Even Permutations as a Product of Two Elements of Order Five

J. L. BRENNER

10 Phillips Road, Palo Alto, California 94303

AND

R. J. EVANS

Department of Mathematics, C-012,
University of California at San Diego, La Jolla, California 92093

Communicated by the Managing Editors

Received April 22, 1986

Let $A_n$ denote the alternating group on $n$ symbols. If $n = 5, 6, 7, 10, 11, 12, 13$ or $n \geq 15$, every permutation in $A_n$ is the product of two elements of order 5 in $A_n$. The same is true for $n \leq 14$, except for thirteen types of permutations, namely $3^1, 2^2, 2^4, 3^3, 2^31^41, 2^51, 2^64, 1^1, 1^2, 1^3, 1^4, 3^11^1, 2^41^1$. (For example, the permutation $(12)(34)(56)(78)(9)$ is not the product of two elements of order 5 in $A_n$.)

1. INTRODUCTION

Let $A_n$ denote the alternating group contained in the symmetric group $S_n$ on $n$ symbols. Throughout, $P$ denotes an element of $S_n$. Write $P = 2^53^24^11^3$, for example, to indicate that $P$ is the product of five 2-cycles, two 3-cycles, and one 4-cycle in $S_{23}$, all cycles disjoint. We say $P$ has type $T(P) = 2^53^24^11^3$ in such a case.

The two main results proved in this paper are

THEOREM 1. Let $n \leq 14$, $P \in A_n$. Then $P$ equals a product of two elements of order 5 in $A_n$ if and only if the type $T(P)$ is not one of $3^1, 2^2, 2^4, 3^3, 2^31^41, 2^51, 2^64, 1^1, 1^2, 1^3, 1^4, 3^11^1, 2^41^1$.

THEOREM 2. Let $n \geq 15$. Then every $P \in A_n$ is the product of two elements of order 5 in $A_n$. 196
Theorem 2 corrects the erroneous statement in [6, p. 39] that every element of $A_n$ is the product of two elements of order 5 in $A_n$ whenever $n > 11$. The corresponding theorem for order 3 [6, p. 39] is much easier to prove.

Theorems 1 and 2 have applications to problems on the universality of words in alternating groups. Parts of these theorems serve to complete proofs in [4]; see the second remark in [4, Sect. 2] and the second proof in [4, Sect. 4]. An immediate corollary of Theorem 2 is that for $n \geq 15$, the word $x^5y^5xy$ is universal in $A_n$; for another result of this type, see [9, Proposition 2(iii)]. In fact, it will be shown in Section 5 that $x^5y^5xy$ is universal in $A_n$ for $n \geq 5$. It has been conjectured that every word $W$ (in the free group on $x, y, ...$) which is not a proper power is $A_n$-universal for $n > n_0(W)$. Special cases of this conjecture have been proved in [4, 7, 9] with estimates of $n_0(W)$. The same conjecture in the unrestricted infinite symmetric group, posed in [8; 14, p. 48] has recently been proved by Lyndon [12], with the help of Mycielski [13].

Several interesting open problems arise in connection with Theorems 1 and 2.

**Problem 1.** For each integer $k \geq 2$, find the smallest integer $n_0(k)$, if it exists, such that when $n > n_0(k)$, every element of $A_n$ is the product of two elements of order $k$ in $A_n$.

It is known that $n_0(2)$ does not exist and that $n_0(3)$ is 2 [6, p. 39]. Theorem 2 above shows that $n_0(5) = 14$. In [3], it is shown that $n_0(7) = 27$ and that $n_0(k) = k + 1$ for all even $k$ with $6 < k < 20$. In [2], it is further shown that if $n > 7$, there is a class $C$ of period 6 in $A_n$ such that $CC = A_n$.

**Problem 2.** For each integer $k \geq 2$, find the smallest $n_1(k)$, if it exists, such that when $n > n_1(k)$, every element of $A_n$ is the product of two elements of order $k$ which are conjugate in $A_n$.

In [3], it is shown that $n_1(k) = k + 1$ for all even $k$ with $6 < k < 20$.

**Problem 3.** Let $n = n_0(k)$ (defined in Problem 1). Find a type of permutation in $A_n$ which is not the product of two elements of order $k$ in $A_n$.

