Some Result about a Product of Conjugate Cycles

Shaimaa Salman Al-Bundi
Department of Mathematics, College of Education, Ibn Al-Haithm, Baghdad University.

Abstract
The aim of this paper is to give a generalization of the theorem that, for \( n \geq 5 \), every even permutation defined on \( n \) symbols is commutator of even permutations \( a \) and \( b \). In particular, \([3n/4] \leq L \leq n\) is shown to be the necessary and sufficient condition on \( L \), in order that every even permutation defined on \( n \geq 5 \) symbols can be expressed as a product of two cycles, each of length \( L \). Results follow, including every odd permutation is a product of a cycle of length \( L \) and a cycle of length \( L + 1 \).

Introduction
In \([1]\), Oystein Ore showed that in the finite symmetric group \( \text{Sym}(n) \) each element of the alternating subgroup \( \text{Alt}(n) \) is commutator. Thus a given permutation \( P \in \text{Alt}(n) \) can be expressed as a product \( R \cdot (S \cdot R^{-1} \cdot S^{-1}) \) of two permutations belonging to the same conjugacy class to which \( R \) belongs depends upon the conjugacy class of \( P \). Ore also announced, and Zvi Arad published a proof \([2]\), that for \( n \geq 5 \) each \( P \in \text{Alt}(n) \) can be expressed as a commutator of permutations in \( \text{Alt}(n) \). Again the conjugacy class of \( R \) depends upon that of \( P \), in the proof.

In \([3]\), J. L. Brenner proposed a problem equivalent to the question whether there exists a conjugacy class \( D_n \) in \( \text{Alt}(n) \), \( n \geq 5 \), such that \( \text{Alt}(n) = D_n \circ D_n^{-1} \). Zvi Arad exhibited such a class in \([2]\), the class is composed of permutations with two non–trivial cycles, as follows:

i. If \( n = 2m + 1 \), \( m \geq 2 \), take \( D_n \) to be the class of all permutations conjugate to \((12)(345 \ldots n)\).

ii. If \( n = 2m \), \( m \geq 2 \), take \( D_n \) equal to the class of all permutations conjugate to \((12)(345 \ldots n - 1 n)\).

It is well known that a conjugacy class in \( \text{Sym}(n) \) is in fact a conjugacy class in \( \text{Alt}(n) \).

A \( \text{Alt}(n) \) if and only if a representative permutation is even and does not correspond to a partition of \( n \) into distinct odd parts. Thus \( D_n \) is a class in \( \text{Alt}(n) \).

For \( L \leq n \), let \( C_L \) denote the (self inverse) conjugacy class of all permutations conjugate to \((1 2 3 \ldots L)\), i.e. the class consisting of each permutation with exactly one cycle of length \( L \) and \( n - L \) cycles of length one (using standard decomposition into disjoint cycles). Our main purpose here will be to characterize those \( L \) for which \( \text{Alt}(n) = C_L \circ C_L \).

Let \( |M(P)| \) denote the number of symbols moved by \( P \in \text{Sym}(n) \) and \( |c^*(P)| \) the number of non–trivial disjoint cycles (length \( \geq 2 \)) in the standard decomposition of \( P \). Our results rest upon constructions which show that given \( P \in \text{Alt}(n) \), \( P \neq C_L \circ C_L^{-1} \), there exist two \( L \)–cycles \( A, B \) such that \( P = B \cdot A \), whenever \( L \geq L(P) \equiv \frac{1}{2} \left( |M(P)| + |c^*(P)| \right) \), for all \( P \in \text{Alt}(n) \), \( \max L(P) = \lfloor 3n/4 \rfloor \), and \( L(P) \) is shown to be the minimum possible \( L \) for such a decomposition of \( P \).

Let \( |c(S)| \) denoted the total number of cycles, including 1-cycles, in the standard decomposition of \( S \in \text{Sym}(n) \). All products of permutations are executed from right to left.

