G$. Let $\{M_i \mid i \in I_T\}$ be a set of pairwise non-$T$-conjugate maximal subgroups of $G$ such that every maximal subgroup of $G$ is $T$-conjugate to some $M_i$, with $i \in I_T$, and let $\mathcal{M}_i := \{t^{-1}M_it : i \in I_T\}$ and $\Pi_i := \Pi \cap \bigcup_{M \in \mathcal{M}_i} M$, for all $i \in I_T$. Let $I \subseteq I_T$. Suppose that the following holds.

1. $\mathcal{M} = \bigcup_{i \in I} \mathcal{M}_i$;
2. $x^t \in \Pi$ for all $x \in \Pi, t \in T$;
3. $\Pi$ is contained in $\bigcup_{M \in \mathcal{M}} M$;
4. if $A, B \in \mathcal{M}$ and $A \neq B$ then $A \cap B \cap \Pi = \emptyset$;
5. $M \cap \Pi \neq \emptyset$ for all $M \in \mathcal{M}$.

Note that this implies in particular that $\{\Pi_i\}_{i \in I}$ is a partition of $\Pi$. Moreover if $A, B$ are $T$-conjugate subgroups then since $\Pi$ and each $\Pi_i$ (for $i \in I_T$) are unions of $T$-conjugacy classes of elements of $T$, we have $|A \cap \Pi| = |B \cap \Pi|$ and $|A \cap \Pi_i| = |B \cap \Pi_i|$.

For any maximal subgroup $M$ of $G$ outside $\mathcal{M}$ define
\[
d(M) := \sum_{i \in I} \frac{|M \cap \Pi_i|}{|M_i \cap \Pi_i|}.
\]

The proof of the following proposition is essentially the same as the one in [10] Section 3 but we include it for completeness.

**Proposition 2.** Assume the above setting. If $d(M) \leq 1$ for all maximal subgroup $M$ of $G$ outside $\mathcal{M}$ then any family of proper subgroups of $G$ whose union contains $\Pi$ has size at least $|\mathcal{M}|$. In other words, $\mathcal{M}$ is a minimal covering of $\Pi$. Moreover, if $d(M) < 1$ for all maximal subgroup $M$ of $G$ outside $\mathcal{M}$ then $\mathcal{M}$ is the unique minimal covering of $\Pi$.

**Proof.** Let $\mathcal{K}$ be any family of maximal subgroups of $G$ such that $\bigcup_{K \in \mathcal{K}} K \supseteq \Pi$ and suppose $\mathcal{K} \neq \mathcal{M}$. We want to prove that $|\mathcal{M}| \leq |\mathcal{K}|$. Define
\[
\mathcal{M}' := \mathcal{M} - (\mathcal{M} \cap \mathcal{K}), \quad \mathcal{K}' := \mathcal{K} - (\mathcal{M} \cap \mathcal{K}).
\]

For any $i \in I$, let $n_i$ be the number of subgroups from $\mathcal{M}_i$ in $\mathcal{M}'$, and for any $j \in I_T$ let $k_j$ be the number of subgroups from $\mathcal{M}_j$ in $\mathcal{K}'$. 

8 FRANCESCO FUMAGALLI, MARTINO GARONZI, AND PIETRO GHERI
Observe that since $\mathcal{K}$ covers $\Pi_i$ and $\mathcal{M}$ partitions $\Pi$, the members of $\mathcal{K}'$ must cover the elements of $\Pi_i$ contained in $\bigcup_{M \in \mathcal{M}} M$. Since $\mathcal{M}$ partitions $\Pi$, the number of such elements is $m_i | M_i \cap \Pi_i |$. Therefore

$$m_i | M_i \cap \Pi_i | \leq \sum_{j \notin I} k_j | M_j \cap \Pi_i |.$$

We claim that if $d(M) \leq 1$ for all $M \in \mathcal{K}'$ then $|\mathcal{M}| \leq |\mathcal{K}|$. Indeed, we have

$$|\mathcal{M}'| = \sum_{i \in I} m_i \leq \sum_{i \in I} \sum_{j \notin I} k_j \frac{|M_j \cap \Pi_i|}{|M_i \cap \Pi_i|} = \sum_{j \notin I} k_j \sum_{i \in I} \frac{|M_j \cap \Pi_i|}{|M_i \cap \Pi_i|} = \sum_{j \notin I} k_j d(M_j) \leq \sum_{j \notin I} k_j = |\mathcal{K}'|.$$

