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 $a\ b\ a^{-1}\ b^{-1}$ 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 Sym(n) each element of the alternating subgroup Alt(n) is commutator. Thus a given permutation $P \in$ Alt(n) can be expressed as a product $R \circ (S \circ R^{-1} \circ S^{-1})$ 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 $P \in$ Alt(n) can be expressed as a commutator of permutations in 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 Alt (n), $n \geq 5$, such that 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 … n – 2 n – 1)(n).

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

It is well known that a conjugacy class in Sym (n) is in fact a conjugaacy class in.

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 Alt (n).

For $L \leq n$, let C_L denote the (self inverse) conjugacy class in Sym (n) of all permutations conjugate to (1 2 3 … 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 Alt (n) = $C_L \circ C_L$.

Let |M (P)| denote the number of symbols moved by $P \in$ Sym (n) and $|c^*(P)|$ the number of non – trivial disjoint cycles (length ≥ 2) in the standard decomposition of P. Our results rest upon constructions which show that given $P \in$ Alt (n), $P \neq C_L \circ C_L^{-1}$, there exist two L – cycles A, B such that $P = B \circ A$, whenever $L \geq L(P) \equiv \dfrac{|M(P)| + |c^*(P)|}{2}$, for all $P \in$ Alt (n), max L(P) = [3n/4], 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 $S \in$ Sym(n). All products of permutations are executed from right to left.

Lemma 1[2] :

Let S be any permutation in Sym(n), $n \geq 2$, and T a transposition. Then $|c(S \mathbf{o} T)| = |c(T \mathbf{o} S)| = |c(S)| + 1$ if the two symbols moved by T belong to the same cycle of S, and $|\mathbf{l}(S \mathbf{o} T)| = |\mathbf{l}(S)| - 1$ if the two symbols moved by T belong to different cycles of S.

Lemma 2 [2]:

Suppose A = $(a_1\ a_2\ \ldots\ a_r)$ and B =$(b_1\ b_2\ \ldots b_s)$ belong to sym(n). Then

$$\left|\{a_i\}_{i=1}^{r} \cap \{b_j\}_{j=1}^{s}\right| = m \geq 1 \Rightarrow |c(B \mathbf{o} A)| \leq m$$

Theorem 1[5] :

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) ≥ [3n/4].

Lemma 3[4] :

Given $P \in$ Alt(n), $L(P) \equiv \frac{|M(P)| + |c^*(P)|}{2}$ is an integer, and $\max_{p} L(P) = \left\lceil \frac{3n}{4} \right\rceil$.

Theorem 2:

Let L>0 by any integer satisfying $\frac{|M(P)| + |c^*(P)|}{2} \leq L \leq n$, with $P \in \mathrm{Alt}(n)$. Then $\frac{|M(P)| + |c^*(P)|}{2}$ there exist L-cycles A, B such that P=B◦A.

Proof:

Assume that P is not identity. The proof will proceed by constructing the appropriate L-cycles, where initially we show that $L = \frac{|M(P)| + |c^*(P)|}{2}$ 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≥1 non-trivial odd length cycles:
$X_i = (x_{i,1}\ x_{i,2}\ \ldots.\ x_{i,\lambda(i)}\ \ldots.\ x_{i,L(i)})$, i = 1, 2, ……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 $Y_i = (y_{i,1}\ y_{i,2}\ \ldots.\ y_{i,\mu(i)}\ \ldots.\ y_{i,m(i)})$, i = 1, 2, ….e, where e denote the even number of disjoint even length cycles of P; here $m(i) = 2(\mu(i) - 1) \geq 4$, i = 1, 2, …. 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) ≥ 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◦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 3a. 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 ≥ 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.