It may be conjectured, e.g., that the type $2^2p^{-2}3^1$ cannot be written as a product of two elements of order $p$ in $A_{4p-1}$ for any prime $p \geq 7$. R. G. List has proved this for $p = 7$ using (1.1), a partial character table for $A_{27}$, and his computer program at the University of Birmingham. One might also conjecture that for prime $p \equiv 1 \pmod{4}$, the type $2^{(3p-5)/2}4^1$ cannot be written as the product of two elements of order $p$ in $A_{3p-1}$; this is true for $p = 5$ by Theorem 1.
PROBLEM 4. Find the smallest \( n_2(k) \), if it exists, such that when \( n > n_2(k) \), every element of \( A_n \) is the product of two elements each of which is a product of disjoint \( k \)-cycles in \( A_n \).

PROBLEM 5. Find the smallest \( n_3(k) \), if it exists, such that for \( n > n_3(k) \), every element of \( A_n \) is the product of two conjugate (in \( A_n \)) elements each of which is a product of disjoint \( k \)-cycles in \( A_n \).

PROBLEM 6. Find the integers \( k > 1 \) for which the following assertion is true: For all \( m \geq 1 \), every element of \( A_{km} \) is a product of two elements of type \( k^m \) in \( S_{km} \).

The assertion is false for \( k = 2, 3 \), and true for \( k = 4 \) [5, p. 103]. We conjecture that it is true for every \( k \geq 4 \).

A somewhat different type of problem is to find the smallest \( N(k, n) \) for which every element of \( A_n \) is a product of at most \( N(k, n) \) \( k \)-cycles in \( A_n \). This has been studied by Herzog and Reid [10].

Let \( C_1, C_2, \ldots \) be the conjugacy classes in a finite group \( G \), with representatives \( g_i \in C_i \). Let \( a_{ijk} \) denote the number of ordered pairs \( x \in C_i, y \in C_j \) such that \( xy = g_k \). It is well known [11, pp. 15, 453] that

\[
a_{ijk} = \frac{|C_i| |C_j|}{|G|} \sum_x \frac{\chi(g_i) \chi(g_j) \bar{\chi}(g_k)}{\chi(1)},
\]

where the sum is over all the irreducible characters of \( G \). Thus Theorem 1 can in principle be proved using character tables for \( A_n, n \leq 14 \). Character tables seem to offer little hope for extension to general orders \( k > 5 \) or for solution of Problems 1–6.

2. Factorization of Special Types

The inductive proofs of Section 4 are based on the (starting) formulas of this section. For ease in expressing permutations \( P \) in Sections 2 and 3 as products of cycles, let \( \{1, 2, \ldots, n\} \) be the set of symbols on which \( S_n \) acts, but write \( A, B, C, \ldots \) in place of symbols 10, 11, 12, \ldots moved by \( P \).

In (2.1)-(2.24), certain types of permutations \( P \in A_n \) are factored. Each of the 24 formulas has the form \( C_1 C_2 \cdots C_r = QR \sim T(P) \). Here, \( C_1 \cdots C_r \) is the canonical factorization of \( P \) into disjoint cycles \( C_i \) in \( S_n \); each factor \( Q, R \) has order 5; and \( R \) is one of \( R_1, R_2, R_3, R_4 \), where \( R_1 = (12345), R_2 = R_1(67894), R_3 = R_2(BCDEF), R_4 = R_3(GHIJK) \). Multiplication is performed from left to right, so that, e.g., \( (12)(23) = (132) \).

In each formula \( C_1 \cdots C_r = QR \sim T(P) \) in (2.1)-(2.18), certain symbols occurring in the cycles \( C_i \) are underlined; each underlined symbol is moved
by exactly one of $Q$, $R$. For example, in (2.11), $B$ is moved by $Q$ but not by $R$, while $7$ is moved by $R$ but not by $Q$. Underlined symbols will be referred to when Lemma 3 is applied to prove Lemma 4 in Section 4.

