Powers of Cycle-Classes in Symmetric Groups

Edward Bertram and Marcel Herzog

Department of Mathematics, University of Hawaii at Manoa, Honolulu, Hawaii; and
School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of
Exact Sciences, Tel-Aviv University, Tel-Aviv, Israel
E-mail: ed@math.hawaii.edu; herzog@math.tau.ac.il

Communicated by the Managing Editors

Received March 1, 1999

DEDICATED TO THE MEMORY OF PAUL ERDŐS, WHO INSPIRED
SO MANY WITH SO MUCH

I. INTRODUCTION

In 1972 the first author proved the following theorem:

**Theorem 1 [Be, Corollary 2.1].** Each permutation in the alternating group $A_n$, $n \geq 2$, is a product of two \( \ell \)-cycles in $S_n$ if and only if either $\lfloor \frac{n}{2} \rfloor \leq \ell \leq n$ or $n = 4$ and $\ell = 2$.

Note. Theorem 1 implies that when $n = 4$ every even permutation is a product of two $\ell$-cycles if and only if $2 \leq \ell \leq 4$.

The aim of the present paper is to extend this result to three and four $\ell$-cycles. Our main results are Theorems 2 and 3:

**Theorem 2.** Each permutation in $A_n$, $n \geq 1$, is a product of three $\ell$-cycles in $S_n$ if and only if $\lfloor \frac{n}{2} \rfloor \leq \ell \leq n$ or $n = 7$ and $\ell = 3$.

**Theorem 3.** Each permutation in $A_n$, $n \geq 2$, is a product of four $\ell$-cycles in $S_n$ if and only if:

1. $\lfloor \frac{n}{2} \rfloor \leq \ell \leq n$ if $n \neq 1$ (mod 8);
2. $\lfloor \frac{n}{2} \rfloor \leq \ell \leq n$ if $n \equiv 1, 0$ (mod 8);
3. $n = 6$ and $\ell = 2$.

\(^1\) The second author is grateful to the Department of Mathematics of the University of Hawaii for its hospitality while this investigation was carried out.

\(^2\) The authors are grateful to the referee for simplifying some of the proofs.
Note. Theorem 2 implies that when \( n = 7 \) every even permutation is a product of three \( \ell \)-cycles if and only if \( \ell = 3, 5 \) or 7. Theorem 3 implies that when \( n = 6 \) every even permutation is a product of four \( \ell \)-cycles if and only if \( 2 \leq \ell \leq 6 \).

Based on these results, we wish to state a conjecture. For \( k \geq 2 \) let \( F(k, n) := f \) be the minimal integer such that
\[
A_n = [f, 1^{n-f}]^k.
\]

**Conjecture.** For \( k \geq 2 \),
\[
\left| F(k, n) - \frac{3n}{2k} \right| \leq 2 + \varepsilon(k)
\]
where
\[
\varepsilon(k) = \begin{cases} 
0 & \text{if } k \text{ is even} \\
1 & \text{if } k \text{ is odd.}
\end{cases}
\]

The bound \( 2 + \varepsilon(k) \) can be approximated arbitrarily closely, for example, when \( k \) is very large with respect to \( n \), because then
\[
F(k, n) = \begin{cases} 
2 & \text{if } k \text{ is even} \\
3 & \text{if } k \text{ is odd},
\end{cases}
\]
while
\[
F(k, n) - \frac{3n}{2k} \approx F(k, n).
\]

It follows from Proposition 15, which will be proved in our last Section V, that for \( n \geq 4 \) and \( k \geq 2 \)
\[
A_n = [\ell, 1^{n-\ell}]^k
\]
if and only if
\[
f \leq \ell \leq n
\]
with \( \ell \) odd if \( k \) is odd.

II. PRELIMINARIES

Let \( \Omega \) denote the set \{1, 2, ..., \( n \)\} and \( S_n \) the symmetric group of all permutations of \( \Omega \). The alternating group of all even permutations of \( \Omega \)
will be denoted by \( A_n \). If \( D \in S_n \), then \( \text{Supp}(D) \), the support of \( D \), is the set \( \{ i \in \Omega \mid D(i) \neq i \} \). Every permutation \( D \in S_n \) can be decomposed into a product of disjoint cycles, including the trivial 1-cycles. This disjoint cycle decomposition of \( D \) (denoted by \( d.c.d(D) \)) is unique, except for a cyclic shift within the cycles and the order in which the cycles are written. Products (i.e., compositions) of permutations will be executed from right to left. The identity permutation is denoted by \( 1 \). A cycle \( (i_1, i_2, ..., i_l) \) is said to have length \( l \), or to be an \( l \)-cycle.

