COLLOQUIUM MATHEMATICUM

VOL. XXXII 1974 FASC. 1

COVERING THEOREMS FOR FINITE NON-ABELIAN SIMPLE GROUPS. I

BY

J. L. BRENNER* (VICTORIA; PALO ALTO), M. RANDALL (AMOCO, CALGARY) AND J. RIDDELL** (VICTORIA)

1. Introduction. In the alternating group A_n, a fixed partition of n into odd unequal parts determines, by its cycle structure, a type that bifurcates into two conjugacy classes. For every other partition of n having an even number of even parts, the cycle structure determines a single class C in A_n.

The symbol $C^2 = CC$ denotes the set of all elements in A_n obtainable by multiplying two elements of C; the symbol $C^\nu = CC^{\nu-1} = C^{\nu-1}C$ is defined inductively.

For each non-trivial class C in any finite non-abelian simple group G, there is a minimal exponent $\nu = \nu(C)$ such that C^ν covers G. The set of these "class exponents" are invariants, just as the periods of the classes are. Thus *they may be used (in part) to categorize finite non-abelian simple groups*. Among the questions studied in this article are

1. If $CC \supset A_n$, what period can C have?

2. For fixed n, what classes C have maximum exponent?

In answer to a research problem [2], Xu showed [8] that the period $2[n/2]-2$ (i.e. $n-2$ or $n-3$ according as n is even or odd) always occurs among classes of exponent 2 in A_n; Bertram [1] showed in addition that all odd periods l, $-1+3n/4 < l < n-1$, also occur. The investigation of periods $l = n$ $[n-1]$, when n is odd [even], is more difficult; negative results (and one positive result) for these cases are given in [3].

Let l be the smallest period of a class C in A_n such that $CC \supset A_n$. The question whether $l = o(n)$ is possible remains open; $l = O(1)$ seems unlikely. (**P 911**)

Another open question is the characterization of all groups G for which $CC \supset C$ for all C in G (**P 912**). (If G and H have this property, so does $G \times H$.)

* Research supported in part by NSF grant GP-32527.

** Research supported in part by NRC (Canada) grant A-5208.

J. G. Thompson conjectured in conversation that in every finite non-abelian simple group G there are classes C and C^* such that the set $\{cc^* \mid c \in C \text{ and } c^* \in C^*\}$ covers G. We know of no such group G for which a class C fails to exist such that $CC \supset G$. The well-known conjecture that every element of a finite non-abelian simple group is a commutator would follow if such a C always exists.

2. Some lemmas.

2.01. LEMMA. *Let* $C = \{xax^{-1} \mid x \in G\}$ *be a class in the group* G *such that* $CC \supset G$. *Then every element of* G *is a commutator.*

2.02. Remark. O. Ore stated, and Ito proved in [6] that in A_n $(n > 4)$ every element is a commutator. Lemma 2.01 shows that the existence of a class C with $CC \supset G$ is a stronger assertion.

Proof of 2.01. Suppose $g = waw^{-1}tat^{-1}$. Since 1 is covered, there are $x, y \in G$ with $xax^{-1}yay^{-1} = 1$. Then

$$g = dfd^{-1}f^{-1}, \quad \text{where } d = wy^{-1}xt^{-1} \text{ and } f = tx^{-1}yay^{-1}xt^{-1}.$$

2.03. Counter-example. The converse of 2.01 is false. Let A_ω (cf. [7]) be the set of all even permutations on the positive integers in which only a finite number of symbols is displaced. Then (i) every element in A_ω is a commutator; (ii) there is no positive integer ν such that C^ν covers A_ω, no matter what C may be.

2.04. LEMMA. *Let* C *and* C^* *be classes in the group* G *such that* $CC^* \supset G$. *Then*

(i) $|C| = |C^*|$ (*cardinality*);

(ii) *every element in* C *has an inverse in* C^*;

(iii) *every element in* G *is a commutator*;

(iv) *for any* $a \in C$ *and* $g \in G$, g *is similar* (*conjugate*) *to a commutator of* a (*i.e., there are* $z, y \in G$ *with* $zgz^{-1} = aya^{-1}y^{-1}$).