\[
(16)(5342) = (16524) \ R_1 \sim 2^1 4^1 \qquad (2.1)
\]

\[
(16)(578234) = (16578) \ R_1 \sim 2^1 6^1 \qquad (2.2)
\]

\[
(1345)(6782) = (12678) \ R_1 \sim 4^2 \qquad (2.3)
\]

\[
(1367245) = (12367) \ R_1 \sim 7^1 \qquad (2.4)
\]

\[
(123456789) = (56789) \ R_1 \sim 9^1 \qquad (2.5)
\]

\[
(165)(243) = (16423) \ R_1 \sim 3^2 \qquad (2.6)
\]

\[
(165)(23478) = (16478) \ R_1 \sim 3^1 5^1 \qquad (2.7)
\]

\[
(16)(57)(234) = (16574) \ R_1 \sim 2^2 3^1 \qquad (2.8)
\]

\[
(1B)(5C)(42D7896A3) = (1B5C4)(D69A2) \ R_2 \sim 2^3 9^1 \qquad (2.9)
\]

\[
(1B)(574)(239D8A6C) = (1B56C)(D7398) \ R_2 \sim 2^1 3^1 8^1 \qquad (2.10)
\]

\[
(69A)(B234)(1785) = (B1684) \ R_2 \sim 3^1 4^2 \qquad (2.11)
\]

\[
(1B5)(4C73)(2D98A6) = (1B4C6)(72D89) \ R_2 \sim 3^1 4^1 6^1 \qquad (2.12)
\]

\[
(18)(74)(A9)(35)(B62) = (17346)(852BA) \ R_2 \sim 2^3 4^3 \qquad (2.13)
\]

\[
(1B)(5C)(7D)(6A)(94238) = (1B5C4)(D6937) \ R_2 \sim 2^4 5^1 \qquad (2.14)
\]

\[
(16)(57)(38)(9A42) = (16574)(3829A) \ R_1 \sim 2^3 4^1 \qquad (2.15)
\]

\[
(17)(43)(9B)(C852A6) = (16C75)(429B8) \ R_2 \sim 2^3 6^1 \qquad (2.16)
\]

\[
(17)(5C)(6A)(43)(9G)(82EFDBHI) = (169G8)(75BHI)(C42DF) \ R_3 \sim 2^5 8^1 \qquad (2.17)
\]

\[
(17)(6C)(A9)(82)(5B)(34) = (16CA8)(75B42) \ R_2 \sim 2^6 \qquad (2.18)
\]

\[
(1A)(27)(5C)(86)(4B)(39)(FED) = (26719)(8A5B3)(C4FDE) \ R_3 \sim 2^6 3^1 \qquad (2.19)
\]

\[
(1AD)(27C)(368)(4B9)(5FE) = (267B8)(193A)(4FD5E) \ R_3 \sim 3^5 \qquad (2.20)
\]

\[
(2B)(1C7)(48F)(5DE)(3496) = (2B1C6)(75DE4)(8F39A) \ R_2 \sim 2^4 3^3 4^1 \qquad (2.21)
\]
\begin{align*}
(15)(2G)(37)(48)(AF)(84)(9D)(EB) & = (1472G)(36BD8)(9CAEF) R_3 \sim 2^8 \\
(14)(35)(6C)(80)(9B)(7FEA)(2) & = (13452)(6B8CA)(9FD7E) R_3 \sim 2^{5} 4^{1} 1^{1}.
\end{align*}

3. Proof of Theorem 1

Let $B_n$ be the subset of $A_n$ consisting of those $P \in A_n$ which are products of two elements of order 5 in $A_n$. By [4, Lemma 4] with $b=5$, we see that $A_n = B_n$ when $5 \leq n \leq 7$. By [4, Lemma 5] with $u=v=5$, $A_n = B_n$ when $10 \leq n \leq 13$. If $n \leq 4$, $A_n$ has no element of order 5, so none of the types $1^1$, $1^2$, $1^3$, $1^4$, $3^11^1$, $3^1$, $2^2$, $4^1$ is in $B_n$. It remains to consider the values $n=8$, $9$, and 14.

For $P \in A_n$, let $c$ denote the number of nontrivial cycles in the canonical decomposition of $P$ into disjoint cycles, and let $t$ be the number of symbols occurring in these $c$ cycles. Thus $P$ fixes $n-t$ symbols.

First let $n=8$ or 9. Then the only elements of order 5 in $A_n$ are of type $5^11^{n-5}$. By [1, Theorem 2.02], $P \in A_n$ is a product of two 5-cycles in $A_n$ (i.e., $P \in B_n$) if $t+c \leq 10$. Since $t+c$ is even for $P \in A_n$, $t+c \geq 10$ implies $t+c \geq 12$. If $P \in A_n$ has $t+c \geq 12$, then $P$ has one of the types $2^4$, $3^3$, $2^13^14^1$, $2^25^1$, $2^14^1$; it is easily checked that $P \notin B_n$ for each such $P$.