Let \( d.c.d(D) = E_1 E_2 \cdots E_{c(D)} \cdots E_{c(D)} \), where \( d.c.d(D) \) has \( c(D) \) disjoint cycles including 1-cycles, and \( c^*(D) \) non-trivial cycles, written first. Define

\[
 r(D) := \sum_{i=1}^{c(D)} (e_i - 1),
\]

where \( e_i \) is the length of the cycle \( E_i \) (so \( e_i \geq 2 \) iff \( i \leq c^*(D) \)). Clearly

\[
 r(D) = n - c(D) = |\text{Supp}(D)| - c^*(D). \tag{1}
\]

If \( a_m \) is the number of \( m \)-cycles (i.e., cycles of length \( m \)) in the \( d.c.d(D) \), \( 1 \leq m \leq n \), then

\[
 n = \sum_{k \geq 1} 2ka_{2k} + \sum_{k \geq 0} (2k + 1) a_{2k+1}. \]

Thus \( c(D) = \sum_{k \geq 1} a_{2k} + \sum_{k \geq 0} a_{2k+1} \) and hence

\[
 r(D) = \sum_{k \geq 1} (2k - 1) a_{2k} + \sum_{k \geq 0} 2ka_{2k+1} \equiv \sum_{k \geq 1} a_{2k} \pmod{2}.
\]

It follows that \( r(D) \) is even if and only if \( D \in A_n \). Now

\[
 |\text{Supp}(D)| + c^*(D) = r(D) + 2c^*(D)
\]

and

\[
 n + c(D) = r(D) + 2c(D).
\]

Consequently \( |\text{Supp}(D)| + c^*(D) \) and \( n + c(D) \) are even if and only if \( D \in A_n \).

Let \( D \in A_n \) and define

\[
 e(D) := \frac{|\text{Supp}(D)| + c^*(D)}{2}.
\]

Then \( e(D) \) is an integer satisfying

\[
 e(D) \leq \left\lfloor \frac{n + \frac{n}{2}}{2} \right\rfloor = \left\lfloor \frac{3n}{4} \right\rfloor. \tag{2}
\]
We say that $D \in S_n$ belongs to the conjugacy class $[D] = [1^a_1, 2^a_2, 3^a_3, \ldots, n^a_n]$, where $\sum_i i a_i = n$. It is well known that the distinct conjugacy classes in $S_n$ are determined by the partitions of $n$ in this way. The conjugacy class of $\ell$-cycles is, of course, $[\ell, 1^{n-\ell}]$. If $K$ denotes a conjugacy class in $S_n$, then $r(K) := r(D)$ for any $D \in K$. When $K_1, K_2, K_3, \ldots, K_m$ are conjugacy classes in $S_n$, $[K_1 K_2 K_3 \ldots K_m]$ denotes the set of all permutations in $S_n$ which are a product $P_1 P_2 P_3 \ldots P_m$ where $P_i \in K_i$.

Note. In this paper $[D]$ denotes the conjugacy class of $D$ in $S_n$ even if $D \notin A_n$.

If $x$ is a real number, we denote by $\lfloor x \rfloor$ the integer $n$ which satisfies: $x \leq n < x + 1$, and by $\lceil x \rceil$ the integer $n$ satisfying $x - 1 < n \leq x$.

Our proofs rely strongly on the following result of R. Ree [Re]:

**Theorem 4 (Ree’s Theorem).** Suppose that $D_i \in S_n$ for $1 \leq i \leq k$ and $D_1 D_2 \cdots D_k = 1$.

If $T$ denotes the number of orbits of the group $\langle D_1, D_2, \ldots, D_k \rangle$ generated by the $D_i$, then

$$\sum_{i=1}^k r(D_i) \geq 2(n - T).$$

In particular, if $D_1, D_2, \ldots, D_{k-1}$ are $\ell$-cycles and $D = D_k^{-1} = D_1 D_2 \cdots D_{k-1}$, then $r(D_i) = \ell - 1$ for $i = 1, 2, \ldots, k - 1$, $r(D_k) = r(D) = n - c(D)$ and Ree’s theorem implies

$$\ell \geq \left\lceil \frac{n + c(D) + k - 2 T - 1}{k - 1} \right\rceil. \tag{3}$$

Ree’s theorem was originally proved by R. Ree in 1971 (see [Re]) using a formula for the genus of Riemann surfaces. In 1975 W. Feit et al. gave a direct combinatorial proof (see [Fe]). A third proof (also direct) was given in 1985 by Y. Dvir (see [DV]).

In addition to the above mentioned Theorem 1, we shall frequently use the following result from [Be]:

**Theorem 5 [Be, Theorem 2].** A permutation $D \in A_n$, $n \geq 1$, is a product of two $\ell$-cycles in $S_n$ if

$$e(D) = \frac{|\text{Supp}(D)| + e^*(D)}{2} \leq \ell \leq n.$$
III. CUBES OF CYCLE-CLASSES

In [DV, Chap. 3], Y. Dvir developed a theory dealing with products of permutations and conjugacy classes in $S_n$. As mentioned above, he was able to give a new proof of Ree's theorem. He also found the "extended covering number" of $A_n$: the least positive integer $m = m(n)$ such that for every collection $\{K_i\}_{i=1}^m$ of non-trivial conjugacy classes of $A_n$, $\Pi_i K_i = A_n$. Finally, he proved a sufficient condition for a class $K \subseteq S_n$ to satisfy $K^3 = A_n$ if $K \subseteq A_n$, and $K^2 = S_n - A_n$ if $K \subseteq S_n - A_n$. We will use this condition (Theorem 6 below) as well as two other results from his paper (Theorems 8 and 9 below), to characterize the cycle-classes $[\ell, 1^{n-\ell}]; \ell$ odd, such that $[\ell, 1^{n-\ell}]^3 = A_n$.