Proof. If $aa^* = 1$, then $(sas^{-1})(sa^*s^{-1}) = 1$, from which (ii) follows. To see (i), observe that $a \to a^{-1}$ gives a one-to-one correspondence between the elements of C and C^*. Regarding (iii), let $g = ab^*$. Then there is an s such that $b^* = sa^{-1}s^{-1}$. To see (iv), note that if $g = (z^{-1}az)(sa^{-1}s^{-1})$, then

$$zgz^{-1} = a(zs)a^{-1}(zs)^{-1}.$$

2.05. LEMMA. *If every element of* G *is conjugate to some commutator of a fixed element* $a \in G$, *then there exist classes* C *and* C^* *satisfying the assumption of Lemma* 2.04. *Moreover,* $a \in C$.

Extensions of 2.04 appear in [4].

3. Classes of period 2. In this section it is proved that, if $n > 6$, there is no class C of period 2 in A_n such that $CC \supset A_n$. (On the other hand, $C^* = \{x(12)(34)x^{-1} \mid x \in A_n\}$ is such a class if $n = 5$ or 6.) The proof separates into four cases, according to the residue of n (mod 4).

3.01. LEMMA. *A k-cycle cannot be written as a product of fewer than $k-1$ transpositions* (see [5], p. 15).

3.02. LEMMA. *Let $n = 4k > 4$. There is no class C of period 2 in A_n such that CC covers A_n.*

Proof. If C is a class generated by a product of $2k-2$ (or fewer) transpositions, CC does not cover a $(4k-1)$-cycle. The same contradiction arises if C is the class generated by a product of $2k$ transpositions, since no element in CC can fix an odd number of letters.

The case $n = 4k+3 > 3$ is similar. The arguments needed in the other two cases (Lemmas 3.03 and 3.04) are of a different sort, and we include a detailed proof of one of these.

3.03. LEMMA. *Let $n = 4k+2 > 6$. There is no class C of period 2 in A_n such that CC covers A_n.*

Proof. It is only necessary to show that if C is the class generated by a product of $2k$ transpositions, then CC contains no permutation $(abc)(de)(fghj)$. If $\sigma = (12)(34)\ldots(n-3, n-2)$, this amounts to showing that there is no collection of distinct letters $a, \ldots, j$ such that $\tau = (abc)(de)(fghj)\sigma$ is a product of $2k$ transpositions. A *reductio ad absurdum* argument is needed in each of the five cases for (abc) equal to (i) (123), (ii) (135), (iii) $(12\ n)$, (iv) $(13\ n)$, (v) $(1, n-1, n)$.

In case (i), $\tau 2 = 4$, but $\tau 4 \neq 2$. In case (iv), $\tau^2 3 = 2$, $\tau^2 3 \neq 3$. In case (v), $\tau^2 1 = n \neq 1$. In case (ii), $\tau 1 = 4$, $\tau 3 = 6$, $\tau 5 = 2$. But then, $(de)(fghj)$ must have the 3-cycle (642) as a factor. In case (iii), the argument is closer: (de) must be either (34), (35) or $(3, n-1)$. These subcases are eliminated individually.

3.04. LEMMA. *If $n = 4k+1 > 5$, there is no class C of period 2 in A_n such that CC covers A_n.*

The class $(abc)(de)(fghj)$ is again not covered.

3.05. THEOREM. *If $n > 6$, there is no class C of period 2 in A_n such that $CC \supset A_n$.*

4. Classes of period 3. Tables in [4] show that, for $n = 5, 7, 8, 9, 11, 12$, there are classes C of type $1^2 3$, $1^1 3^2$, $1^2 3^2$, $1^3 3^2$, $1^2 3^3$, $1^3 3^3$, respectively, such that $CC \supset A_n$.