Finally, let $n=14$. Setting $I=(5, 5)$ in the theorem in [1, p. 168] (note the misprints listed in the first remark of [4, Sect. 3]), we see that $P \in B_{14}$ for each $P \in A_{14}$ such that $t+c < 20$. If $P \in A_{14}$ has $t+c \geq 20$, then $T(P) - 254^1$ or $T(P) - 2^{43^2}$. Since the type $2^{43^2}$ can be thought of as a product of two permutations each of type $2^23^1$, it follows from (2.8) that $P \in B_{14}$ when $T(P) = 2^{43^2}$. It remains to show that $P \notin B_{14}$ when $T(P) = 2^54^1$. Using a file of the characters of $A_{14}$, Ursula Bicker of RWTH (Aachen) has confirmed this. (Moreover, the computer printout showed that every element of $A_{14}$ not of type $2^54^1$ is a product of two elements each of type $5^21^4$.) We present another proof, since the combinatorial methods may be of interest.

Assume $P \in B_{14}$, $T(P) = 2^54^1$. Without loss of generality, $P = C_1C_2R$, where $C_1$ and $C_2$ are disjoint 5-cycles in $A_{14}$ and $R = (56789)(ABCDE)$. It is not difficult to check that among the symbols 1, 2, 3, 4 (i.e., the symbols fixed by $R$), no three can occur in either $C_1$ or $C_2$. Thus, without loss of generality,
1, 2 occur in $C_1$, and 3, 4 occur in $C_2$. \hfill (3.1)

Since $RC_1C_2$ has the same type as $P$, an analogous argument, with $(56789)$, $(ABCDE)$, and $C_1C_2$ in place $C_1$, $C_2$, and $R$, respectively, shows that

exactly three of 5, 6, 7, 8, 9, and exactly three of $A$, $B$, $C$, $D$, $E$, occur in $C_1C_2$. \hfill (3.2)

By (3.1), we need only consider the three cases $C_1C_2 = (12uvw)(34xyz)$, $C_1C_2 = (12uvw)(3x4yz)$, and $C_1C_2 = (1u2vw)(3x4yz)$, since the second case is equivalent to $C_1C_2 = (1u2vw)(34xyz)$ after suitable renumbering. Without loss of generality, $w = 5$ throughout.

First suppose that

$$P = C_1C_2R = (12uw5)(34xyz)(56789)(ABCDE).$$

Since $T(P) = 2^54^1$, we have $P = (5 \ 12 \ R(u))...$, where $R(u)$ is the image of $u$ under $R$. Now $P(3) = 4$ but $P(4) \neq 3$, which contradicts the fact that $T(P) = 2^54^1$.

Next suppose that

$$P = C_1C_2R = (12uw5)(3x4yz)(56789)(ABCDE).$$

Either $u = 6, 7, 8, 9$, or, without loss of generality, $A$. If $u = A$, then $P = (512B) \ (x4)...$. Since $P(B) = 5$, this forces $y = B, z = 9$. Since $P(4) = x$, this forces $x = C$. Now, $P(9) = 3$ but $P(3) \neq 9$, a contradiction. If $u = 6$, then $P = (5127)...$, so $P(v) - 6$, $P(6) \neq v$. If $u - 7$, then $P = (5128)...$. Then $P(8) = 5$, which forces $y = 8, z = 9$. Now $P(4) = 9, P(9) \neq 4$. If $u = 9$, then $P = (512)...$, which is absurd. Thus $u = 8$. If $v = 6$, then $P(6) = 6$. If $v = 7$, then $P(8) = 8$. If $v = 9$, then $P = (5296)...$. Thus $v = A$, without loss of generality, so $P = (5129)(8B)....$ Since $P(B) = 8$, this forces $y = B, z = 7$. Now $P(A) = 6, P(6) \neq A$, a contradiction.

Finally, suppose that

$$P = C_1C_2R = (1u2v5)(3x4yz)(56789)(ABCDE).$$

Observe that $P(5) = 1$. There are two cases.