We remind the reader that in this paper $[D]$ always denotes the conjugacy class of $D$ in $S_n$ (even if $D \not\in A_n$).

**Theorem 6** [DV, Theorem 10.2]. Let $D \not\in S_n$ and $[D] \neq [2^k]$ for $k > 1$. If $r(D) \geq \frac{1}{2} (n-1)$, then $[D]^3 = A_n$ if $D \in A_n$ and $[D]^3 = S_n - A_n$ if $D$ is odd.

**Corollary 7.** If $\ell \geq \frac{n+1}{2}$ then

$$[\ell, 1^{n-\ell}]^3 = \begin{cases} A_n & \text{if } \ell \text{ is odd} \\ S_n - A_n & \text{if } \ell \text{ is even.} \end{cases}$$

We need two more results of Dvir. For this part only we follow Dvir’s notation. In particular we use $0_{\ell}$ instead of $[\ell, 1^{n-\ell}]$ to denote the class of $\ell$-cycles in $S_n$. When $A_1, A_2, \ldots, A_r$ are non-empty subsets of $S_n$, $(\prod_{i=1}^k A_i)_n$ denotes the set of all “transitive products” $a_1 a_2 \cdots a_r$, where $a_i \in A_i$ for $1 \leq i \leq r$, and the group $\langle a_1, a_2, \ldots, a_r \rangle$ generated by the permutations $a_i$ is transitive on $\{1, 2, \ldots, n\}$. Let $D_1, D_2, \ldots, D_k$ be conjugacy classes in $S_n$.

**Theorem 8** [DV, Theorem 7.5]. $1 \in 0_n \prod_{i=1}^k D_i$ if and only if the following two conditions hold:

(i) $r(0_n) + \sum_{i=1}^k r(D_i) \geq 2(n-1)$ and

(ii) $r(0_n) + \sum_{i=1}^k r(D_i) \equiv 0 \pmod{2}$.

**Theorem 9** [DV, Lemma 7.6]. Assume that at least one of $D_1, D_2$ is not $[2^k]$. Then $1 \in (0_{n-1}, D_1 D_2)_n$ if and only if the following two conditions hold:

(i) $r(0_{n-1}) + r(D_1) + r(D_2) \geq 2(n-1)$ and

(ii) $r(0_{n-1}) + r(D_1) + r(D_2) \equiv 0 \pmod{2}$.

We apply Theorems 8 and 9 in order to prove one more auxiliary result.
PROPOSITION 10. Let \( n \equiv 2 \) (mod 4). Then \( \lfloor \frac{n}{2}, 1^{n/2} \rfloor = A_n \).

Proof. We may assume \( n \geq 6 \). Clearly \( \lfloor \frac{n}{2}, 1^{n/2} \rfloor \subset A_n \) and \( \lfloor \frac{n}{2}, 1^{n/2} \rfloor \neq \lfloor 2^4 \rfloor \). It suffices to show that if \( C \) is any class in \( S_n \) and \( C \subset A_n \), then \( 1 \in D^3 C \), where \( D = \lfloor \frac{n}{2}, 1^{n/2} \rfloor \). If \( r(C) \geq \frac{n}{2} + 1 \), then \( r(C) + r(D) \geq \left( \frac{n}{2} + 1 \right) + \left( \frac{n}{2} - 1 \right) = n \) and by Theorem 9 \( 1 \in 0_{n-1} D C \). In \( S_{n-1} \), let \( D' = \lfloor \frac{n}{2}, 1^{n/2-1} \rfloor \), i.e., \( D \) less one of its 1-cycles. Then \( r(0_{n-1}) + r(D') + r(D') = 2(n - 2) \), so \( 1 \in 0_{n-1} D' \) in \( S_{n-1} \) by Theorem 8. But then \( 1 \in 0_{n-1} D' \) in \( S_{n} \) and together with \( 1 \in 0_{n-1} D C \) we conclude that \( 1 \in D^3 C \), as required.

So assume that \( r(C) < \frac{n}{2} + 1 \). By assumption \( \frac{n}{2} + 1 \) is even. Since \( C \subset A_n \), \( r(C) \) is also even, so \( r(C) \leq \frac{n}{2} - 1 \). Thus, letting \( f(C) \) denote the number of 1-cycles of \( C, \frac{1}{2} (n - f(C)) \leq r(C) \leq \frac{n}{2} - 1 \) and hence \( f(C) \geq 2 \). In \( S_{n-2} \), let \( D'' = \lfloor \frac{n}{2}, 1^{n/2-2} \rfloor \) and let \( C'' \) be the class of all permutations in \( S_{n-2} \) with two fewer 1-cycles than \( C \) has, but otherwise identical in cycle structure. Then \( r(D'') = \frac{n}{2} - 1 \geq \frac{1}{2} ((n - 2) - 1) \) and \( D'' \neq \lfloor 2^3 \rfloor \), so by Theorem 6 \( (D'')^3 = A_{n-2} \). Since \( C'' \subset A_{n-2} \), \( 1 \in (D'')^3 C'' \). But then in \( S_n \), \( 1 \in D^3 C \), as required.