This implies

$$|\mathcal{M}| = |\mathcal{M} \cap \mathcal{K}| + |\mathcal{M}'| \leq |\mathcal{M} \cap \mathcal{K}| + |\mathcal{K}'| = |\mathcal{K}|,$$

and therefore $\mathcal{M}$ is a covering of $\Pi$ of minimal size. Moreover, if $d(M) < 1$ for all maximal subgroup $M$ of $G$ outside $\mathcal{M}$, then the above argument shows that $|\mathcal{M}| < |\mathcal{K}|$ whenever $\mathcal{M} \neq \mathcal{K}$, proving that $\mathcal{M}$ is the unique covering of $\Pi$ of minimal size. \qed

From now on let $n \geq 21$ be a positive integer congruent to 3 modulo 18 and let $q := n/3, G := A_n, T := S_n$. Note that $q \equiv 1 \pmod{6}$. We prove Theorem 2 by showing (with the use of Proposition 2) the existence of a minimal covering $\mathcal{M}$ for $A_n$ of size

$$\frac{1}{6} \frac{n!}{q!^3} + \sum_{i=1}^{q-2} \binom{n}{i}.$$

If $n = \sum_{i=1}^t a_i$ and $1 \leq a_1 \leq a_2 \leq \ldots \leq a_t$ we denote by $(a_1, \ldots, a_t)$ the set of elements of $A_n$ whose cycle structure consists of $t$ disjoint cycles each of length $a_i$, for $i = 1, \ldots, t$. Note that each $(a_1, \ldots, a_t)$ is either empty or an $A_n$-conjugacy class or the union of two $A_n$-conjugacy classes. The latter case occurs if and only if the numbers $a_1, \ldots, a_t$ are all odd and pairwise distinct.

Let $\Pi_{-1} = (n)$ be the set of all $n$-cycles and for every integer $a$ such that $1 \leq a \leq q-2$ define

$$\Pi_a := \begin{cases} (a, \frac{n-a-1}{2}, \frac{n-a+1}{2}) & \text{if } a \equiv 0 \pmod{2} \\ (a, \frac{n-a}{2} - 1, \frac{n-a}{2} + 1) & \text{if } a \equiv 1 \pmod{2}. \end{cases}$$

We define the collection $\mathcal{M}$ of $S_n$-conjugacy classes of maximal subgroups of $A_n$ as follows.

$\mathcal{M}_{-1}$ is the set of maximal imprimitive subgroups of $A_n$ with 3 blocks. Thus the elements of $\mathcal{M}_{-1}$ are subgroups isomorphic to $(S_q \wr S_3) \cap A_n$.

For every $a$ such that $1 \leq a \leq q-2$ define $\mathcal{M}_a$ to be the set of maximal intransitive subgroups of $A_n$ which are the stabilizers of a set of size $a$.

Finally, let

$$\Pi := \bigcup_{a = -1, 1, \ldots, q-2} \Pi_a \quad \text{and} \quad \mathcal{M} := \bigcup_{a = -1, 1, \ldots, q-2} \mathcal{M}_a.$$
Lemma 6. If $j \in I_{S_n}$ and $M_j \in \mathcal{M}_j$ then
\[
|M_j \cap \Pi_i| = \frac{m_j(i) \cdot |N_{S_n}(M_j)| \cdot |\Pi_i|}{|S_n|} \leq \frac{m_j(i) \cdot |M_j| \cdot |\Pi_i|}{|A_n|}.
\]
Moreover, if $M_j$ is not primitive then this inequality is actually an equality.