Case 1. $P = (51)...$

Since $P(1) = 5, u = 9$. Either $v = 6, 7, 8$, or, without loss of generality, $A$. If $v = 6$, then $P(6) = 6$. If $v = 7$ or $v = 8$, then $x, y, z > 9$ by (3.2), so $P = (892)$ or $P = (867)...$, respectively. Thus $v = A$. Then $P = (92Bf)$ for some symbol $f$. Since $P(A) = 6$, we have $P(6) = A$, which forces $y = 6, z = E$. Then $P(4) = 7$, so $P(7) = 4$, which forces $x = 7$. Now $P(3) = 8, P(8) \neq 3$, a contradiction.
Case 2. $P = (5 \ 1 \ R(u) \ f)\ldots$ for some symbol $f$.

Since $P(u) = 2, f \neq 2$. Thus $P = (5 \ 1 \ R(u) \ f)\ldots u \ldots$. Suppose that $f = 6$. Then $P(6) = 5$, which forces $v = 6, z = 9$. Since $P(9) = 3$, we have $P(3) = 9$, so $x = 8$. Now $P(8) = 4, P(4) \neq 8$. Thus $f \neq 6$, so

$$P = (5 \ 1 \ R(u) \ f)\ldots u\ldots$$

(3.3)

Suppose that $y = 6$. Then $P(4) = 7$, so $P(7) = 4$. Thus $x = 7$. By (3.2), $u, v, z > 9$. Now $P(3) = 8, P(8) \neq 3$. Thus $y \neq 6$. Moreover, by (3.3) none of $u, v, x, z$ can be 6. Thus the symbol 6 does not occur in $C_1 C_2$, so $P(6) = 7$. Then $v = 7$, by (3.3). It follows that $P(2) = 8$, so $u = 8$ by (3.3). By (3.2), $x, y, z > 9$. Thus $P(9) = 5$, so $f = 9$. However, $R(u) = R(8) = 9 = f$, which contradicts (3.3). \[\blacksquare\]

4. Proof of Theorem 2

We give an inductive proof of Theorem 2 based on two ideas. The first is concatenation. For example, the type $2^53^14^41^1$ is seen to lie in $B_{18}$ because it is the concatenation of the two types $2^41^11^1, 2^43^1$ which lie in $B_7, B_{11}$, respectively, by Theorem 1. The second idea is a "stitching" argument, embodied in Lemma 3. Lemma 3 asserts that if the type $c_1^i\ldots c_r^i$ is in $B_n (n = \sum c_i)$, then under a certain condition, the type $(c_1 + 4a_1)^1\ldots(c_r + 4a_r)^1$ is in $B_m (m = \sum (c_i + 4a_i))$ for any $r$-tuple of nonnegative integers $a_1,\ldots, a_r$. (Here $4a_i$ symbols have been stitched into the cycle of length $c_i (1 \leq i \leq r)$.)

**Lemma 3.** Let $1 \leq s \leq r$ and let $P = C_1 \cdots C_r \in A_n$, where the $C_i$ are non-trivial disjoint $c_i$-cycles in $S_n$. Suppose that $P = QR$, where $Q$ and $R$ each have order 5 in $A_n$. Suppose further that for each $i \leq s$, there is a symbol occurring in $C_i$ which is moved by exactly one of $Q, R$. Let $a_1,\ldots, a_r$ be any $s$-tuple of nonnegative integers. Then every permutation of type $(c_1 + 4a_1)^1\cdots(c_r + 4a_r)^1$ is expressible as the product of two elements of order 5 in $A_m (m = n + 4 \sum a_i)$.

**Proof.** We begin by considering the case $a_1 = 1, a_2 = \cdots = a_s = 0$. It may be supposed that 1 is a symbol occurring in $C_1$ which is moved by exactly one of $Q, R$, and that the symbols $w, x, y, z$ are not moved by $P$. Let $P^*$ be the permutation in $A_{n+4}$ obtained from $P$ by replacing each $C_i$ by $C_i^*$, where $C_i^* = C_i$ for $i > 1$ and $C_1^*$ is the $(c_1 + 4)$-cycle equal to $C_1(1wxyz)$ or $(1wxyz)C_1$ according as $Q$ or $R$ moves 1. Then $P^* = Q(1wxyz) R = Q^* R^*$, where

<table>
<thead>
<tr>
<th>$Q^* = Q(1wxyz)$</th>
<th>$R^* = R$</th>
<th>if $R$ moves 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q^* = Q$</td>
<td>$R^* = (1wxyz) R$</td>
<td>if $Q$ moves 1</td>
</tr>
</tbody>
</table>
Note that $Q^*$ and $R^*$ have order 5 in $A_{n+4}$. Moreover, for each $i \leq s$, there is a symbol occurring in $C_i^*$ that is moved by exactly one of $Q^*$, $R^*$ (the symbol $z$ may be taken in the case $i = 1$). Thus the result for $a_1 = 1$, $a_2 = \cdots = a_s = 0$ is proved and the general result follows by induction on $\sum a_i$.

