J. Austral. Math. Soc. 25 (Series A) (1978), 210–214

COVERING THEOREMS FOR FINASIGS VIII—ALMOST ALL CONJUGACY CLASSES IN $\mathscr{A}_n$ HAVE EXPONENT $\leqslant 4$

J. L. BRENNER

(Received 21 April; revised 15 November 1976)

Communicated by W. D. Wallis

Abstract

The product of two subsets C, D of a group is defined as

$$CD = \{\alpha\beta \mid \alpha \in C, \beta \in D\}.$$

The power C^e is defined inductively by $C^0 = \{1\}$, $C^e = CC^{e-1} = C^{e-1}C$. It is known that in the alternating group $\mathscr{A}_n$, $n > 4$, there is a conjugacy class C such that CC covers $\mathscr{A}_n$. On the other hand, there is a conjugacy class D such that not only $DD \neq \mathscr{A}_n$, but even $D^e \neq \mathscr{A}_n$ for $e < [n/2]$. It may be conjectured that as $n \to \infty$, almost all classes C satisfy $C^3 = \mathscr{A}_n$. In this article, it is shown that as $n \to \infty$, almost all classes C satisfy $C^4 = \mathscr{A}_n$.

Subject classification (Amer. Math. Soc. (MOS) 1970): 20 D 05, 20 B 99.

1. Introduction

Let G be a FINASIG (finite nonabelian simple group), and let C be a conjugacy class in G. The power C^ν is defined inductively by

$$C^1 = C, \quad C^2 = CC, \quad C^\nu = CC^{\nu-1} = C^{\nu-1}C,$$

where $CD = \{\alpha\beta \mid \alpha \in C, \beta \in D\}$. The questions considered in this note revolve around the set of values that can be assumed by $\nu(C)$, the lowest exponent for which $C^\nu = G$. In particular, what is the expected value of ν? A modest start is made on this question by establishing that, if G runs through the collection of finite alternating groups, the expected value of this exponent (for covering) is $\leqslant 4$. I believe the expected value to be 3; the methods that will be needed to establish that fact are considerably more elaborate than the methods of this article. To paraphrase the main result, if κ_n is the relative frequency of classes C in $\mathscr{A}_n$ with the property $C^4 = \mathscr{A}_n$, then $\kappa_n \to 1$ as $n \to \infty$. It might be possible to reduce "4" to "3" by applying the present methods, but elaborating the technique.

Next, let C_n, D_n, E_n, F_n be any four conjugacy classes in $\mathscr{A}_n$. The statistical probability that $C_n D_n E_n F_n$ covers $\mathscr{A}_n \setminus 1$ seems again to be $1 - \varepsilon_n$, where $\varepsilon_n \to 0$ as $n \to \infty$. For the product $C_n D_n$ of two randomly chosen conjugacy classes, this is no longer true. The truth of the corresponding assertion for the product $C_n D_n E_n$ of three conjugacy classes remains open.

https://doi.org/10.1017/S1446788700038799 Published online by Cambridge University Press

Certain results concerning $\mathscr{A}_\omega$, the alternating (finite support) permutation group on the positive integers, follow from the results of this article.

2. Some lemmata

First, a description of the conjugacy classes in the symmetric and alternating groups, $\mathscr{S}_n$ and $\mathscr{A}_n$.

2.01 LEMMA. *Two permutations are conjugate in $\mathscr{S}_n$ if and only if they have the same (canonical) cycle structure. This condition is tantamount to the requirement that the permutations have orbits that match in number and respective lengths.*

2.02 LEMMA. *A permutation $P \in \mathscr{S}_n$ (and hence its class) lies in $\mathscr{A}_n$ if and only if it has an even number (or 0) orbits of even degree.*

2.03 LEMMA (Scott (1964), p. 299). *With certain exceptions, a class in $\mathscr{S}_n$ is also a class in $\mathscr{A}_n$ (if the class intersects $\mathscr{A}_n$). The exceptional classes are those in which all orbits have different odd degrees: these classes bifurcate into two conjugacy classes in $\mathscr{A}_n$.*

They are relatively rare, that is, the asymptotic density is 0 for this collection of classes. This is intuitively clear; the formal proof is omitted. A "trivial orbit" has degree 1.

2.04 LEMMA. (Hardy and Ramanujan (1918)). *The number $\rho(n)$ of nonexceptional classes in $\mathscr{A}_n$ increases like $c\exp(\alpha\sqrt{n})/n$, where c, α are constants.*

Indeed somewhat more than half the partitions of n correspond to a non-exceptional class in $\mathscr{A}_n$.