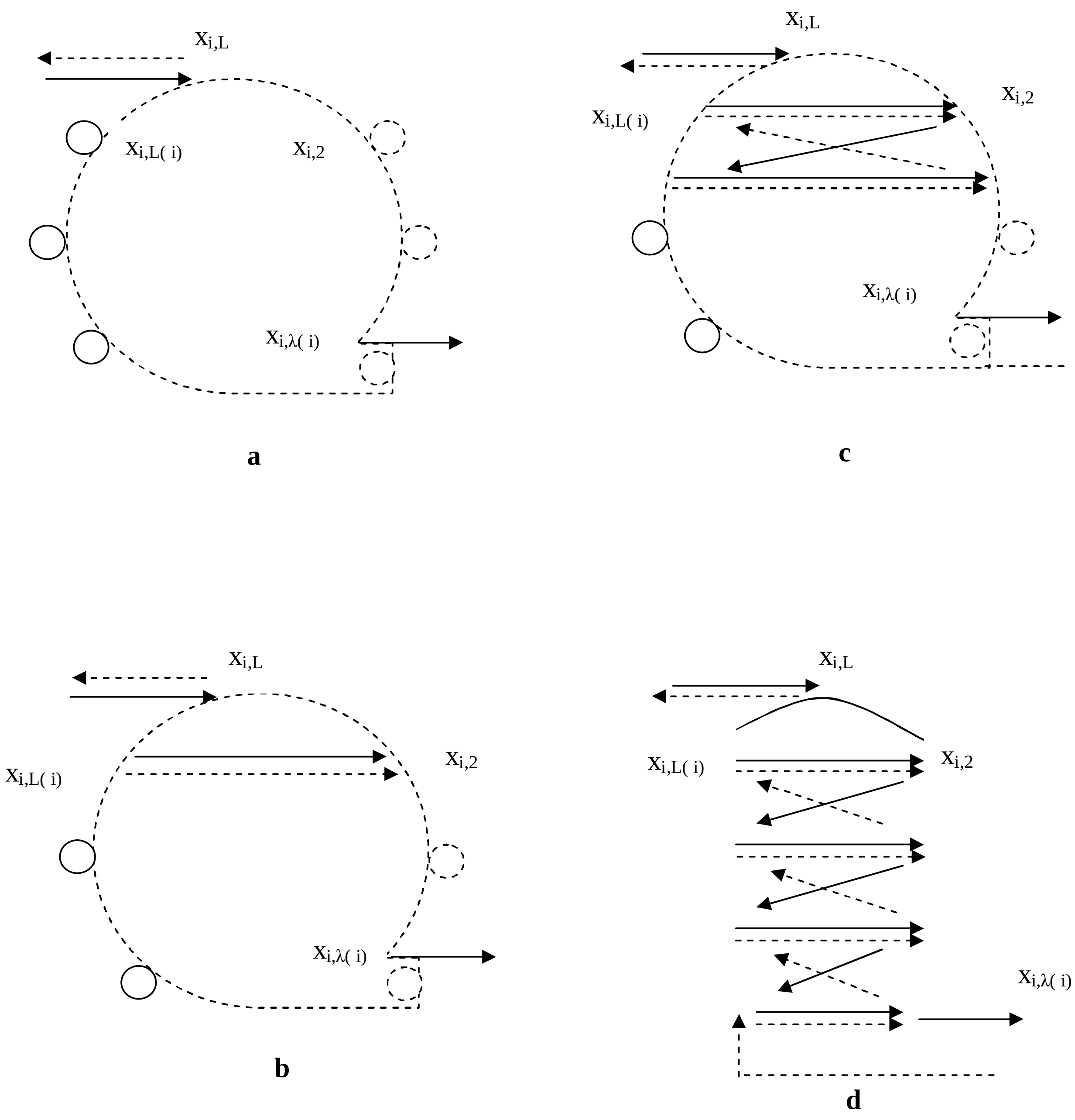

Fig.(1) The relation between A and B. Define A on the set {$x_{i,j}$, j ^{1} l (i)}, and B on the set { $x_{i,j}$, j ^{1} 1}.