Proof. Consider the bipartite graph with set of vertices $\Pi_i \cup \mathcal{M}_j$ and where there is an edge between $g \in \Pi_i$ and $M \in \mathcal{M}_j$ if and only if $g \in M$. Since $\Pi_i$ is a conjugacy class of $S_n$, the family $\mathcal{M}_j$ covers $\Pi_i$ if one of its members intersects it. By assumption the number of edges of this graph equals both $m_j(i) \cdot |\Pi_i|$ and $|S_n : N_{S_n}(M_j)| \cdot |M_j \cap \Pi_i|$. We are left to prove that
\[
|A_n : M_j| \leq |S_n : N_{S_n}(M_j)|
\]
This follows from the fact that $M_j$ is self-normalized in $A_n$, being a maximal subgroup (and $n \geq 5$), and $|S_n : N_{S_n}(M_j)|$ is the number of $S_n$-conjugates of $M_j$, while $|A_n : M_j| = |A_n : N_{A_n}(M_j)|$ is the number of $A_n$-conjugates of $M_j$.

Lemma 7. Assume $m$ is a positive integer divisible by 3. An element of $S_m$ of cycle type $(a, b, c)$, with $a, b, c \geq 1$ and $a + b + c = m$, stabilizes a partition of \{1, \ldots, m\} with 3 blocks if and only if at least one of the following holds:

1. $a = b = c = m/3$.
2. $3$ divides $\gcd(a, b, c)$.
3. One of $a, b, c$ equals $2m/3$.
4. One of $a, b, c$ equals $m/3$ and the other two are even.

Proof. Straightforward.

We have the following.

1. $\bigcup_{M \in \mathcal{M}} M = A_n$. To see this let $g \in A_n$, and let $(a_1, \ldots, a_k), 1 \leq a_1 \leq \ldots \leq a_k,$ be the cycle type of $g$, with $\sum_{i=1}^{k} a_i = n$. Note that, since $g \in A_n$ and $n$ is odd, $k$ must be odd. If $a_1 < q - 1$ then $g$ belongs to a member of $\mathcal{M}_{a_1}$. Now assume that $a_1 \geq q - 1$, so that $a_i \geq q - 1$ for all $i = 1, \ldots, k$. It follows that $3q = n = \sum_{i=1}^{k} a_i \geq k(q - 1)$, therefore $k \leq 3$ being $q > 3$ odd. If $k = 1$ then $g$ belongs to a member of $\mathcal{M}_{-1}$, so now assume that $k = 3$. Since $q - 1 \leq a_1 \leq a_2 \leq a_3$, the only possibilities for $(a_1, a_2, a_3)$ are either $(q - 1, q - 1, q + 2)$ or $(q - 1, q, q + 1)$, therefore $g$ belongs to a member of $\mathcal{M}_{-1}$ by Lemma 7 since $q \equiv 1 \pmod{6}$ (respectively case (2) and case (4)). Note that here is the point where we use the crucial assumption $n \equiv 3 \pmod{18}$.

2. For every $g \in \Pi_1$ there exists a unique $M \in \mathcal{M}$ such that $g \in M$. More precisely, if $g \in \Pi_1$ then the unique member of $\mathcal{M}$ containing $g$ is the unique member of $\mathcal{M}_{-1}$ whose blocks are the three orbits of $g^3$, and if
If \( g \in \Pi_a, \ a \in \{1, \ldots, q-2\} \), then the unique member of \( \mathcal{M} \) containing \( g \) is the subgroup in \( \mathcal{M}_a \) sharing an orbit of size \( a \) with \( g \). This is because no element of \( \Pi \) which is not an \( n \)-cycle stabilizes a partition with 3 blocks, a fact that can be easily proved by using Lemma\(^2\).