\textbf{Lemma 1}\cite{2}:
Let \( S \) be any permutation in \( \text{Sym}(n) \), \( n \geq 2 \), and \( T \) a transposition. Then \( |c(S \circ T)| = |c(T \circ S)| = |c(S)| + 1 \) if the two symbols moved by \( T \) belong to the same cycle of \( S \), and \( |\ell(S \circ T)| = |\ell(S)| - 1 \) if the two symbols moved by \( T \) belong to different cycles of \( S \).

\textbf{Lemma 2}\cite{2}:
Suppose \( A = (a_1 \ a_2 \ldots a_r) \) and \( B = (b_1 \ b_2 \ldots b_s) \) belong to \( \text{sym}(n) \). Then
\[ |\left\{ a_i \right\}_{i=1}^r \cap \left\{ b_j \right\}_{j=1}^s| = m \geq 1 \implies |c(B \circ A)| \leq m \]
**Theorem 1[3]**:

For \( n \neq 4 \), let \( L(n) \) denote the smallest positive integer such that every permutation in \( Alt(n) \) can be expressed as a product of two \( L \)-cycles. Then \( L(n) \geq [3n/4] \).

**Lemma 3[4]**:

Given \( P \in Alt(n) \),

\[
\sum_{c \in P, m(c) \geq 4} \sum_{M \in Alt(n), m(M) \geq 4} \sum_{L \in Alt(n), m(L) \geq 4} \frac{M(P) + c^*(P)}{2} = \text{an integer}, \text{ and } \max_{P} L(P) = \left\lceil \frac{3n}{4} \right\rceil.
\]

**Theorem 2**:

Let \( L > 0 \) be any integer satisfying

\[
\sum_{c \in P, m(c) \geq 4} \sum_{M \in Alt(n), m(M) \geq 4} \sum_{L \in Alt(n), m(L) \geq 4} \frac{M(P) + c^*(P)}{2} \leq L \leq n, \text{ with } P \in Alt(n).
\]

Then there exist \( L \)-cycles \( A, B \) such that \( P = B \circ A \).

**Proof**:

Assume that \( P \) is not identity. The proof will proceed by constructing the appropriate \( L \)-cycles, where initially we show that

\[ L = \frac{\sum_{c \in P, m(c) \geq 4} \sum_{M \in Alt(n), m(M) \geq 4} \sum_{L \in Alt(n), m(L) \geq 4} \frac{M(P) + c^*(P)}{2}}{2} \]

is admissible.

The restrictions of \( A \), and of \( B \), to the symbols of each odd length cycle of \( P \), and to the symbols of each pair of even length cycles of \( P \), are first defined. These restrictions are then (pieced together) to form cycles \( A \), and \( B \), which we show (are non-disjoint) and have the required length. Note that we need only construct the factorization for one member of each conjugacy class.

Suppose that \( P \), in its slandered decomposition, has \( d \geq 1 \) non-trivial odd length cycles:

\[ X_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,\lambda(i)}), \quad i = 1, 2, \ldots, d \]

where \( L(i) = 2\lambda(i) - 1 \geq 3 \).

Define \( A \) on the set \( \{x_{i,j} : j \neq \lambda(i)\} \) and \( B \) on the set \( \{x_{i,j} : j \neq 1\} \) as in Fig.(1a).

Where the edges of the directed graph representation of \( A \) designated by solid arrows and the edges for \( B \) are given by broken arrows. Let \( Y_i = (y_{i,1}, y_{i,2}, \ldots, y_{i,\mu(i)}), \quad i = 1, 2, \ldots, v \), where \( e \) denote the even number of disjoint even length cycles of \( P \); here \( \mu(i) = 2(\mu(i) - 1) \geq 4 \), \( i = 1, 2, \ldots, v \), and \( m(i) = \mu(i) = 2 \) for \( v + 1 \leq i \leq e \) (i.e. the transpositions are listed last). For the symbols of each pair \( Y_i, Y_{i+1} \) with \( m(i), m(i + 1) \geq 4 \) define \( A \) on the set \( \{y_{i,j} \cup y_{i+1,j} : j \neq \mu(i + 1) - 1\} \) and \( B \) on the set \( \{y_{i,j} : j \neq \mu(i)\} \cup \{y_{i+1,j}\} \) as in Fig.(2a).