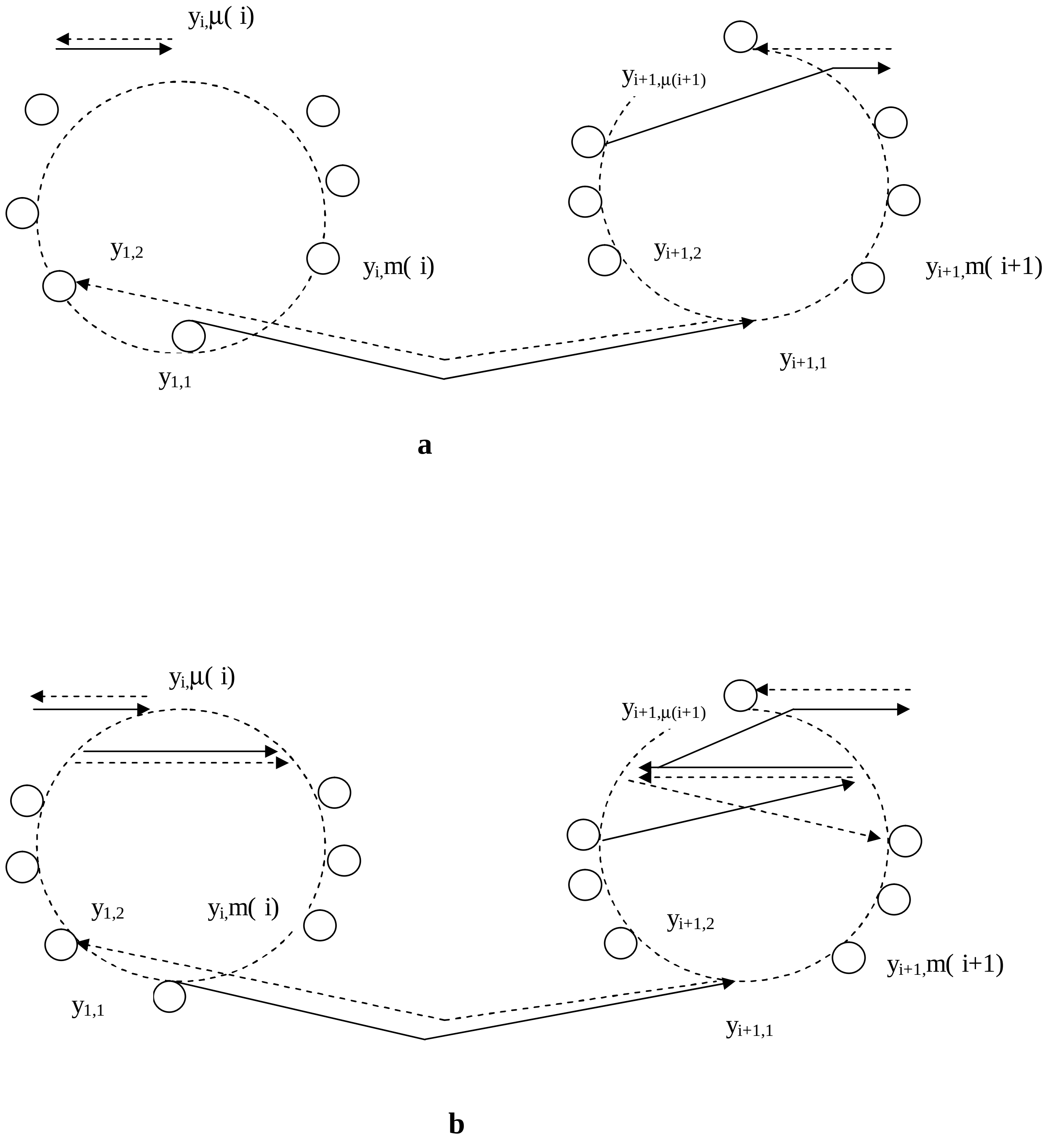

Fig.(2) The relation between A and B.
define A on the set {$y_{i,j}$}È{$y_{i+1,j}$, j ¹ m(i + 1) – 1}, B on the set {$y_{i,j}$, j ¹ m(i)} È{$y_{i+1,j}$}.