From now on let \( \mathcal{M}_j \) be a \( S_n \)-class of maximal subgroups of \( A_n \) not contained in \( \mathcal{M} \) (in other words we think of \( j \) as an index in \( I_{S_n} \setminus I \)) and let \( M_j \) be any element of \( \mathcal{M}_j \). We deduce from Lemma\(^3\) that, if \( i \in I \), then

\[
d(M_j) = \sum_{i \in I} \frac{|M_j \cap \Pi_i|}{|\Pi_i \cap \Pi_j|} \leq \sum_{i \in I} \frac{m_j(i)|M_j|}{m_i(i)|\Pi_i|} \leq |M_j| \sum_{i \in I} \frac{m_j(i)}{|\Pi_i|}.
\]

Now, if \( \mathcal{M}_j \) is a \( S_n \)-class of maximal intransitive subgroups of \( A_n \) then \( m_j(-1) = 0 \), while \( m_j(i) \leq 1 \) for \( 1 \leq i \leq q-2 \) and also \( m_j(i) = 0 \), except for at most 4 values of \( i \). This is because, thinking of \( j \) as the size of an orbit of the members of \( \mathcal{M}_j \), with \( q-1 \leq j < n/2 \), the possible values of \( i \) such that \( 1 \leq i \leq q-2 \) and \( m_j(i) \neq 0 \) are obtained by solving the equations \( j = (n-i)/2-1, j = (n-i)/2+1, j = (n-i-1)/2 \) and \( j = (n-i+1)/2 \). Note that if \( M_j \) is of type \( (S_{q-1} \times S_{2q+1}) \cap A_n \), then \( M_j \cap \Pi = \emptyset \), implying that \( d(M_j) = 0 \). If this is not the case then \( |M_j| \leq q!/(2q)! \), therefore

\[
d(M_j) \leq \frac{4 \cdot q! \cdot (2q)!}{(q-2)! \cdot (2q+2)!} = \frac{4(q-1)}{(q-2)(2q+1)(2q+2)} < 1.
\]

If \( \mathcal{M}_j \) is a \( S_n \)-class of transitive subgroups of \( A_n \) then \( m_j(i) \leq n^3 \) by Lemma\(^2\). Moreover, if \( M_j \) is imprimitive then \( |M_j| \leq (n/5e)^n(5n)^{5/2}e\sqrt{n} \) by Lemma\(^3\) and if \( M_j \) is primitive then \( |M_j| \leq 2^n \) by\(^4\). Since \( |M_j| \geq |(S_q \wr S_3) \cap A_n| = 3q!^3 > 3(n/3e)^n \) for every \( i \in I \) and \( |I| < n \), we obtain that

\[
d(M_j) \leq |M_j| \sum_{i \in I} \frac{m_j(i)}{|\Pi_i|} \leq \frac{n^4(5n)^{5/2}e\sqrt{n}}{3(n/3e)^n} = \frac{5^{5/2}e}{3} n^7(3/5)^n < 1,
\]

as long as \( n \geq 65 \).

Finally when \( n = 21, 39 \) or 57, then \( q \) is a prime, respectively: 7, 13 and 19. Since \( |I| = q-1 \) and \( m_j(i) \leq n^3 \), we can use the bound

\[
d(M_j) \leq |M_j| \sum_{i \in I} \frac{m_j(i)}{|\Pi_i|} \leq \frac{(q-1)n^3|M_j|}{3 \cdot q!^3},
\]

which gives the result when \( n \in \{39, 57\} \) or when \( n = 21 \) and \( M_j \) is primitive, by making use of the bound \( |M_j| \leq 3!^q \cdot q! \). Here we use the list of primitive subgroups of a given (small) degree, available in\(^5\) Table B.2.

Now assume \( n = 21 \) and \( M = M_j \) is imprimitive, so that \( M \cong (S_3 \wr S_7) \cap A_{21} \). Then the only elements of \( \Pi \) that stabilize a partition with 7 blocks are those of type \( (21) \) or of type \( (4, 8, 9) \). Moreover \( |M \cap \Pi_{-1}| = |M|/21 \) and \( |M \cap \Pi_4| = \left(\frac{7}{9}\right)^{3!} \cdot 3! \cdot 2^3 \cdot 7! = 48, \) while \( |M_{-1} \cap \Pi_{-1}| = |M_{-1}|/21 \) and \( |M_4 \cap \Pi_4| = 3! \cdot \left(\frac{7}{8}\right)^4 \cdot 7! \cdot 8! \), hence

\[
d(M) = \frac{3!^7 \cdot 7!}{7!^3 \cdot 3!} + \frac{7! \cdot 48}{3! \cdot \left(\frac{7}{8}\right)^4 \cdot 7! \cdot 8!} = \frac{315059}{171531360} < 1.
\]