From now on, $d$ is an odd integer $\geq 3$, and $e, e_1, e_2$ are even integers $\geq 2$. Define $B_n$ as in Section 3.

**Lemma 4.** Each of the following types of permutations in $A_n$ lies in $B_n$:

- $d^1 \text{ if } d \geq 7$ (4.1)
- $e_1^1e_2^1 \text{ if } e_1 + e_2 \geq 6$ (4.2)
- $3^1e_1^1e_2^1 \text{ if } e_1 + e_2 \geq 8$ (4.3)
- $3^1d^1 \text{ if } d \geq 3$ (4.4)
- $2^5e^1 \text{ if } e \geq 6$ (4.5)
- $2^4d^1 \text{ if } d \geq 3$ (4.6)
- $2^3e^1 \text{ if } e \geq 4$ (4.7)
- $2^2d^1 \text{ if } d \geq 7$. (4.8)

**Proof.** The result will follow from Lemma 3 after it is proved for appropriate initial cases. Thus (2.4) and (2.5) yield the result for (4.1). Further, use (2.1)–(2.3) for (4.2); (2.8) and (2.10)–(2.12) for (4.3); (2.6)–(2.7) for (4.4); (2.17)–(2.18) for (4.5); (2.13)–(2.14) for (4.6); (2.15)–(2.16) for (4.7); and (2.8)–(2.9) for (4.8).

Let $A'_n$, $S'_n$ denote the set of permutations in $A_n$, $S_n$, respectively, with no fixed points. By convention, $A'_0$ consists of the identity permutation. For $P \in S_n$, $P = P_1 \cdot P_2$ means that $P$ is the product of disjoint $P_1$, $P_2 \in S_n$. Often we will view $P_i \in S'_n$, where $t_i$ is the number of symbols moved by $P_i$. We may also use notation such as $P = P_1 \cdot 2^13^2$, for example, if $P = P_1 \cdot P_2$ with $T(P_2) = 2^13^2$.

Theorem 2 states that for $n \geq 15$, $P \in B_n$ whenever $P \in A_n$. We first prove this in case $P$ has no fixed points (Lemma 5) and then prove Theorem 2 in complete generality.

**Lemma 5.** Suppose that $P \in A'_n$, $P \notin B_n$ for some $n \geq 1$. Then $P \in S$, where $S$ is the set of permutations of types $3^1, 2^2, 2^4, 3^3, 2^13^14^1, 2^25^1, 2^44^1$ (so in particular, $n \leq 14$).

**Proof.** Assume that it is possible to choose $P \in A'_n$, $P \notin B_n$ with $n \geq 1$
minimal such that \( P \notin S \). By Theorem 1, \( n \geq 15 \). By Lemma 4, \( P \) cannot have the type (4.1) or (4.2). Thus \( P = P_1 \cdot P_2 \) for some nontrivial \( P_i \in A_i \). One of \( P_1, P_2 \) is in \( S \); otherwise, by minimality of \( n \), each \( P_i \) is in \( B_n \) and consequently \( P \) would be in \( B_n \).

We now claim that \( P \) has the form \( P = V \cdot W \) where either

\[
V \sim 3^2 \tag{4.9}
\]
\[
V \sim 2^1 4^1 \tag{4.10}
\]
\[
V \sim 5^1 \tag{4.11}
\]
\[
V \sim 3^1 2^2, \quad T(W) \text{ has no } 3, 4, \text{ or } 5\text{-cycles} \tag{4.12}
\]
\[
V \sim 3^1 2^1, \quad T(W) \text{ has no } 2, 3, 4, \text{ or } 5\text{-cycles} \tag{4.13}
\]
\[
V \sim 3^1, \quad T(W) \text{ has no } 2, 3, \text{ or } 5\text{-cycles} \tag{4.14}
\]

or

\[
V \sim 2^m (m \geq 2), \quad T(W) \text{ has no } 2, 3, 4, \text{ or } 5\text{-cycles.} \tag{4.15}
\]