We are now ready to approach the main problem of this section. First we prove the necessity of the conditions of Theorem 2.

LEMMA 11. Suppose every permutation in \( A_n \) is a product of three \( \ell \)-cycles. Then \( \ell \) is odd and either \( \lfloor \frac{n}{2} \rfloor \leq \ell \leq n \) or \( n = 7 \) and \( \ell = 3 \).

Proof. Clearly \( \ell \) must be odd and \( \ell \leq n \). For \( n = 1, 2 \) we have \( \ell = 1 \) and for \( n = 3, 4 \) it is easily seen that \( \ell = 3 \), as claimed. Assume, therefore, that \( n \geq 5 \). For each congruence class of \( n \) (mod 4) we choose a permutation \( D \in A_n \), with the d.c.l(D) containing at most one cycle of length \( \geq 3 \) and \( \mid \text{Supp}(D) \mid = n \). In each case, the given bound will be shown to be necessary. Suppose \( D = C_1 C_2 C_3 \), with each \( C_i \) an \( \ell \)-cycle, and let \( G = \langle C_1, C_2, C_3 \rangle \), the group generated by the \( C_i \). If \( G \) is transitive, Ree’s inequality (3) gives \( \ell \geq B \), where \( B \) is the smallest odd integer \( \geq \frac{2 + \sqrt{8n^3 + 1}}{3} \). This information is displayed in the following table:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( D )</th>
<th>( c(D) )</th>
<th>( B )</th>
<th>( n/2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4m</td>
<td>( (12)(34) \cdots (n - 1 \ n) )</td>
<td>2m</td>
<td>2m + 1</td>
<td>2m</td>
</tr>
<tr>
<td>4m + 1</td>
<td>( (12345)(67) \cdots (n - 1 \ n) )</td>
<td>2m - 1</td>
<td>2m + 1</td>
<td>2m + 1</td>
</tr>
<tr>
<td>4m + 2</td>
<td>( (1234)(56) \cdots (n - 1 \ n) )</td>
<td>2m</td>
<td>2m + 1</td>
<td>2m + 1</td>
</tr>
<tr>
<td>4m + 3</td>
<td>( (123)(45) \cdots (n - 1 \ n) )</td>
<td>2m + 1</td>
<td>2m + 3</td>
<td>2m + 2</td>
</tr>
</tbody>
</table>

In each case \( B \geq \lfloor \frac{n}{2} \rfloor \), so assume that \( G \) is not transitive. Considering the possible intersections of the three supports of the \( \ell \)-cycles, at least one orbit
of $G$ must have length $\ell$, and thus $\ell$ must be the length of a cycle of $D$ and $\ell < n$. Since $\ell$ must be odd, the only cases which arise in the above table are with $n$ odd. Hence, either $n \equiv 1 \pmod{4}$ and $\ell = 5$, or $n \equiv 3 \pmod{4}$ and $\ell = 3$. Because of our choice for $D$, $G$ cannot have three orbits, so $G$ must have exactly two orbits and Ree’s inequality (3) gives $n \leq 3\ell - c(D) + 1$. If $\ell = 5$ and $n \equiv 1 \pmod{4}$, then $c(D) = \frac{n-1}{2}$ and the inequality yields $n \leq 11$. Since $n > \ell = 5$, we conclude that $n = 9$ and $\ell = 5$, as claimed. If $\ell = 3$ and $n \equiv 3 \pmod{4}$, then $c(D) = \frac{n-1}{2}$ and the inequality yields $n \leq 7$, so $n = 7$.

The proof of the lemma is complete.

**Theorem 2.** Each permutation in $A_n$, $n \geq 1$, is a product of three $\ell$-cycles in $S_n$ if and only if $\ell$ is odd and either $\lceil \frac{n}{2} \rceil \leq \ell \leq n$ or $n = 7$ and $\ell = 3$.

**Proof.** By Corollary 7, if $\ell$ is odd and $\ell \geq \frac{n+1}{2}$, then $[\ell, 1^{n-\ell}]^3 = A_n$. Setting $n = 4m + r$ with $r \in \{0, 1, 2, 3\}$, it is easy to check that $\ell \geq \frac{n+1}{2}$ if $\ell$ is odd and $r = 0, 1$ or $3$. Thus it follows from the opening observation and Lemma 11 that the theorem is proved, except when $n = 7$ and $\ell = 3$, or $n = 4m + 2$.

When $n = 4m + 2$, Proposition 10 implies that $[[\frac{3}{2}, 1^{n-\frac{3}{2}}]]^3 = [2m+1, 1^{2m+1}]^3 = A_n$ and since $\lceil \frac{n}{2} \rceil = 2m + 1$ and here the smallest odd integer $\geq \frac{n+3}{2}$ is $2m + 3$, by the previous paragraph the theorem holds in this case too.