Again \( P = B \circ A \) wherever \( A \) has been defined. For each pair of transpositions \( Y_k, Y_{k+1} \), define \( A \) on \( \{y_{k,1}, y_{k,2}, y_{k+1,2}\} \) and \( B \) on \( \{y_{k,1}, y_{k+1,2}, y_{k+1,2}\} \) as in figure 2a. In case \( P \) has an odd number of transpositions \( v \) is odd), define \( A \) and \( B \) on the symbols of the \( v \)-th cycle (even length \( \geq 4 \)) and on those of the first transposition by piecing together the first half of Fig.(2a) and the last half of Fig.(3a) in the obvious way.
**Fig. (1) The relation between A and B.** Define A on the set \( \{x_{i,j}, j \neq \lambda(i)\} \), and B on the set \( \{x_{i,j}, j \neq 1\} \).
Fig.(2) The relation between A and B.

Define A on the set \( \{y_{i,j} \cup \{y_{i+1,j}, j \neq \mu(i+1) - 1\}\} \), B on the set \( \{y_{i,j}, j \neq \mu(i)\} \cup \{y_{i+1,j}\} \).
The relation between $A$ and $B$. Define $A$ on the set \( \{ y_{i,j} \} \cup \{ y_{i+1,j}, j \neq \mu(i + 1) - 1 \} \), $B$ on the set \( \{ y_{i,j}, j \neq \mu(i) \} \cup \{ y_{i+1,j} \} \).

**Fig. (2)**
Fig. (3) The relation between A and B. define A on \{y_{k,1}, y_{k,2}, y_{k+1,2}\} and B on \{y_{k,1}, y_{k+1,2}, y_{k+1,1}\}.

Finally, we piece together the restrictions in such a way that both A and B become cycles of the same length. For this, define A and B on the remaining symbols of M(P) as follows:

\[
\begin{align*}
X_{i,\lambda(i)} & \xrightarrow{A} X_{i+1,1} \xrightarrow{B} X_{i,\lambda(i)+1} & \text{for } 1 \leq i \leq d-1 \quad (d \geq 2), \\
x_{d,\lambda(d)} & \xrightarrow{A} \begin{cases} 
Y_{1,\mu(1)} & \xrightarrow{B} x_{d,\lambda(d)+1}, \text{if } e > 0 \\
X_{1,1} & \xrightarrow{B} x_{d,\lambda(d)+1}, \text{if } e = 0 
\end{cases} \\
Y_{i,1} & \xrightarrow{A} Y_{i+1,1} \xrightarrow{B} Y_{i,2}, & i = 1, 3, 5, \ldots, e - 1, \\
Y_{i,\mu(i)-1} & \xrightarrow{A} Y_{i+1,\mu(i)+1} \xrightarrow{B} Y_{i,\mu(i)}, & i = 2, 4, 6, \ldots, e - 2 \\
x_{e,\mu(e)-1} & \xrightarrow{A} \begin{cases} 
Y_{1,1} & \xrightarrow{B} x_{e,\mu(e)}, \text{if } d \geq 0 \\
x_{1,\mu(1)} & \xrightarrow{B} x_{e,\mu(e)}, \text{if } d = 0 
\end{cases} 
\end{align*}
\]

Note that A and B each move \(x_{1,1}\) and \(y_{1\mu(1)}\), P = B \(\circ\) A on all n symbols, and A and B each contain exactly one nontrivial cycle in their standard decompositions.

The cycle of A is seen to have length

\[
\sum_{j=1}^{d} \lambda(j) + \sum_{j=1}^{e-1} (m(j) - \mu(j) + 2) + \sum_{j=2}^{e} (\mu(j) - 1) \quad (*)
\]

Since \(m(j)+2 = 2\mu(j)\) and \(L(j) + 1 = 2\lambda(j)\), then * is equal to

\[
\frac{1}{2}(|M(P)| + |c^*(P)|) \quad \text{Here we have used}
\]

\[
\sum_{j=1}^{d} L(j) + \sum_{j=1}^{e} m(j) = |M(P)|
\]

and

\[
d + e = |c^*(P)|.
\]

In the same way, the cycle length of B is also found to be

\[
\frac{1}{2}(|M(P)| + |c^*(P)|)
\]

We have thus shown that, given P, the minimum possible value for L is also admissible. The result will finally be proved for all integers L with \(\frac{1}{2}(|M(P)| + |c^*(P)|) \leq L \leq n\), if we show that we may increase this initial value of L by one unit at a time, at each step preserving P = B \(\circ\) A, until L reaches n.