**References**

[1] N. Alon, J. H. Spencer. The probabilistic method. Fourth edition. Wiley Series in Discrete Mathematics and Optimization. John Wiley and Sons, Inc., Hoboken, NJ, 2016.
[2] S. R. Blackburn. Sets of permutations that generate the symmetric group pairwise. *J. Combin. Theory Ser. A* 113 (2006), no. 7, 1572–1581.
[3] J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, A. Maróti. Sets of elements that pairwise generate a linear group. *J. Combin. Theory Ser. A* 115 (2008), no. 3, 442–465.
[4] P. J. Cameron, C. Y. Ku, Intersecting families of permutations. *European Journal of Combinatorics* 24 (2003) 881–890.
[5] J. D. Dixon, B. Mortimer, Permutation groups, *Graduate Texts in Mathematics*, 163, Springer-Verlag, New York, 1996.
[6] P. Erdős, L. Lovász. Problems and results on 3-chromatic hypergraphs and some related questions, A. Hajnal, R. Rado, V. Sós (Eds.), *Colloquium Math. Society Janos Bolyai*, vol. 11, North-Holland, Amsterdam, 1973, pp. 609–627.
[7] P.E. Haxell, A Note on Vertex List Colouring, *Combinatorics, Probability and Computing*, 10 (2001), no. 4, 345–347.
[8] Isaacs, I. Martin, Character theory of finite groups, *Dover Publications*, Inc., New York, 1994 or *AMS Chelsea Publishing*, Providence RI, 2006.
[9] G. James, A. Kerber, The representation theory of the symmetric group. *Encyclopedia of Mathematics and its Applications*, 16. Addison-Wesley Publishing Co., Reading, Mass., 1981.
[10] G. A. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory*, 5, (2002), no. 4, 403–407.
[11] A. Lucchini, A. Maróti. On the clique number of the generating graph of a finite group. *Proc. Amer. Math. Soc.* 137 (2009), no. 10, 3207–3217.
[12] M.W. Liebeck, A. Shalev, Maximal subgroups of symmetric groups, *J. Combin. Theory Ser. A* 75 (1996) 341–352.
[13] A. Maróti, Covering the symmetric groups with proper subgroups, *J. Combin. Theory Ser. A* 110 (2005), no. 1, 97–111.
[14] A. Maróti, On the orders of primitive groups, *J. Algebra* 258 (2002), no. 2, 631–640.
[15] L. Stringer, Pairwise generating sets for the symmetric and alternating groups, PhD thesis, *Royal Holloway, University of London* (2008).
[16] E. Swartz. On the covering number of symmetric groups having degree divisible by six. *Discrete Math.* 339(11): 2593–2604, 2016.
[17] S. Guest, J. Morris, C.E. Praeger and P. Spiga, Affine transformations of finite vector spaces with large orders or few cycles, *J. Pure Appl. Algebra* (2015), no. 2, 308–330.
[18] S. Guest, J. Morris, C.E. Praeger and P. Spiga, Finite primitive permutation groups containing a permutation having at most four cycles, *J. Algebra* (2016), 233–251.

Dipartimento di Matematica e Informatica ‘Ulisse Dini’, Viale Morgagni 67/A, 50134 Firenze, Italy

Email address: francesco.fumagalli@unifi.it

Departamento de Matemática, Universidade de Brasília, Campus Universitário, Darcy Ribeiro, Brasília-DF, 70910-900, Brazil.

Email address: mgaronzi@gmail.com

Dipartimento di Matematica e Informatica ‘Ulisse Dini’, Viale Morgagni 67/A, 50134 Firenze, Italy

Email address: pietro.gheri@unifi.it