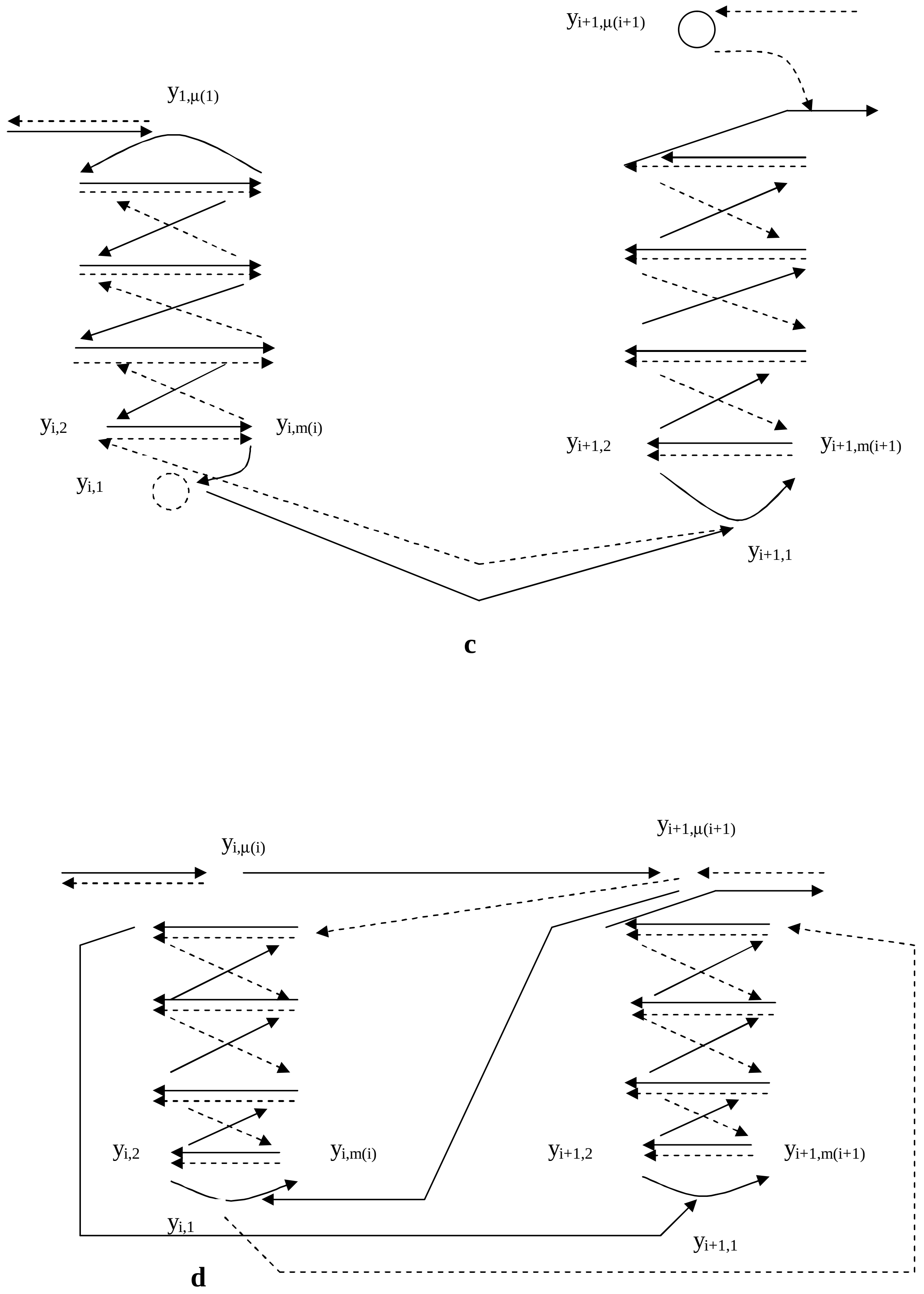

Fig.(2) The relation between A and B. define A on the set {$y_{i,j}$}È{$y_{i+1,j}$, j ¹ m(i + 1) – 1},
B on the set {$y_{i,j}$, j ¹ m(i)} È{$y_{i+1,j}$}.

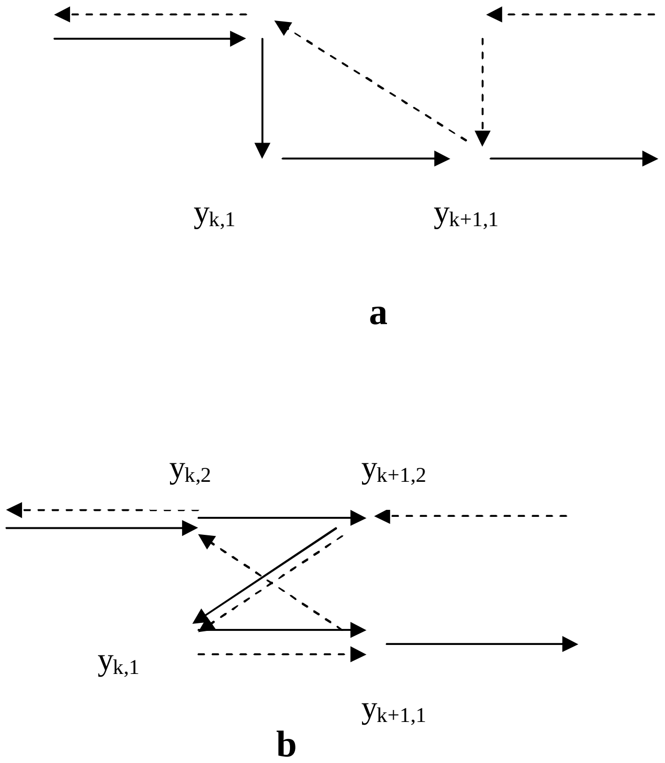

Fig.(3) The relation between A and B. define A on {$y_{k,1}$, $y_{k,2}$, $y_{k+1,2}$} and B on {$y_{k,1}$, $y_{k+1,2}$, $y_{k+1,2}$}.