If \( 3^2, 2^1 4^1, \text{ or } 5^1 \) is a factor of \( T(P) \), obviously (4.9), (4.10), or (4.11) holds, respectively. Now suppose none of \( 3^2, 2^1 4^1, 5^1 \) are factors of \( T(P) \). Then, since \( P = P_1 \cdot P_2 \) with one of \( P_1, P_2 \) in \( S \), it follows by definition of \( S \) that either \( 3^1 \) or \( 2^2 \) is a factor of \( T(P) \). If \( 3^1 \) is a factor of \( T(P) \), clearly one of (4.12), (4.13), (4.14) holds. Finally, if \( 3^1 \) is not a factor of \( T(P) \), then \( 2^2 \) is a factor of \( T(P) \) and (4.15) holds for some \( m \geq 2 \).

We will obtain a contradiction by ruling out (4.9)--(4.15). The idea is to show that \( W \) or some particular factor of \( W \) must lie in \( S \); this will lead to a contradiction. At this point, note that \( V \in S_n, W \in S_k \), where \( k = n - 6 \geq 9 \) if (4.9) or (4.10) holds, \( k = n - 5 \geq 10 \) if (4.11) or (4.13) holds, etc.

**Case 1.** One of (4.9)--(4.12) holds.

By Theorem 1, \( V \in B_{n-k} \). Thus \( W \notin B_k \) because \( P = V \cdot W \notin B_n \). By minimality of \( n \),

\[
W \in S. \tag{4.16}
\]

Say (4.12) holds. Then \( W \sim 2^4 \) and \( P \sim 3^1 2^6 \), since \( W \in S \), \( T(W) \) has no 3, 4, or 5-cycles, and \( n \geq 15 \). Thus by (2.19), \( P \in B_n \), a contradiction.

Say (4.11) holds. Then \( W \sim 2^4 1 \) and \( P \sim 2^5 4^1 5^1 = (2^4 1) \cdot (2^5 5^1) \). Theorem 1 shows that these (even) permutations in parentheses lie in \( B_9 \) and \( B_{13} \), respectively. Thus we again arrive at the contradiction \( P \in B_n \).

Say (4.10) holds. Then \( T(P) \) is one of \( 2^4 1^3, 2^2 4^2 3^1, 2^3 4^1 5^1, 2^5 4^2 \). In
PRODUCT OF ELEMENTS OF ORDER FIVE

view of (2.21) and the factorizations $2^2 4^2 3^1 = (2^2 3^1) \cdot (4^2)$, $2^4 4^1 5^1 = (2^3 4^1) \cdot (5^1)$, and $2^6 4^2 = (2^3 4^1) \cdot (2^3 4^1)$, we obtain $P \in B_n$.

Finally, say (4.9) holds. Then $T(P)$ is one of $3^2 2^4 1^1$, $3^2 2^2 5^1$, $3^2 1^4 1^1$, $3^5$. In view of (2.20)–(2.21) and the factorizations $3^2 2^4 1^1 = (2^3 3^1) \cdot (2^3 3^1) \cdot (2^1 4^1)$ and $3^2 2^5 1^1 = (2^3 1^1) \cdot (3^1 5^1)$, we obtain $P \in B_n$.

Case 2. (4.13) holds.

Since $W$ is odd, $W = X \cdot e^1$ for some (even) $e \geq 6$ and some $X \in A_{k-e}$. In view of (4.3), $X$ is nontrivial, and by the proof of (4.16), $X \in S$. This contradicts the fact that $T(W)$ has no 2- or 3-cycles.

Case 3. (4.14) holds.

Since $W \in A_{n-3}$, either $W = X \cdot d^1$ or $W = X \cdot e^1_1 e^1_2$, for (odd) $d \geq 7$, (even) $e_i \geq 4$, and some $X \in A_{k-f}$, where $f = d$ or $e_1 + e_2$. By (4.3) and (4.4), $X$ is nontrivial, and by the proof of (4.16), $X \in S$. This contradicts the fact that $T(W)$ has no 2- or 3-cycles.

Case 4. (4.15) holds.