2.05. LEMMA. *Let $n > 5$ be odd; let C_n be a class of n-cycles in $\mathscr{A}_n$. Then $C_n C_n$ covers $A_n \setminus 1$.*

2.06 LEMMA (Brenner and Riddell (1976), p. 102, Theorems 7.07, 7.08). *Let $n > 6$ be even; $n = 2m$. Let C_n be the class of type m^2 in $\mathscr{A}_n$. Then C_n^2 covers $\mathscr{A}_n$.*

3. The main theorem

The principal tool is Lemma 3.01.

3.01 LEMMA. *Let $n > 5$, $n = l(1) + l(2) + \dots + l(r)$, $r > 1$, $1 < l(i) \leqslant n$, be a decomposition of n into r summands, all exceeding 1. Let T be the corresponding type (conjugacy class in $\mathscr{S}_n$).*

(i) *If n is odd, T^2 contains all n-cycles.*

(ii) *If $n = 2m$ is even, T^2 contains the class m^2 in $\mathscr{A}_n$.*

PROOF. Direct construction. Let $k(i) = \sum_1^i l(j)$, $P = \sigma_1 \sigma_2 \dots \sigma_r$,

$$\sigma_1 = (1,2,\dots,k(1)),$$
$$\sigma_2 = (k(1)+1,\dots,k(2)),$$
$$\sigma_i = (k(i-1)+1,\dots,k(i)),$$
$$\sigma_r = (k(r-1)+1,\dots,k(r)).$$

Define Q from P by swapping the end-letters of each cycle, thus

$$Q = \tau_1 \tau_2 \dots \tau_r,$$

where

$$\tau_1 = (1,2,\dots,k(1)-1,k(1)+1),$$
$$\tau_2 = (k(1),k(1)+2,\dots,k(2)-1,k(2)+1),$$
$$\tau_i = (k(i-1),k(i-1)+2,\dots,k(i)-1,k(i)+1),$$
$$\tau_r = (k(r-1),k(r-1)+2,\dots,k(r)),$$
$$Q = \beta^{-1}P\beta, \quad \beta = (k(1),k(1)+1)(k(2),k(2)+1)\dots(k(r-1),k(r-1)+1).$$

Then PQ has the form asserted.

For example:

$$(123)(45)(678)\cdot(124)(36)(578) = (1475)(2683),$$
$$(123)(45)(67)\cdot(124)(36)(57) = (1473265).$$

So far, the lemma is proved when n is even; when n is odd, it is clear that T^2 contains n-cycles. But an outer automorphism of $\mathscr{A}_n$ produces all n-cycles from any one of them.

3.02 DEFINITION. Let P be a permutation in $\mathscr{A}_n$, $P = C_1 \dots C_h D_1 \dots D_s$, where C_i are all nontrivial cycles (orbits), D_i are all 1-cycles (trivial orbits). The *orbital excess* of P is $\sum_i(|C_i|-2)-s$.

3.03 LEMMA. *Let $P \in \mathscr{A}_n$ have nonnegative orbital excess, $n > 5$.*

(i) *If n is odd, every n-cycle is a product of two conjugates of P.*

(ii) *If n is even, every permutation of type $(\frac{1}{2}n)^2$ is a product of two conjugates of P.*

PROOF. Let P be given; form Q from P as in the proof of 3.01. Then replace the excess letters in some or all of the τ_i by the letters $k(r)+1,\dots,n$. The *excess letters* are by definition the letters that are not explicitly displayed in P. The permutation Q_1 formed from Q in this way:

$$Q_1 = \gamma^{-1}Q\gamma,$$
$$\gamma = (1,k(r)+1)(2,k(r)+2)\dots(k(1)-1,\dots)(k(1)+2,\dots)\dots,$$

is such that PQ_1 is an n-cycle if n is odd, and is the product of two disjoint $(\frac{1}{2}n)$-cycles if n is even.

REMARK. If r is odd, and if $P \in \mathscr{A}_n$, then P, Q belong to the same class in $\mathscr{A}_n$. If r is even, the same assertion is true, unless P belongs to an exceptional class in $\mathscr{A}_n$. Furthermore, Q, Q_1 belong to the same class in $\mathscr{A}_n$ if this is not an exceptional class.

3.04 LEMMA. *If C is a nonexceptional class in $\mathscr{A}_n$, then $CC \supset 1$. If C is any class in $\mathscr{A}_n$, then $CC \supset C$.*

The second assertion is proved in Brenner (1973).

3.05 THEOREM. *Let C be a nonexceptional class in $\mathscr{A}_n$ with orbital excess $\geqslant -1$. Then $C^4 = \mathscr{A}_n$.*

PROOF. This follows from the lemmata.