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:

$$x_{i,\lambda(i)} \xrightarrow{A} x_{i+1,1} \xrightarrow{B} x_{i,\lambda(i)+1}$$

for $1 \le i \le d-1$ $(d \ge 2)$,

$$x_{d,\lambda(d)} \xrightarrow{A} \begin{cases} y_{1,\mu(1)} \xrightarrow{B} x_{d,\lambda(d)+1}, \text{if } e \ \mathbf{f}\ 0 \\ x_{1,1} \xrightarrow{B} x_{d,\lambda(d)+1}, \text{if } e = 0 \end{cases}$$

$$y_{i,1} \xrightarrow{A} y_{i+1,1} \xrightarrow{B} y_{i,2},$$

$i = 1, 3, 5,..., e - 1$,

$$y_{i,\mu(i)-1} \xrightarrow{A} y_{i+1,\mu(i+1)} \xrightarrow{B} y_{i,\mu(i)},$$

$i = 2, 4, 6,\dots, e - 2$

$$x_{e,\mu(e)-1} \xrightarrow{A} \begin{cases} y_{1,1} \xrightarrow{B} x_{e,\mu(e)}, \text{if } d \ge 0 \\ x_{1,\mu(1)} \xrightarrow{B} x_{e,\mu(e)}, \text{if } d = 0 \end{cases}$$

Note that A and B each move $x_{1,1}$ and $y_{1\mu(1)}$, P= B∘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

$$\sum_{j=1}^{d} \lambda(j) + \sum_{\substack{j=1 \\ (j\,\text{odd})}}^{e-1} (m(j) - \mu(j) + 2) + \sum_{\substack{j=2 \\ (j\,\text{even})}}^{e} (\mu(j) - 1) \qquad *$$

Since m(j)+2 = 2μ(j) and L(j) + 1 = 2λ(j), then * is equal to

½(|M(P) +|c*(P)|) Here we have used

$$\sum_{j=1}^{d} L(j) + \sum_{j=1}^{e} m(j) = |M(P)| \qquad \text{and}$$

$$d + e = |c^*(P)|.$$

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

½(|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 ½(|M (P) |+|c*(P)|) ≤ L ≤ 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 ∘ 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 ≥ 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,…, p_f be the symbols fixed by P. If P contains a pair of even length cycles ($y_{1,1}$ $y_{2,2}$ …) and ($y_{2,1}$ $y_{2,2}$ …) note that the following sequences occur within the cycles of A and B, when

$L= ½(|M (P) +|c^*(P)|)$, $A=(\dots\ y_{1,1}\ y_{2,1}\ \dots)$, $B=(\dots\ y_{2,1}\ y_{1,2}\ \dots)$.

Then the j-th step of the cycle length increases on the set $\{p_i\}_1^f$ is defined by inserting $p_1, p_2, \dots, p_j$ as follows:

$A = (\dots\ y_{1,1}\ p_1\ p_2\ \dots\ p_j\ y_{2,1}\ \dots)$,
$B = (\dots\ y_{2,1}\ p_j\ p_{j-1}\ \dots\ p_1\ y_{1,2}\ \dots)$.

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 Alt (n) can be expressed as a product of four k – cycles. Then k (n) ≤ [3n/8] + 1.

Proof:

By corollary in [2] (In sym(n), n ≠ 4, let C_L denote the conjugacy class of all L-cycles. Then Alt (n) = $C_L \circ C_L^{-1}$ if and only if [3n/4] ≤ L ≤ n. if n is even, then n – k ≥ [3n/4] if and only if n ≥ 4k – 2. If n is odd, then n – k ≥ [3n/4] if and only if n ≥ 4k – 3).

If [3n/4] is odd, we factor each even permutation into the product of two [3n/4] – cycles,

If [3n/4] is even we factor each even permutation into the product of two [3n/4] + 1 cycles,

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 μ = ½ (q + 1), since (1 2 … q) = (μ + 1 μ + 2 … q 1) ∘ (1 2 … μ).