4.01. LEMMA. *There is no class C of period 3 in A_6 such that $CC \supset A_6$.*

Proof. There are two classes of period 3. The class of 3-cycles is, obviously, not a candidate ((12)(3456) is not covered). To complete the proof, it is enough to show that $(ab)(cdef)(123)(456)$ cannot be a product of two disjoint 3-cycles. The only cases are $a = 1$, $b = 2$ and $a = 1$, $b = 4$. The details are easily supplied.

4.02. LEMMA. *If $n = 12l+10$ $(l \geqslant 0)$, there is no class C of period 3 such that $CC \supset A_n$.*

The proof is lengthy; details are given in the Appendix. The type $2^{6k+3}4$ is not covered, and in A_{10} this is the only class not covered.

4.03. Remark. Let r and ν be given. There may be an $N = N(r, \nu)$ such that, for all $n > N$ (or for infinitely many $n > N$), there is no class C of period r such that $C^{\nu} \supset A_n$. Theorem 3.05 and Lemma 4.02 decide this problem in the cases $r = 2, 3$ and $\nu = 2$.

5. The maximal value of $\nu(C)$ in A_n. If a class C s small, its exponent $\nu(C)$ may be very large. In this section it is shown that, for the class $1^{n-3}3^1$ of period 3, the exponent ν is $[n/2]$. For $n > 6$, this is the smallest non--trivial class in A_n.

5.01. LEMMA. *If C is the class of a 3-cycle in A_n $(n > 4)$, and $e = [n/2]$, then C^{e-1} does not cover A_n.*

Proof. If n is odd and the product of $e-1$ 3-cycles is a k-cycle, then $k \leqslant 3(e-1)-(e-2) < n$, so an n-cycle is not obtainable. If n is even, the product of $e-1$ 3-cycles cannot yield $(12)(34 \ldots n)$. (To avoid a 3-cycle in the product, each factor must have a letter in common with another factor.)

5.02. THEOREM. *If C is the class $1^{n-3}3^1$ in A_n, then $\nu(C) = [n/2] = e$.*

Proof. It has to be shown that every permutation $g \in A_n$ is a product of e 3-cycles. If g is a k-cycle and $r = (k+1)/2$, the formula

$$(1, 2, k)(k, 3, k-1)(k-1, 4, k-2) \ldots (k-r+3, r, k-r+2) = (12 \ldots k)$$

shows that g is a product of $(k-1)/2$ 3-cycles. If g is a product of several disjoint cycles, one of which is a k-cycle in A_n, an inductive argument can be used. It will conclude with the observations

$$(k-1)/2+(n-k)/2 = [n/2] \quad \text{if } n \text{ is odd},$$

and

$$(k-1)/2+(n-k-1)/2 < [n/2] \quad \text{if } n \text{ is even}.$$

Finally, g can be a product of several disjoint cycles, none of which by itself is in A_n. The only case requiring a detailed proof is that in which g is a product of only two disjoint cycles, each of which involves an even number of letters. The following formulas suggest the proof:

$$\begin{aligned}
(143)(142) &= (12)(34),\\
(123)(316)(645) &= (12)(3456),\\
(123)(318)(847)(756) &= (12)(345678),\\
&\ldots\ldots\ldots\ldots\\
(145)(423)(518)(867) &= (1234)(5678).
\end{aligned}$$

(The notation needed to make the proof formally correct would not make the proof more comprehensible.)

PROBLEM. Presumably, for every class C in A_n, $\nu(C) \leqslant [n/2]$. **(P 913)**

6. Covering theorems in $PSL(n, K)$. The group $PSL(3, 4)$ has 20160 elements (but is not isomorphic to A_8). There are 11 classes in A_8, but only 10 in $PSL(3, 4)$; their periods are 1, 2, 3, 4, 4, 4, 5, 5, 7, 7. The class of period 3 has the exponent 2, as tables in [4] show. So also does each class of period 4.

6.01. LEMMA. *Let K be an infinite field and let $n > 1$. There is a class C in $PSL(n, K)$ that involves no more than $2n-1$ parameters (i.e., it lies on an algebraic manifold of dimension not greater than $2n-1$).*

Proof. The class C of the transvection

$$\operatorname{diag}[F, I], \qquad F = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

has this property.

