Covering Theorem for Finite Nonabelian Simple Groups

Shaimaa Salman Abd Mohsen*

Date of acceptance 3/10/2006

Abstract:

In this paper, we show that for the alternating group An, the class C of n- cycle, CC covers A_n for n when n = 4k + 1 > 5 and odd. This class splits into two classes of A_n denoted by C and $C^/$, CC= $C^/C^/$ was found.

Introduction:

Let G be a group. We say α and β are conjugate in G (and all β a conjugate of α) if $\lambda^{-1}\alpha\lambda = \beta$ for some λ in G. The conjugacy class of α is the set $\{\lambda^{-1}\alpha\lambda : \lambda \in G\}$.[2,3]

Now, let C be any non trivial conjugacy class (C ≠ 1) of G, we say C covers G if there exists a positive integer number m such that $C^m = G$. [4]

We denote to the symmetric group of finite set H = {1, 2, ….., n} by P_n and to the alternating group by A_n. The problem of covering is determining the minimal value of m which is as yet unsolved completely [1]. But there are many authors have worked on this field and they have many interesting results. One of them is Bertram [1] who proved that for n ≥ 5, every permutation in A_n is the product of two L – cycles for every $[\frac{3n}{4}] \le L \le n$. Hence A_n Can be covered by products of two n – cycles and also by products of two (n – 1) – cycles. But Bertram also showed that if n is odd is the n – cycles in A_n fall into two conjugate classes C, $C^/$, and similarly for the (n – 1) – cycles if n is even, so that the quoted results does not decide whether

$$CC = A_n \;\ldots\ldots\; (1)$$

Theorem 1: For n = 4k + 1 > 5, the class C of the cycle (1 2 …… n) has property (1).

To prove this theorem, this required (The case when n = 9 and Lemma 1):

The Case n = 9: Let a = (123456789). For every class in A^9, a conjugate b of a can be found such that ab represents (line in) that class. This assertion is the substance of the table below

b	**ab**
a^{-1}	**1 (1 is the identity)**
(193248765)	**(14)(38)**
(176235894)	**(13)(25)(48)(79)**
(132987654)	**(193)**
(134765289)	**(18)(24)(379)**
(132798465)	**(174)(369)**
(184523796)	**(135)(274)(698)**
(137259486)	**(15)(276)(3849)**
(123794865)	**(1384)(2769)**
(132798654)	**(17693)**
(189623574)	**(13)(25)(47986)**
(132869745)	**(18764)(359)**
(132845697)	**(18746)(359)**
(159348726)	**(162495)(38)**
(186974532)	**(3598764)**
(12345789) = a	**(135792468)**
(125678934)	**(157924683)**

*Department of Mathematics, College of Education, Ibn Al-Haithm, Baghdad University.

Lemma 1: If n = 4k + 1, CC contains the type $2^{2k}\ 1^1$.
Proof:
1. If n ≡ 1 (mod 8), n > 9 then
x = (n n – 3 n – 2 n – 1 n – 4 n – 7 n – 6 n – 5……. 9 6 7 8 5 2 3 4 1) is conjugate to a and
ax = (1 3) (2 4) (5 7) (6 8)…. (n – 4 n – 2) (n – 3 n – 1)

n ≡ 1 (mod 8)
⇒ n – 1 = 8k
⇒ n = 8k +1
n = 8k +1, n > 9
If k = 1 ⇒ n = 9
∴ x = (967852341) is conjugate to a and
ax = (13)(24)(57)(68)

If k = 2 ⇒ n = 17
∴x = (17 14 15 16 13 10 11 12 967852341) is conjugate to a and
ax = (1 3)(2 4)(5 7)(6 8)(9 11)(10 12)(13 15)(14 16)

If k = 3 ⇒ n =25
x = (25 22 23 24 21 18 19 20 17 14 15 16 13 10 11 12 967852341) is conjugate to a and
ax = (1 3)(2 4)(5 7)(6 8)(9 11)(10 12)(13 15)(14 16)(17 19)(18 20)(21 23)(22 24)

2. If n = 5 (mod8), n > 13 then
y = (n n – 3 n – 2 n – 1 n – 4 n – 7 n – 6 n – 5....... 13 9 6 10 12 7 8 11 5 2 3 4 1) is conjugate to a and
ay = (1 3)(2 4)(5 10)(6 8)(7 11)(9 12)(13 15)…… (n – 4 n – 2)(n – 3 n – 1).

n ≡ 5 (mod 8)
⇒ n – 5 = 8k
⇒ n = 8k + 5
n = 8k + 5, n > 13

If k = 2 ⇒ n = 21
∴y = (21 18 19 20 17 14 15 16 13 9 6 10 12 7 8 11 5 2 3 4 1) is conjugate to a and
ay = (1 3)(2 4)(5 10)(6 8)(7 11)(9 12)(13 15)(14 16)(17 19)(18 20)

If k = 3 ⇒ n =29
y = (29 26 27 28 25 22 23 24 21 18 19 20 17 14 15 16 13 9 6 10 12 7 8 11 5 2 3 4 1) is conjugate to a and
ay = (1 3)(2 4)(5 10)(6 8)(7 11)(9 12)(13 15)(14 16)(17 19)(18 20)(21 23)(22 24).