Finally, suppose that $n = 7$. By the previous paragraph (or direct construction) $[3, 1^3]^3 = A_6$, so for the set $S$ of permutations in $A_7$ with at least one 1-cycle, we have $[3, 1^4]^3 \subseteq S$. The other cases are represented by $(123)(45)(67) = (123)(476)(456)$ and $(1234567) = (167)(145)(123)$, so $[3, 1^4]^3 = A_7$ and the proof is complete.

**IV. FOURTH POWERS OF CYCLE-CLASSES**

Our aim in this section is to prove Theorem 3. First we prove a simple lemma.

**Lemma 12.** Every permutation in $A_n$ is the product of four transpositions if and only if $1 < n \leq 6$.

**Proof.** Suppose $n \geq 7$ and $(1234567) = (x_1, x_2)(x_3, x_4)(x_5, x_6)(x_7, x_8)$. Since $|\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}| \geq 7$ the right hand side of the above equation contains a disjoint 2-cycle, a contradiction. So $1 < n \leq 6$ and Lemma 12 follows from

$$(123) = (23)(13)^3, \quad (12)(34) = (12)(34)^3, \quad (12345) = (15)(14)(13)(12),$$


"
We are now ready to show that for \( n \geq 7 \) the conditions of Theorem 3 are necessary.

**Lemma 13.** Suppose every permutation in \( A_n \), \( n \geq 7 \), is the product of four \( \ell \)-cycles. Then \( \lceil \frac{n}{4} \rceil \leq \ell \leq n \) if \( n \not\equiv 1 \pmod{8} \), and \( \lfloor \frac{n}{4} \rfloor \leq \ell \leq n \) if \( n \equiv 1 \pmod{8} \).

**Proof.** By Lemma 12, we may assume that \( \ell \geq 3 \). For each congruence class of \( n \pmod{8} \) we choose a permutation \( D \in A_n \), with the d.c.d.(\( D \)) containing at most one cycle of length \( \geq 3 \) and \( |\text{Supp}(D)| = n \). In each case the given bound will be shown to be necessary. Suppose \( D = C_1 C_2 C_3 C_4 \), with each \( C_i \) an \( \ell \)-cycle, and let \( G = \langle C_1, C_2, C_3, C_4 \rangle \), the subgroup of \( S_n \) generated by the \( C_i \), while \( T \) is the number of orbits of \( G \).

Considering the possible intersections of the four supports of the \( \ell \)-cycles, if \( T \geq 3 \) then at least two of the orbits of \( G \) would be of length \( \ell \), and at least two of the cycles in the d.c.d.(\( D \)) would be of length \( \ell \), contrary to our choices for \( D \). Thus \( T < 2 \). If \( T = 1 \), then by Ree’s inequality \( \ell \geq \lceil \frac{n+4D-2}{4} \rceil := B_1 \), whereas if \( T = 2 \) Ree’s inequality \( \ell \geq \lceil \frac{n+4D-1}{8} \rceil := B_2 \). We display this information in the following table:

<table>
<thead>
<tr>
<th>( n )</th>
<th>( D )</th>
<th>( c(D) )</th>
<th>( B_1 )</th>
<th>( B_2 )</th>
<th>( \frac{3m}{8} )</th>
<th>( \frac{3n}{8} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>8m</td>
<td>((12)(34)\ldots(n-1\ n))</td>
<td>4m</td>
<td>3m+1</td>
<td>3m</td>
<td>3m</td>
<td>3m</td>
</tr>
<tr>
<td>8m+1</td>
<td>((12345)(67)\ldots(n-1\ n))</td>
<td>4m-1</td>
<td>3m-1</td>
<td>3m</td>
<td>3m+1</td>
<td>3m+1</td>
</tr>
<tr>
<td>8m+2</td>
<td>((1234)(56)\ldots(n-1\ n))</td>
<td>4m</td>
<td>3m+1</td>
<td>3m+1</td>
<td>3m+1</td>
<td>3m+1</td>
</tr>
<tr>
<td>8m+3</td>
<td>((123)(45)\ldots(n-1\ n))</td>
<td>4m+1</td>
<td>3m+2</td>
<td>3m+1</td>
<td>3m+2</td>
<td>3m+2</td>
</tr>
<tr>
<td>8m+4</td>
<td>((12)(34)\ldots(n-1\ n))</td>
<td>4m+2</td>
<td>3m+2</td>
<td>3m+2</td>
<td>3m+2</td>
<td>3m+2</td>
</tr>
<tr>
<td>8m+5</td>
<td>((12345)(67)\ldots(n-1\ n))</td>
<td>4m+1</td>
<td>3m+2</td>
<td>3m+2</td>
<td>3m+2</td>
<td>3m+2</td>
</tr>
<tr>
<td>8m+6</td>
<td>((1234)(56)\ldots(n-1\ n))</td>
<td>4m+2</td>
<td>3m+2</td>
<td>3m+2</td>
<td>3m+2</td>
<td>3m+2</td>
</tr>
<tr>
<td>8m+7</td>
<td>((123)(45)\ldots(n-1\ n))</td>
<td>4m+3</td>
<td>3m+3</td>
<td>3m+3</td>
<td>3m+3</td>
<td>3m+3</td>
</tr>
</tbody>
</table>