Now let $p(\,)$ be the unrestricted partition function. The arguments needed to complete the proof of the asymptotic result stated in the introduction are as follows. The orbital excess of any class (or permutation) is $n-2r$, where r is the number of orbits. Only if $n-2r<-1$ does the relation $C^4 = \mathscr{A}_n$ fail to hold. But then, $r > \frac{1}{2}(n+1)$: the number of orbits must be large. The corresponding partition of n has a "conjugate partition" in which the largest part exceeds $\frac{1}{2}(n+1)$. Now the number of partitions of n in which the largest part is exactly d is $p(n-d)$. Thus the number of classes C that do not satisfy $C^4 = \mathscr{A}_n$ is less than $\sum_{i \leqslant \frac{1}{2}n+1} p(i)$. D. H. Lehmer pointed out to me that this sum is asymptotic to

$$\sqrt{8}\, c \exp\{\alpha \sqrt{n}/\sqrt{2}\}/(\alpha \sqrt{n}).$$

Thus, as asserted, the ratio of this sum to $p(n)$, and hence to the number of classes in $\mathscr{A}_n$, approaches 0 as $n \to \infty$. This is what was asserted.

3.06 LEMMA. *Let T be the type 2^{2m} in $\mathscr{A}_{4n}$. The type $1^{4m-3}\,3^1$ is not included in any of T, T^2, T^3.*

PROOF. Anything in T^2 has double type $1^{2x}\,2^{2y}\,3^{2z} \ldots$. Thus T^3 can include the permutation $P = (123)$ of type $1^{4m-3}\,3^1$ only if there is a permutation Q in T such that PQ has double type. There is obviously no such permutation Q.

Lemma 3.06 shows that any improvement of the main theorem (replacing 4 by 3) will require some modifications. In particular not only the class 2^{2m}, but also (for large m) all classes $T \oplus 2^{2m}$ must probably be excluded. It is an open question whether other classes must be excluded.

Material correlative to the subject matter of this article appears in Herzog and Reid (1976, 1977). The exponent 4 appears in Rabinovič and Feĭnberg (1974) in connection with the transformations of a totally ordered set.

A weak covering theorem for $\mathscr{A}_\omega$ follows from the present results. The group $\mathscr{A}_\omega$ is the (simple) group of permutations of finite support on the postive integers. The group $\mathscr{A}_\infty$ is the group of all permutations on the same set.

3.07. THEOREM. *Let C be a class in $\mathscr{A}_\infty$ with infinite support. Then C^4 covers $\mathscr{A}_\omega$.*

REFERENCES

J. L. Brenner (1973), "Covering theorems for nonabelian simple groups II", *J. Combinatorial Theory* (A) **14**, 264–269.

J. L. Brenner (1975), "Covering theorems for finite nonabelian simple groups, IV", *Jñānabha*, Section A, **3**, 77–84.

J. L. Brenner (1977), "Covering theorems for FINASIGS. IX", *Ars Combinatoria* **4**, 151–176.

J. L. Brenner and L. Carlitz (1976), "Covering theorems for finite nonabelian simple groups. III. Solution of the equation $x^2+y^2+y^{-2} = a$ in a finite field", *Rend. Seminario Mat. di Padova* **55**, 81–90.

J. L. Brenner, R. M. Cranwell and J. Riddell (1974), "Covering theorems for nonabelian simple groups. V", *Pacific J. Math.* **58**, 55–60.

J. L. Brenner, M. Randall and J. Riddell (1974), "Covering theorems for nonabelian simple groups. I", *Colloq. Math.* **32**, 39–48.

J. L. Brenner and J. Riddell (1976), "Covering theorems for nonabelian simple groups. VII. Asymptotics in the alternating groups", *Ars Combinatoria* **1**, 77–108.

J. L. Brenner and J. Riddell (1977), "Noncanonical factorization of a permutation ($\equiv$Covering Theorems VI)" *American Mathematical Monthly*, **84**, no. 1, 39–40.

G. H. Hardy and S. Ramanujan (1918), "Asymptotic formulae in combinatory analysis", *Proc. London Math. Soc.* (2) **17**, 75–115.

M. Herzog and K. B. Reid (1976), "Number of factors in k-cycle decompositions of permutations", *Proc. 4th Australian Conference Combinatorial Math* (Springer Lecture Notes in Math **560**, 123–131).

M. Herzog and K. B. Reid (1977), "Representation of permutations as products of cycles of fixed length", *J. Austral. Math. Soc.* **22**, (Ser. A), 321–331.

E. B. Rabinovič and V. Z. Feĭnberg (1974), "Normal divisors of a 2-transitive group of automorphisms of a linearly ordered set", *Mat. Sbornik* **93** (135), no. 2, 189–202.

W. R. Scott (1964), *Group Theory* (Prentice-Hall, Englewood Cliffs, N.J.).

10 Phillips Road
Palo Alto, CA 94303