6.02. THEOREM. *If K is an infinite field, there is a class C in $PSL(n, K)$ such that $\nu(C) \geqslant (n^2-2)/(2n-1)$.*

Proof. $PSL(n, K)$ is an algebraic manifold, and its dimension is at least n^2-2.

7. Self-coverings.

7.01. THEOREM. *Let C be any class in A_n and let C^* be its conjugate in S_n $(n > 4)$. Then $CC \supset C$ and $CC \supset C^*$.*

The proof is an easy consequence of Lemmas 7.02 and 7.03.

7.02. LEMMA. *Let g and h be disjoint cycles on $2l > 0$ and $2m-2l > 0$ letters, respectively. Then there exist cycles k_1, t_1, k_2, t_2 such that $k_1 t_1 k_2 t_2 = gh$ and, for each $i = 1, 2$, k_i is a $2l$-cycle, t_i is a disjoint $(2m-2l)$-cycle, and k_i, t_i move exactly the same $2m$ letters as g, h do.*

For example, $(13)(2546)(23)(1465) = (12)(3456)$.

Proof. If

$$g = (2, 4, 6, \ldots, 2l-2, 2l, 3, 5, \ldots, 2l-1, 2l+1),$$
$$h = (1, 2l+3, 2l+5, \ldots, 2m-3, 2m-1, 2l+2, 2l+4, \ldots, 2m-2, 2m),$$

the formulas for k_i and t_i are

$$k_1 = (1, 2, \ldots, 2l), \qquad t_1 = (2l+1, 2l+2, \ldots, 2m),$$
$$k_2 = (1, 3, 4, \ldots, 2l, 2l+1), \qquad t_2 = (2, 2l+3, 2l+4, \ldots, 2m, 2l+2).$$

7.03. LEMMA. *Let $r > 3$ be odd. Then there exist r-cycles k, t_1, t_2 on the letters $1, 2, \ldots, r$, in the same class in A_r (and in A_{r+1}), such that kt_1 and kt_2 are both r-cycles, but belong to different classes in A_r (and in A_{r+1}).*

Proof. Take $t_1 = k = (12 \ldots r)$ and $t_2 = (13)(24)k(13)(24)$. Then

$$kt_1 = (1, 3, 5, \ldots, r, 2, 4, \ldots, r-3, r-1),$$
$$kt_2 = (3, 1, 5, \ldots, r, 2, 4, \ldots, r-3, r-1),$$

as asserted.

Appendix. The proof of Lemma 4.02 is carried in two stages: Lemma 1 and Lemma 2.

LEMMA 1. *Let* $n = 12l+10$ $(l \geqslant 0)$ *and let* C *be the class of type* 3^{3+4l} *in* A_n. *The CC does not cover the type* $2^{6l+3}4$ *in* A_n.

Proof. Let σ be a product of $4l+3$ disjoint 3-cycles. We prove that there is no permutation τ of type $2^{6l+3}4$ such that $\tau\sigma$ is a product of $4l+3$ disjoint 3-cycles. It will be convenient to write $k = 4l+3$, so that $n = 3k+1$.

We shall assume that there is such a τ, and arrive at a contradiction in every case. First note that exactly one letter is fixed in $\tau\sigma$.

We let, without loss of generality,

$$\sigma = (123)(456)(789)\ldots(3k-2, 3k-1, 3k),$$

and consider the various possibilities for τ. The letters of the 4-cycle in τ can be disposed among the 3-cycles of σ and the letter $3k+1$ as in Table 1.

Consider the 7 cases in the table in order.

1 (a) $(1234)\sigma = (1\,3\,5\ldots$; need (35) in τ to close off 3-cycle.
  (b) $(1324)\sigma = (1)(3)\ldots$; 2 letters fixed.