For [3n/4] even, we may thus express every even permutation as the product of four cycles, each of length

$$\frac{\left[\frac{3n}{4}\right]+2}{2}=\left[\frac{3n}{4}\right]+1\ .$$

For [3n/4] is odd, we can factor every even permutation into the product of four cycles, each of length

$$\frac{\left[\frac{3n}{4}\right]+1}{2}=\left[\frac{3n}{8}\right]+1 .$$

Corollary 2.2:

If L is an even integer satisfying [3n/4] – 1 ≤ L ≤ n, then every odd permutation in sym(n) can be expressed as a product of three L – cycles.

Proof:

Suppose first that [3n/4] – 1 ≤ L ≤ n, and let P be an L – cycles.

If Q is any odd permutation in sym (n), P ∘ Q ∈ Alt (n).

Thus P ∘ Q = S ∘ T, where S and T are L – cycles.

since R = P^{-1} is also an L – cycles, Q = R ∘ S ∘ T is the product of three L – cycles.

If [3n/4] – 1 is even, we choose symbols a, b (via the constructions of Theorem 2) in such a way that (a b) ∘ Q = B ∘ A, where B and A are (3n/4) – cycles, and B = (… b a …). Then

Q = ((a b) ∘ A, where (a b) ∘ B is a ([3n/4] – 1) – cycle.

Furthermore, the [3n/4] – cycle A may be expressed as the product of two ([3n/4] – 1) – cycles; for q odd,

(1 2 3 … q) = (λ + 1 λ + 2 λ - 1 λ +3 λ – 2 … q – 1 3 q 2 1) ∘ (1 q 2 q – 1 3 q – 2 … λ + 3 λ - 2 λ + 2 λ – 1 λ)

where λ = (q + 1) / 2 and the latter two cycles are each of length q – 1.

Theorem 3:

Let Q be an odd permutation in Sym (n). Then if L is any integer satisfying

$$\frac{|M(Q)|+|c^*(Q)|-1}{2}\le L\le n-1\ ,$$

Q may be expressed as a product B∘ A of an L – cycle B and an (L + 1) – cycle A.

Proof:

Case 1. Q contains a cycle (… a b c …) of length ≥ 3.

Then Q ∘ (a b) ∈ Alt (n) and contains (b) (… a c …).

From the constructions given in the proof of Theorem 2 it is evident that Q ∘ (a b) can be represented as a product B ∘ C of two cycles of length L, whenever L satisfies

$\frac{(|M(Q)| - 1) + |c^*(Q)|}{2} \leq L \leq n - 1$, where $a \in M(C)$ and $b \notin M(C)$. 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

$A = C \circ (a\ b)$ 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 $Q = (a\ b)\ (c\ d) \ldots$, then $Q \circ (b\ c)$ is even and contains … (a b d c) … . Again, the constructions of theorem 2 show that $Q \circ (b\ c)$ may be represented as a product $B \circ C$ of two cycles of length L, for each L satisfying $\frac{|M(Q)| + (|c^*(Q)| - 1)}{2} \leq L \leq n - 1$, with $b \in M(C)$ and $c \notin M(C)$.

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

References

[1] O. Ore, "Some remarks on Commutates", Proc. Amer. Math.Soc., Vol. 2, 1951, pp. 307-314.

[2] A. Zvi, & M. Herzog, "Product of Conjugacy Classes in Groups, Lecture Notes in Mathematics", Springer Vol. 1112, 1985.

[3] J. L. Brenner, "Research Problems, 1. group Theory, Bull. Amer. Math. Soc. Vol. 66 1990,pp. 275-283.

[4] A. Zvi, "On the number of Conjugacy Classes of a Finite Solvable Groups II", Jor. of Alg., Vol. 270, No. 2, 2003, pp. 660-669.

[5] Britnell & W. Bull, "On the Distribution of Conjugacy Classes Between the Costes of a finite Group in a Cyclic Extension", London Math. Soc. 40, 2008, pp. 897-906.

الخلاصة

فهدل ا من هذا البحث يتولد من المبرهنة الاتية، لكل n ≥ 5 فانه لكل تبديل زوجي يعرف على n من الرموز هو تبديل $a\ b\ a^{-1}\ b^{-1}$ للتباديل الزوجية a وb. على وجه التخصيص [3n/4] ≤ L ≤ n. برهنت شرط ضروري ومكافئ عل L. لأجل ذلك كل تبديل زوجي يعرف على n ≥ 5 ممكن يعبر عنه كضرب دورتين كلا منهما طولها L. النتائج الاحقة تتضمن كل تبديل فردي هو ضرب دورة طولها L ودورة طولها L + 1.