First suppose $m \geq 6$. Then $P = X \cdot Y$, for $X \sim 2^6$, $Y \in A_{n-12}$, where $T(Y)$ has no 3, 4, or 5-cycles. By Theorem 1, $X \in B_{17}$, so by the proof of (4.16), $Y \in S$. Thus $Y \sim 2^2$ or $Y \sim 2^4$, so $P \sim 2^8$ or $P \sim 2^{10}$. In view of (2.22)–(2.23), we obtain the contradiction $P \in B_n$.

Next suppose that $m = 3$ or 5. Since $W$ is odd, $W = X \cdot e^1$ with $e \geq 6$, $X \in A_{k-e}$. By (4.5) or (4.7), $X$ is nontrivial. We have $P = Y \cdot Z$ for $Y \sim 2^1 e^1$, $Z = X \cdot 2^m 1^1$, where $Z \in A_{k-f}$ with $f = e - 2^m 1^1$. By (4.2), $Y \in B_{e+2}$. Thus, by the proof of (4.16), $Z \in S$. This contradicts the facts that $T(X)$ has no 2- or 5-cycle and $X$ is nontrivial.

Finally, suppose that $m = 2$ or 4. Then $W = X \cdot d^1$ or $W = X \cdot e^1_1 e^1_2$ with $d \geq 7$, $e_i \geq 4$, $X \in A_{k-f}$, where $f = d$ or $e_1 + e_2$. First suppose that $W = X \cdot d^1$. By (4.6) or (4.8), $X$ is nontrivial. We have $P = Y \cdot Z$ for $Y \sim d^1$, $Z = X \cdot 2^m 1^1$. By (4.1), $Y \in B_d$, so, by the proof of (4.16), $Z \in S$. This contradicts the fact that $T(X)$ has no 2 or 5-cycles and $X$ is nontrivial. Now suppose that $W = X \cdot e^1_1 e^1_2$. We have $P = Y \cdot Z$ for $Y \sim 2^1 e^1_1$, $Z = X \cdot 2^m 1^1 e^1_2$. By (4.2), $Y \in B_d$, so $Z \in S$. This contradicts the fact that $T(X)$ has no 2 or 3-cycles.

Proof of Theorem 2. Fix $n \geq 15$ and assume that $P \in A_n$, $P \notin B_n$. Let $P' \in A'_i$ be obtained from $P$ by ignoring the $n-t$ fixed points of $P$. By Lemma 5, $P' \in S$. It must be the case that $P' \sim 2^5 4^1$; otherwise we would have $P \in B_{15}$, because by Theorem 1, $B_{10}$ contains every permutation of type $3^1 1^7$, $2^2 1^6$, $2^4 1^2$, $3^1 1^1$, $2^1 3^1 4^1 1^1$, or $2^5 1^1 1^1$. Thus $T(P' \cdot 1^1) = 2^5 4^1 1^1$, so $P' \cdot 1^1 \in B_{15}$ by (2.24). Thus $P = P' \cdot 1^{n-14} \in B_n$, a contradiction.
5. UNIVERSALITY OF $x^5 y^5 x y$

We prove the following corollary of Theorems 1 and 2.

**Theorem 3.** If $n \geq 5$, the word $x^5 y^5 x y$ is universal in $A_n$.

**Proof.** In view of Theorems 1 and 2, it suffices to show that for each of $P_1 \sim 2^4$, $P_2 \sim 2^4 1^1$, $P_3 \sim 3^3$, $P_4 \sim 2^3 1^4$, $P_5 \sim 2^2 5^1$, and $P_6 \sim 2^2 4^1$, there exist appropriate $x_i, y_i$ such that $P_i = x_i^5 y_i x_i y_i$. Choose

\[
\begin{align*}
  x_1 &= x_2 = (1234)(5678), & y_1 &= y_2 = (13)(24)(57)(68), \\
  x_3 &= (123)(456)(789), & y_3 &= (234)(567)(891), \\
  x_4 &= (12)(3456)(789), & y_4 &= (123)(46789), \\
  x_5 &= (13)(24)(5689), & y_5 &= (123); \text{ and} \\
\end{align*}
\]

**References**

2. J. L. Brenner, Covering theorems for finite nonabelian simple groups XI. Covering of $A_n$ by the square of a class of period 6, preprint.
3. J. L. Brenner, Unpublished manuscript.