In case \( n = 8m+1 \), \( \lceil \frac{n}{4} \rceil = 3m = B_2 \), so whether \( T = 1 \) or \( T = 2 \) we obtain \( \ell \geq \lceil \frac{n}{4} \rceil \), as claimed. If \( n \equiv 1 \pmod{8} \), in each case except \( n \equiv 3 \) or 6 (mod 8) we see that \( \lceil \frac{n}{4} \rceil = B_2 \) and thus \( \ell \geq \lceil \frac{n}{4} \rceil \), again the conclusion sought. If \( T = 1 \) and \( n \equiv 3 \) or 6 (mod 8), then \( \lceil \frac{n}{4} \rceil = B_1 \) and thus \( \ell \geq \lceil \frac{n}{4} \rceil \), as claimed.

Hence we are finished unless \( T = 2 \) and either \( n = 8m+3 \) or \( n = 8m+6 \). Suppose some orbit of \( G \) consists of the support of exactly one \( \ell \)-cycle. Then \( \ell \) is the length of a cycle in d.c.d.(\( D \)) and \( n \geq 2\ell \). When \( n = 8m+3 \), our choice of \( D \) implies that \( \ell = 3 \) and an even permutation on \( 8m \) symbols, consisting of \( 4m \) transpositions is now a product of three 3-cycles, in
contradiction to Theorem 2. Otherwise \( n = 8m + 6, \ell = 4 \) and \( m \geq 1 \). Thus an odd permutation on \( 8m + 2 \geq 10 \) symbols, consisting of exactly \( 4m + 1 \) transpositions, is the product of three 4-cycles. Since \( T(G) = 2 \), the subgroup generated by these three 4-cycles is transitive, and by Ree’s theorem we have \((4m + 1) + 9 \geq 2(8m + 2 - 1)\), that is \( 8 \geq 12m \), a contradiction.

Hence each orbit of \( G \) consists of the support of exactly two \( l \)-cycles. So \( D \) restricts to an even permutation on each of these orbits, since there it is the product of two \( l \)-cycles. Let \( n_0 \) denote the shortest possible length for the longest orbit \( O \) of \( G \). Since \( D \) restricts to an even permutation on \( O \), if \( n = 8m + 3 \) then \( O \) must contain either the symbols of \( 2m + 2 \) disjoint transpositions or the symbols of one 3-cycle and \( 2m \) transpositions, disjoint from each other and from the 3-cycle. Thus \( n_0 \geq 4m + 3 \) and by Theorem 1

\[
\ell \geq \left\lceil \frac{3n_0}{4} \right\rceil \geq 3m + 2 = \left\lceil \frac{3n}{8} \right\rceil
\]
as claimed. Similarly, if \( n = 8m + 6 \), then \( n_0 \geq 4m + 4 \) and

\[
\ell \geq \left\lceil \frac{3n_0}{4} \right\rceil \geq 3m + 3 = \left\lceil \frac{3n}{8} \right\rceil
\]
and the proof of necessity is completed.

**THEOREM 3.** Each permutation in \( A_n, n \geq 2 \), is a product of four \( \ell \)-cycles in \( S_n \) if and only if:

1. \( \lceil \frac{3n}{8} \rceil \leq \ell \leq n \) if \( n \not\equiv 1 \pmod{8} \);
2. \( \lfloor \frac{3n}{8} \rfloor \leq \ell \leq n \) if \( n \equiv 1, 0 \pmod{8} \);
3. \( n = 6 \) and \( \ell = 2 \).

**Proof.** If \( \ell = 2 \) then by Lemma 12 \( 2 \leq n \leq 6 \). This establishes case (3), and since \( \lceil \frac{3n}{8} \rceil = 2 \) only for \( 2 \leq n \leq 5 \) and \( \lfloor \frac{3n}{8} \rfloor = 3 \) for \( n = 9 \), Theorem 3 holds for \( \ell = 2 \) and \( 2 \leq n \leq 6 \). Thus we may assume that \( n \geq 7 \) and \( \ell \geq 3 \).

By Lemma 13 the conditions in (1) and (2) are necessary, so we need only to show that they are sufficient.

Let \( n = 8k + s, 0 \leq s \leq 7 \) and let \( 3n = 4q + r, 0 \leq r \leq 3 \). Then \( q = \lceil \frac{3n}{8} \rceil \) and suppose \( D \in A_n \).

First suppose that \( q \) is odd, which corresponds to \( s = 2, 4, 5, \) or 7. We know by Theorem 1 that \( D \) is the product of two \( q \)-cycles and from Theorem 5 that each of these \( q \)-cycles is the product of two \( \ell \)-cycles, for any \( \ell \geq \frac{q+1}{2} \). Since \( \frac{q}{2} = \frac{s+1}{2} + \frac{r}{2} \), we see that \( \frac{q+1}{2} = \lceil \frac{3n}{8} \rceil \), and \( \ell \geq \lceil \frac{3n}{8} \rceil \) is sufficient whenever \( q \) is odd, i.e. whenever \( s = 2, 4, 5, \) or 7.
Suppose, from now on, that $q$ is even, which corresponds to $s = 0, 1, 3, 6$ and $r = 0, 3, 1, 2$, respectively. Then $D$ is the product of two $(q + 1)$-cycles, and if $\ell \geq \frac{q+2}{2}$ then $D$ is the product of four $\ell$-cycles, again by Theorems 1 and 5. Now $\frac{q+2}{2} = \frac{s+2}{2} + \frac{r}{2}$, so whenever $s = 3$ or $6$, $\ell = \frac{s+2}{2}$, and again $\ell \geq \frac{q+2}{2}$ is sufficient.