Referring to the appropriate directed graphs, we see that this step by step increase may indeed be carried out for A and B restricted to the symbols of

i. each non-trivial odd length cycle of P (Figures 1b, c, d),

ii. each pair of even length cycles (Figs. 2b, c, d, 3b).

In case P has an odd number of transpositions, it should be clear from the figures how we may define A and B on the symbols of the v-th cycle (of even length \(\geq 4\)) and on those of the first transposition. For example, the last step, with each symbol moved, is found by piecing together the first half of Fig.(2d) and the last half of Fig.(3b).

Let \(p_1, p_2, \ldots, p_t\) be the symbols fixed by P. If P contains a pair of even length cycles (\(y_{1,1} y_{2,2} \ldots\)) and (\(y_{2,1} y_{2,2} \ldots\)) note that the following sequences occur within the cycles of A and B, when
Then the j-th step of the cycle length increases on the set \( \{ p_1, \ldots, p_j \} \) is defined by inserting \( p_1, p_2, \ldots, p_j \) as follows:

A = (\( \ldots y_{1,1} y_{1,2} \ldots \)),
B = (\( \ldots y_{2,1} y_{1,2} \ldots \)).

If there are no even length cycles for \( P \), replace \( y_{1,1} \) by \( x_{d,\lambda(d)} \), \( y_{2,1} \) by \( x_{1,1} \), and \( y_{1,2} \) by \( x_{d,\lambda(d)+1} \), the result is the same.

**Corollary 2.1:**
Let \( k(n) \) denote the smallest positive integer such that every permutation in \( \text{Alt}(n) \) can be expressed as a product of four \( k \) -cycles. Then \( k(n) \leq \lceil \frac{3n}{8} \rceil + 1 \).

**Proof:**
By corollary in \([2]\) (In \( \text{sym}(n) \), \( n \neq 4 \), let \( C_L \) denote the conjugacy class of all \( L \)-cycles. Then \( \text{Alt}(n) = C_L \odot C_L^{-1} \) if and only if \( \lceil \frac{3n}{4} \rceil \leq L \leq n \), if \( n \) is even, then \( n - k \geq \lceil \frac{3n}{4} \rceil \) if and only if \( n \geq 4k - 2 \). If \( n \) is odd, then \( n - k \geq \lceil \frac{3n}{4} \rceil \) if and only if \( n \geq 4k - 3 \).

If \( \lceil \frac{3n}{4} \rceil \) is odd, we factor each even permutation into the product of two \( \lceil \frac{3n}{4} \rceil \) -cycles, each of length \( \lceil \frac{3n}{4} \rceil \), if \( \lceil \frac{3n}{4} \rceil \) is even we factor each even permutation into the product of two \( \lceil \frac{3n}{4} \rceil + 1 \) cycles, each of length \( \lceil \frac{3n}{4} \rceil + 1 \).

Each even permutation is thus factored into the product of two cycles of odd length.

Now note that each cycle of odd length \( q \) can be factored into the product of two cycles of length \( \mu = \frac{1}{2} (q + 1) \), since \( (1 \ 2 \ \ldots \ q) = (\mu + 1 \ \mu + 2 \ \ldots \ q) \circ (1 \ 2 \ \ldots \ \mu) \).