2 (a) $(123\ 3k+1)\sigma = (1\ 3\ 3k+1\ 2)\ldots$
  (b) $(132\ 3k+1)\sigma = (2\ 3k+1)\ldots$

3 (a) $(1245)\sigma = (25)\ldots$
  (b) $(1246)\sigma = (625\ldots$; need $5 \to 5$ in τ to close off 3-cycle.
  (c) $(1346)\sigma = (1)(4)\ldots$; 2 letters fixed.

4 (a) $(1247)(3x)\ldots\cdot\sigma = (13y\ldots$; here, $x \to y$ in σ. To close off the 3-cycle, we need $(3y)$ in τ, requiring $x = y$.

(b) $(1347)\ldots\cdot\sigma = (1)(35\ y)(48\ v)(72\ z)\ldots$, say, where first we need $(5x)(2y)$ in τ and $x \to y$ in σ in order to close off the first 3-cycle. Then $(9z)$ in τ and $y \to z$ in σ are required to close off the third 3-cycle. None of x, y, z appears in the 4-cycle, and hence $(xyz) \neq (123)$, (456), (789). Therefore, without loss of generality, $(xyz) = (10\ 11\ 12)$.

Table 1

Case No.	3-cycles in σ (123)	(456)	(789)	(10 11 12)...	letter $3k+1$	4-cycles in τ that must be considered
1	3	1				(a) (1234), (b) (1324)
2	3				1	(a) $(123\ 3k+1)$, (b) $(132\ 3k+1)$
3	2	2				(a) (1245), (b) (1246), (c) (1346)
4	2	1	1			(a) (1247), (b) (1347)
5	2	1			1	(a) $(124\ 3k+1)$, (b) $(134\ 3k+1)$
6	1	1	1	1	(assuming $n = 3k+1 > 10$)	(147 10)
7	1	1	1		1	$(147\ 3k+1)$

Table 2

Case No.	3-cycles in σ (123)(456)(789)...		letters a_1	a_2	a_3	a_4	4-cycles in τ that must be considered
We have cases 1 to 7 as before. In addition:							
5′	2		1	1			(a) $(12a_1a_2)$, (b) $(13a_1a_2)$
7′	1	1	1	1			$(14a_1a_2)$
7″	1		1	1	1		$(1a_1a_2a_3)$
7‴			1	1	1	1	$(a_1a_2a_3a_4)$

Now $(8u)$ and $(6v)$ in τ and $u \to v$ in σ are required to close off the second 3-cycle. Without loss of generality, $u = 13$ and $v = 14$. Thus we have

$$\tau\sigma = (1347)(5\,10)(2\,11)(9\,12)(8\,13)(6\,14)\ldots\cdot\sigma = (1)(35\,11)(48\,14)(72\,12)\ldots$$

In τ, 15 must pair with a letter from a 3-cycle in σ other than (13 14 15), without loss of generality, with 16. Thus (15 16) is in τ and we have $\tau\sigma = (16\ 13\ 9\ 10\ \ldots$

Note that if n is too small (less than 22), we cannot fill out the transpositions in τ that are needed to close the 3-cycles. A similar remark applies elsewhere in the proof.

5 (a) $(124\ 3k+1)\sigma = (4\ 3k+1\ 2\ 5\ \ldots$

(b) $(134\ 3k+1)\ldots\cdot\sigma = (1)(3\ 5\ \text{-})(4\ 3k+1\ 2)\ldots$, and (26) is needed in τ to close off the last 3-cycle. But then $\tau\sigma = (6\ 3\ 5\ \ldots$ and to close off this 3-cycle we need $5 \to 5$ in τ.

6. Consider $3k+1$ (recall we assume here that $3k+1 > 10$).

(i) $(147\ 10)(2\ 3k+1)\sigma = (2\ 3k+1\ 3\ \ldots$; need (13) in τ to close.

(ii) $(147\ 10)(3\ 3k+1)\sigma = (3\ 3k+1\ 1\ 5\ \ldots$

(iii) $(1\ 4\ 7\ 10)(13\ 3k+1)\ldots\cdot\sigma = (13\ 3k+1\ 14)\ldots$; this requires (14 15) in τ to close the 3-cycle. Note that 15 is thus fixed.