It remains to deal with the cases $s = 0, 1$ corresponding to $r = 0, 3$, respectively. Since if $s = 0$, $w_3(n) = n + 2$, and if $s = 1$, $w_3(n) = n + 3$, we must show that in both cases $\ell w_3(n)$ is sufficient. By inequality (2) in Section II $c(D) = |\text{Supp}(D)| + c^*(D) \leq \left\lfloor \frac{3n}{4} \right\rfloor = q$.

If $c(D) \leq q - 1$, then again by Theorem 5 $D$ is the product of two $(q - 1)$-cycles, so $D$ is the product of four $\ell$-cycles if $\ell \geq \frac{q}{2}$. But $\frac{q}{2} = \frac{2}{2} + \frac{r}{2}$ and we see that $\ell \geq \frac{q+2}{2}$ is sufficient.

Thus suppose that $c(D) = q$, so $3n = 4q + r = 2(|\text{Supp}(D)| + c^*(D)) + r$. Always $c^*(D) \leq \frac{|\text{Supp}(D)|}{2}$, so if $|\text{Supp}(D)| \leq n - 1$ we obtain $3 \leq r$ and hence $s = 1$, $r = 3$ and $|\text{Supp}(D)| = n - 1 = 2c^*(D)$. By Eq. (1) in Section II $c(D)$ $= n - |\text{Supp}(D)| + c^*(D) = 1 + c^*(D)$, whence it follows that

$$[D] = [(1)(23)(45)(67)(89) \cdots (n-1 \ n)], \quad s = 1. \quad (a)$$

We shall return to this case later.

Otherwise $|\text{Supp}(D)| = n$ and $n = 2c^*(D) + r$. If $s = 0$, then $r = 0$ and $c^*(D) = \frac{q}{2}$, yielding

$$[D] = [(12)(34)(56) \cdots (n-1 \ n)], \quad s = 0. \quad (b)$$

If $s = 1$, then $r = 3$, $c^*(D) = \frac{q-1}{2}$, $|\text{Supp}(D)| = n$ and if $u$ denotes the number of cycles of $D$ of length $\geq 3$, then $n \geq 3u + (\frac{q-1}{2} - u)2$, yielding $3 \geq u$. So, taking into account the fact that $D \in A_u$, we get the following 3 additional possible cases, corresponding to $u = 1, 2$ and 3, respectively,

$$[D] = [(12345)(67)(89) \cdots (n-1 \ n)], \quad s = 1, \quad (c)$$

$$[D] = [(1234)(567)(89) \cdots (n-1 \ n)], \quad s = 1 \quad (d)$$

and

$$[D] = [(123)(456)(789)(10 11) \cdots (n-1 \ n)], \quad s = 1. \quad (e)$$

It remains to deal with the 5 possible cases (a) through (e) above. Partition the set $\{1, 2, \ldots, n\}$ into two parts, the last $4k$ numbers and the remaining ones. If $s = 0$ or if $s = 1$ and $n > 9$, in each of the 5 possibilities above, $D$ is an even permutation on each part and thus, by Theorem 1, it can be
expressed on each part as a product of two ℓ-cycles for ℓ ≥ \left\lceil \frac{3(nk+1)}{n} \right\rceil = 3k = \left\lceil \frac{3n}{2} \right\rceil$, and our claim follows in these cases. This statement is also true if \( n = 9 \) and one of the cases (a) or (c) holds. So it remains to prove the sufficiency of \( \ell \geq \left\lceil \frac{3}{2} \right\rceil = 3 \) for \( [D] = [(1234)(567)(89)] \) and \( [D] = [(123)(456)(789)] \), i.e., to prove that
\[
[2, 3, 4] \cup [3^3] \subseteq [\ell, 1^{\ell-\ell}]^4 \quad \text{for } \ell \geq 3.
\]

By Theorem 2, \([2, 4] \subseteq [3, 1^3]^3\), whence
\[
\]

By Theorem 1, \([3, 1^6] \cup [2, 4, 1^3] \subseteq [\ell, 1^{\ell-\ell}]^2\) for \( \ell \geq 4 \), yielding
\[
[2, 3, 4] \subseteq [2, 4, 1^3][3, 1^6] \subseteq [\ell, 1^{\ell-\ell}]^4 \quad \text{for } \ell \geq 4.
\]

Thus \([2, 3, 4] \subseteq [\ell, 1^{\ell-\ell}]^4\) for \( \ell \geq 3 \), as claimed.