For \( \lceil \frac{3n}{4} \rceil \) even, we may thus express every even permutation as the product of four cycles, each of length

\[
\frac{3n}{4} + 2 = \lceil \frac{3n}{4} \rceil + 1.
\]

For \( \lceil \frac{3n}{4} \rceil \) odd, we can factor every even permutation into the product of four cycles, each of length

\[
\frac{3n}{4} + 1 = \lceil \frac{3n}{4} \rceil + 1.
\]

**Corollary 2.2:**
If \( L \) is an even integer satisfying \( \lceil \frac{3n}{4} \rceil - 1 \leq L \leq n \), then every odd permutation in \( \text{sym}(n) \) can be expressed as a product of three \( L \) -cycles.

**Proof:**
Suppose first that \( \lceil \frac{3n}{4} \rceil - 1 \leq L \leq n \), and let \( P \) be an \( L \) -cycle. If \( Q \) is any odd permutation in \( \text{sym}(n) \), \( P \circ Q \in \text{Alt}(n) \).

Thus \( P \circ Q = S \circ T \), where \( S \) and \( T \) are \( L \) -cycles.

If \( \lceil \frac{3n}{4} \rceil - 1 \) is even, \( P \) is also an \( L \) -cycle, \( Q = R \circ S \circ T \) is the product of three \( L \) -cycles.

Furthermore, the \( \lceil \frac{3n}{4} \rceil \) -cycle \( A \) may be expressed as the product of two \( \lceil \frac{3n}{4} \rceil - 1 \) -cycles; for \( q \) odd,

\[
(1 \ 2 \ 3 \ \ldots \ q) = (\lambda + 1 \ \lambda + 2 \ \ldots \ q 1) \circ (1 \ q 2 \ q - 1 \ q 3 \ \ldots \ q - 2 \ \lambda + 2 \ \lambda + 2 \ \lambda - 1 \lambda)
\]

where \( \lambda = (q + 1) / 2 \) and the latter two cycles are each of length \( q - 1 \).

**Theorem 3:**
Let \( Q \) be an odd permutation in \( \text{Sym}(n) \). Then if \( L \) is any integer satisfying

\[
\frac{3n}{4} + 1 \leq L \leq n - 1,
\]

\( Q \) may be expressed as a product \( B \circ A \) of an \( L \) -cycle \( B \) and an \( (L + 1) \) -cycle \( A \).

**Proof:**
Case 1. \( Q \) contains a cycle \( (\ldots a b c \ldots) \) of length \( \geq 3 \).

Then \( Q \circ (a b) \in \text{Alt}(n) \) and contains \( (b) (\ldots a c \ldots). \)

From the constructions given in the proof of Theorem 2 it is evident that \( Q \circ (a b) \) can be represented as a product \( B \circ C \) of two cycles of length \( L \), whenever \( L \) satisfies...
\[
\left( \left\lfloor \frac{M(Q) - 1}{2} \right\rfloor + \left\lceil \frac{Q}{2} \right\rceil \right) \leq L \leq n - 1, \quad \text{where } a \in M(C) \text{ and } b \not\in M(C). \text{ Thus}
\]
\[
Q = (Q \circ (a b)) \circ (a b) = B \circ (C \circ (a b)),
\]
may be expressed as a product \( B \circ A \), where \( B \) is a cycle of length \( L \) and
\[
A = C \circ (a b) \text{ is a cycle of length } L + 1.
\]

Case 2. \( Q \) contains an odd number of transpositions and possibly 1–cycle.

If \( Q \) is a transposition, the result immediate.

Otherwise \( Q = (a b) (c d) \ldots, \text{ then } Q \circ (b c) \text{ is even and contains } \ldots (a b d c) \ldots. \text{ Again, the constructions of theorem 2 show that } Q \circ (b c) \text{ may be represented as a product } B \circ C \text{ of two cycles of length } L, \text{ for each } L \text{ satisfying}
\[
\frac{M(Q) + \left\lceil \frac{Q}{2} \right\rceil - 1}{2} \leq L \leq n - 1, \text{ with } b \in M(C)
\]
and \( c \not\in M(C) \).

Then \( Q = (Q \circ (b c)) \circ (b c) = (B \circ (C \circ (b c)) \text{ may be expressed as a product } B \circ A, \text{ a cycle of length } L \) and \( A = C \circ (b c) \text{ a cycle of length } L + 1.\)

References