Now we examine the consequences of closing other 3-cycles in the product $\tau\sigma$:

$$\tau\sigma = (13\ 3k+1\ 14)(1\ 5\ y)(4\ 8\ v)(7\ 11\ s)(10\ 2\ n)\ldots$$

In order to close these 3-cycles we would require, successively:

$(5x)(3y)$ in τ and $x \to y$ in σ,
$(8u)(6v)$ in τ and $u \to v$ in σ,
$(11r)(9s)$ in τ and $r \to s$ in σ,
$(2m)(12\,n)$ in τ and $m \to n$ in σ.

One can easily check that no three of $x, y, u, v, \ldots$ can be in the same 3-cycle in σ. For example, if (xyu) were in σ, then $v = x$, and then $(5x)$ and $(6x)$ would both have to appear in τ. Thus, without loss of generality, we have

$\tau =$

$(1\,4\,7\,10)(13\ \ 3k+1)(14\,15)(5\,16)(3\,17)(8\,19)(6\,20)(11\,22)(9\,23)(2\,25)(12\,26)$

and

$$\tau\sigma = (13\ 3k+1\ 14)(1\ 5\ 17)(4\ 8\ 20)(7\ 11\ 23)(10\ 2\ 26)\ldots$$

Now consider the letter 18:

(18 21) in τ gives $\tau\sigma = (18\ 19\ 9\ 24\ \ldots;$

(18 28)(29 21) in τ gives $\tau\sigma = (18\ 29\ 19\ 9\ \ldots;$

(18 28)(29 30) in τ fixes 30 in $\tau\sigma$, and 15 is already fixed;

(18 28)(29 31) in τ gives $\tau\sigma = (18\ 29\ 32\ \ldots$, and this last requires (32 17) in τ to close off the 3-cycle.

The argument above is valid for $n \geqslant 34$. If $n = 22$, then there are not enough letters to fill out all of the transpositions that are needed to close the 3-cycles involved.

7. First consider the case $n = 3k+1 = 10$. Then $\sigma = (123)(456)(789)$ and, therefore, by the assumption,

$$\tau\sigma = (147\ 10)\ldots\cdot\sigma = (15\ \text{-})(48\ \text{-})(7\ 10\ 2).$$

Here we required (29) in τ in order to close the last 3-cycle. The letters 3, 5, 6, 8 form the remaining transpositions. Since one letter in $\tau\sigma$ must be fixed, we need (56). But

$$(1\ 4\ 7\ 10)(29)(56)(\text{-}\ \text{-})\sigma = (5\ 4\ 8\ \ldots$$

and we would need (48) in τ to close off this cycle.

Now let $n \geqslant 22$. We have

$$(147\ 3k+1)\sigma = (7\ 3k+1\ 2\ \ldots$$

and this requires (29) in τ to close off. Since one letter in $\tau\sigma$ is fixed, another transposition must be, without loss of generality, (56) or (10 11). As above, (56) does not work. With (10 11) in τ, we still have to dispose the letter 8; the transpositions containing 8 can, without loss of generality, be (83), (85), (86), (8 12) or (8 13):

$$
\begin{aligned}
&(83)(10\ 11)(2\ 9)(1\ 4\ 7\ 3k+1)\sigma = (4\ 8\ 15\ \ldots,\\
&(85)\ \ldots\ldots\ldots\ldots\ldots\ldots = (4\ 8\ 6\ x\ \ldots, \qquad \text{where } x \neq 4,\\
&(86)\ \ldots\ldots\ldots\ldots\ldots\ldots = (48)\ldots,\\
&(8\ 12)\ \ldots\ldots\ldots\ldots\ldots = (4\ 8\ 10\ 12\ \ldots,\\
&(8\ 13)\ \ldots\ldots\ldots\ldots\ldots = (4\ 8\ 14)(13\ 9\ 3)\ldots
\end{aligned}
$$

In the last case, in order to close the 3-cycles shown, we need (6 14) and (3 15) in τ. But

$$(6\ 14)(3\ 15)(8\ 13)(10\ 11)(2\ 9)(1\ 4\ 7\ 3k+1)\sigma = (6\ 15\ 1\ 5\ \dots).$$

We have excluded all possibilities for τ, and so Lemma 1 is proved.