Finally, \([3^2, 1^3] \subseteq [3, 1^6]^2\) and by Theorem 1, \([3^2, 1^3] \subseteq [\ell, 1^{\ell-\ell}]^2\) for \( \ell \geq 4 \), so \([3^2, 1^3] \subseteq [\ell, 1^{\ell-\ell}]^2\) for \( \ell \geq 3 \). Clearly \([3, 1^6] \subseteq [3, 1^6]^2\), which together with Theorem 1 yields \([3, 1^6] \subseteq [\ell, 1^{\ell-\ell}]^3\) for \( \ell \geq 3 \). We may now conclude that
\[
[3^3] \subseteq [3^2, 1^3][3, 1^6] \subseteq [\ell, 1^{\ell-\ell}]^4 \quad \text{for } \ell \geq 3
\]
thus completing the proof of the theorem.

V. ON LENGTHENING CYCLES

We now prove Proposition 15 mentioned in the Introduction. First we need a preliminary lemma.

**Lemma 14.** Let \( S_n \) act on \( \Omega \) and let \( R \) be an \( r \)-cycle in \( S_n \) and \( S \) be an \( s \)-cycle in \( S_n \). Suppose that \( 2 \leq s \leq r \leq n-1 \). Then there exist an \((r+1)\)-cycle \( R' \) in \( S_n \) and an \((s+1)\)-cycle \( S' \) in \( S_n \) such that \( RS = R'S' \).

**Proof.** Let \( R = (a_1 \cdots a_r) \) and \( S = (b_1 \cdots b_s) \). We distinguish between two complementary cases.

Suppose, first, that \( \text{Supp } S \not\subseteq \text{Supp } R \). Then there exist \( a_i \not\in \text{Supp } S \) and \( b_j \not\in \text{Supp } R \). We may adjust notation so that: \( a_r \not\in \text{Supp } S \) and \( b_s \not\in \text{Supp } R \). Then
\[
RS = R(b_1 a_s)(b_1 a_r) S = (a_1 \cdots a_r b_1)(b_1 \cdots b_s a_r) = R'S'
\]
with \( |\text{Supp } R'| = r + 1 \) and \( |\text{Supp } S'| = s + 1 \), as required.
Suppose, next, that Supp $S \subseteq \text{Supp } R$. Adjust notation so that $b_1 = a_\ell$. As $r < n$, there exists $x \in \Omega - \text{Supp } R$ and

$$RS = R(xa_\ell)(b_1 x) S = (a_1 \cdots a_\ell, x)(b_1 \cdots b_n) = R'S$$

with $|\text{Supp } R'| = r + 1$ and $|\text{Supp } S'| = s + 1$, as required. 

**Proposition 15.** Let $\ell$, $k$, $n$ be integers, where $2 \leq \ell \leq n$ and if $k$ is even then $2 \leq \ell \leq n - 1$, while if $k$ is odd, then $2 \leq \ell \leq n - 2$. Suppose that $A_n = [\ell, 1^n - 1]^k$. Then $A_n = [\ell + 1, 1^n - 1]^k$ if $k$ is even, while $A_n = [\ell + 2, 1^n - \ell - 2]^k$ if $k$ is odd.

**Proof.** Suppose, first, that $k$ is even and consider

$$\pi = (C_1C_2)(C_3C_4)\cdots(C_{k-1}C_k) \in A_n,$$

where the $C_i$ are all $\ell$-cycles. Then, by Lemma 14, we get

$$\pi = (C_1'C_2')(C_3'C_4')\cdots(C_{k-1}'C_k'),$$

where the $C_i'$ are all $(\ell + 1)$-cycles. It follows that $A_n = [\ell + 1, 1^n - 1]^k$, as claimed.

Suppose, next, that $k$ is odd and consider

$$\pi = (C_1C_2)(C_3C_4)\cdots(C_{k-1}C_{k-2}C_{k-1})C_k \in A_n,$$

where the $C_i$ are all $\ell$-cycles. By the lemma we get

$$\pi = (C_1'C_2')(C_3'C_4')\cdots(C_{k-1}'C_{k-2}'C_{k-1})C_k,$$

where the $C_i'$ are all $(\ell + 1)$-cycles. As $\ell + 1 < n$, we may apply Lemma 14 again to the couples at the bottom line, obtaining

$$\pi = (C_1'C_2')(C_3'C_4')\cdots(C_{k-1}'C_{k-2}'C_{k-1})C_k = (C_1'C_2')(C_3'C_4')\cdots(C_{k-1}'C_{k-2}'C_{k-1})C_k,$$

where the $C_i''$ are all $(\ell + 2)$-cycles and $C_k''$ is an $(\ell + 1)$-cycle. Applying the Lemma once more to $(C_1'C_k')$ at the bottom line, we obtain

$$\pi = (C_1'C_k')(D_2D_3D_4\cdots D_{k-2}D_{k-1}),$$

where $C_1''$ and $C_k''$ are $(\ell + 2)$-cycles and the $D_i$, being equal to $(C_k')^{-1}C_i''C_k''$, are also $(\ell + 2)$-cycles. It follows that $A_n = [\ell + 2, 1^n - \ell - 2]^k$ as claimed. 


REFERENCES