If k = 4 ⇒ n =37
y = (37 34 35 36 33 30 31 32 29 26 27 28 25 22 23 24 21 18 19 20 17 14 15 16 13 9 6 10 12 7 8 11 5 2 3 4 1).
ay = (1 3)(2 4)(5 10)(6 8)(9 12)(7 11)(13 15)(14 16)(17 19)(18 20)(21 23)(22 24)(25 27)(26 28)(29 31)(30 32)(33 35)(34 36).

If n = 13 we use the last 13 letters of y, when
y = (n n – 3 n – 2 n – 1 n – 4 n – 7 n – 6 n – 5....... 13 9 6 10 12 7 8 11 5 2 3 4 1).
The pattern of y differs from that of x only in the last 8 letters between 13 9 …. 11, in which the number of reversals is odd, whereas in every other such 8 letters in either x or y, the number of reversals is even).

The Induction:

The induction proceeds from n – 4 to n = 4k + 1. The induction hypothesis is:
For every permutation T in A n – 4, there are two (n – 4) – cycles Z_1 and Z_2 both in the class of the (n – 4) – cycle (123….n – 6 n – 5 n – 4) and also two other (n – 4) – cycles Z'_1 and Z'_2 both in the class of (123 ……n – 6 n – 4 n – 5), such that $T = Z_1Z_2 = Z'_1Z'_2$.
Let P ≠ 1 be a permutation in A_n. To show that CC contains S we consider several cases. In each case we find a

conjugate P1of P, and a certain permutation g in An, such that T = P1g-1 fixes the letters n, n – 1, n – 2, n – 3 and thus its restriction to 1, 2, ….., n – 4 lies in An -4.

Case1. P contains a cycle with 5 or more letters take

g = (n n – 1 n – 2 n – 3 n – 4).

Case2. P contains no cycle with 5 or more letters, but P contains at least one cycle with 4 letters, take

g = (n n – 1 n – 2 n – 3) (n – 4) (n – 5).

Case3. P contain no cycle with more than 3 letters, but P does contain two 3 – cycles, take

g = (n n – 1 n – 2) (n – 3 n – 4 n – 5).

Case4. P is of type $3^1\ 2^{2k-2}\ 1^2$, take

g = (n n – 1 n – 2).

Now, if P contains no cycle longer than transposition (permutation is a cycle of length 2), either P is of type $2^{2k}\ 1^1$, whence CC contains P by the lemma, or we have

Case5. P fixes 5 or more letters, take

g = 1

the proof in case5 is simple, since P fixes 5 or more letters P has conjugate P1 that fixes n, n – 1, n – 2, n – 3 and by the induction hypothesis.

$P_1 = Z_1Z_2$, where Z_1 and Z_2 both fix n, n – 1, n – 2, n – 3 and can be expressed

Z_1 = (a1 a2….. an – 5 n – 4)

Z_2 = (b1 b2….. bn – 5 n – 4).

Where the permutation ai →bi is an even permutation of the letters 1, 2, …., n – 5.

Then $P_1 = Z_3Z_4$ with

Z_3 = (a1 a2….. an – 5 n n – 1 n – 2 n – 3 n – 4)

Z_4 = (b1 b2….. bn – 5 n – 4 n – 3 n – 2 n – 1 n).

and Z_3, Z_4 belong to the class, be it C or C'. if the other part of the induction hypothesis is used in a similar fashion, the assertion that CC contains P follows.

The details for case1 are as follows, since $T = P_1g^{-1}$ move at most the first n – 4 letters

By the induction ⇒ $T = Z_1Z_2 = Z'_1Z'_2$,

Z_1, Z_2 [Z'_1, Z'_2] are from the same class in An – 4

Writing Z_1 = (a1 a2….. an – 5 n – 4)

Z_2 = (b1 b2….. bn – 5 n – 4)

The permutation ai →bi is an even permutation of 1, 2, ……, n – 5.