LEMMA 2. *Let* $n = 12l+10$ $(l \geqslant 0)$, *and let* C *be a class of type* 3^t, $t < 4l+3$. *Then* CC *does not cover the class of type* $2^{6l+3}4$ *in* A_n.

Proof. We proceed as in Lemma 1. Let

$$\sigma = (123)(456)\dots(3t-2, 3t-1, 3t),$$

$k = 4l+3$, and τ as before. Note that in $\tau\sigma$ at least 4 letters are fixed. The letters of the 4-cycle in τ can be disposed among the cycles of σ and the letters $3k+1$, $3k$, $3k-1$, $3k-2$ (denote these by a_1, a_2, a_3, a_4, respectively) as in Table 2.

The cases 1 (a) and 2-6 are disposed of as in Lemma 1. So is the case 7, with t in place of k there. We consider the remaining cases.

1 (b) $(1324)(56)\sigma = (1)(3)(254)\dots$; we require (56) in τ to close the 3-cycle here. This fixes 6, and one more letter must be fixed. This requires, without loss of generality, (78), and hence also (9 10). But

$$(1324)(56)(78)(9\ 10)\big(11\ \ \tau(11)\big)\sigma = (1)(3)(6)(8)(254)(7\ 9\ 11\dots$$

and $\tau(11) \neq 9$, so that this last cycle is not closed at length 3.

Here, if the number t of 3-cycles in σ were too small, then while the argument above would not be appropriate, it would be the case that some of the transpositions in τ would be left over in $\tau\sigma$. A similar remark applies in some of the other cases.

5′ (a) Without loss of generality, one transposition is (34). Thus $(12\, a_1\, a_2)(34)\sigma = (a_1\, a_2\, 2)(1\ 3\ 5\dots$; require (35) in τ to close.

(b) $(13\, a_1\, a_2)(24)\sigma = (a_1\, a_2\, 25\dots$

7′. $(14\, a_1\, a_2)\sigma = (a_1\, a_2\, 2\dots)$; need $(2\, a_1)$ in τ to close.

7″. $(1\, a_1\, a_2\, a_3)\sigma = (a_1\, a_2\, a_3\, 2\dots$

7‴. $(a_1\, a_2\, a_3\, a_4)\sigma = (a_1\, a_2\, a_3\, a_4)\dots$

All possibilities for τ having been excluded, we have proved Lemma 2.

Acknowledgment. We acknowledge with thanks criticism and contributions from W. G. Brown, and from J. Wiegold, who has kindly communicated the proof of Lemma 7.02. B. H. Neumann kindly supplied some references. We are indebted to D. H. Lehmer for assistance in programming one of our computations.

REFERENCES

[1] E. A. Bertram, *Even permutations as a product of two conjugate cycles*, Journal of Combinatorial Theory 12 (1972), p. 368-380.

[2] J. L. Brenner, *Research problem in group theory*, Bulletin of the American Mathematical Society 66 (1960), p. 275.

[3] — *Covering theorems for nonabelian simple groups. II*, Journal of Combinatorial Theory 14 (1973), p. 264-269.

[4] — M. Randall and J. Riddell, *Covering theorems for finite nonabelian simple groups. I*, University of Victoria Report 1971.

[5] R. D. Carmichael, *Introduction to the theory of groups of finite order*, New York 1956.

[6] N. Ito, *A theorem on the alternating group* $\mathfrak{A}_n$ ($n \geqslant 5$), Mathematica Japonicae 2 (1950-1952), p. 59-60.

[7] J. Schreier and S. Ulam, *Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Mathematica 4 (1933), p. 134-141.

[8] Cheng-hao Xu, *The commutators of the alternating group*, Scientia Sinica 14 (1965), p. 339-342.

Reçu par la Rédaction le 15. 1. 1973