Now

∵ $T = P_1g^{-1} \Rightarrow P_1 = T_g$

∵ $P_1 = Z_3Z_4 \Rightarrow P_1 = Tg = Z_3Z_4$, g = (n n – 1 n – 2 n – 3 n – 4)

and Z_3 = (a1 a2….. an – 5 n – 2 n n – 3 n – 1 n – 4)

Z_4 = (b1 b2….. bn – 5 n n – 3 n – 1 n – 4 n – 2)

Z_3 and Z_4 are in the same class, be it C or C' in A_n.

By again using Z_1 and Z_2 in place of Z_1 and Z_2, the proof is completed in this case.

In case2, P has a conjugate P_1 such that $T = P_1g^{-1}$ fixes at least 5 letters. Hence without loss of generality the factors Z_1, Z_2 [Z'_1, Z'_2] can be chose so that $T = Z_1Z_2 = Z'_1Z'_2$ with

Z_1 = (a1…….an – 6 n – 5 n – 4), Z'_1 = (a/1 ……...a/n – 6 n – 5 n – 4)

Z_2 = (b1…….bn – 6 n – 4 n – 5), Z'_2 = (b/1 ……...b/n – 6 n – 4 n – 5)

and where $a_i \to b_i$ [$a'_i \to b'_i$] is an odd permutation of the letters1, 2, ….., n – 6.

Now $T_g = Z_3Z_4$ where

Z_3 = (a1 a2….. an – 6 n – 1 n – 5 n – 3 n – 2 n n – 4)

Z_4 = (b1 b2….. bn – 6 n – 5 n – 2 n n – 3 n – 4 n – 1)

The permutation Z3 and Z4 belong to the same class in An. Priming the ai and bi completes the proof in this case.

In case3, P has at least two 3 – cycles, and has a conjugate P_1, such that $T = P_1g^{-1}$ fixes the letters n, n – 1, n – 2, n – 3, n – 4, n – 5.

By the induction permutations Z_1 and Z_2 exist such that $T = Z_1Z_2$ with Z_1 = (n – 4 a1……..ak n – 5 ak +1……. an – 6)

Z_2 = (n – 4 b1……..bh n – 5 bh +1……. bn – 6)\

And where Z_1 and Z_2 are in the same in A_n.

Now $P_1 = Z_1Z_2$ where $Z_3 = Z_1f$,

$$Z_4 = f^{-1} Z_2\, g$$

and f = (n – 5 n – 3 n – 2)(n – 4 n – 1 n). Then Z_3 and Z_4 are both n – cycles and in the same class in An. It has only to be checked that they are in the same class in A_n, to do this is tedious, but straightforward. To complete the proof in this case we observe that since P contains two 3- cycles and $P_1 = Z_3\, Z_4$, the decomposition P_1 = Z/3Z/4 can be obtained by applying a certain outher automorphism of A_n.

In the only remaining case (case 4), P fixes 2 letters, and therefore has a conjugate P_1 such that $T = P_1g^{-1}$ fixes n, n – 1, n – 2, n – 3, n – 4. Again we have $T = Z_1Z_2$, where we can write

Z_1 = (a1…. an – 6 n – 4 n – 5)

Z_2 = (b1…. bn – 6 n – 5 n – 4)

and where the permutation ai→ bi is an odd permutation of the letters 1, 2, …., n – 6. Then $P_1 = T_g = Z_3Z_4$, with

Z_3 = (a1… an – 6 n – 1 n n – 3 n – 2 n – 4 n – 5)

Z_4 = (b1… bn – 6 n – 5 n – 4 n n – 2 n – 3 n – 1)

and these belong to the same class. By priming we again conclude CC contains P, and the proof is complete in all cases. Hence theorem 1.

References:

1. Bertram, E. A., 1972. ‘Even Permutation as a product of two Conjugate cycles’, (1972) J. Combinatorial Theory (A) 12:368-380.

2. Burton David, M.,1967.‘Introduction to Modern Abstract Algebra’, Addison – Wesley Publishing Company

3. Surowski, D., 2002. ‘Work Book in Higher Algebra’. www.geocities.com/alek–stef/mylist. Html.

4. Arad, Z., and M. Herzong, 1985. ‘Product of Conjugacy Classes In Groups’ Lecture Notes in Mathematics, Vol. 1112, Springer.

نظرية الغطاء للزمر المنتهية غير الابدالية البسيطة

شيماء سلمان عبد محسن*

* قسم الرياضيات ، كلية التربية- أبن الهيثم، جامعة بغداد.

الخلاصــة:

في هذا البحث نبين أن في الزمرة المتناوبة A_n ،ان صف التكافؤ C الذي يتكون من n من الدورات، أستنتجنا أن CC يغطي A_n عندما تكون $n = 4k + 1$ و $n > 5$ و n عدد فردي وينقسم صف التكافؤ هذا على قسمين ويرمز لهذين القسمين بالرمز C و $C^/$ وبينت بأنه $CC = C^/C^/$.