ISRAEL JOURNAL OF MATHEMATICS, Vol. 67, No. 2, 1989

THE COVERING NUMBERS OF THE SPORADIC SIMPLE GROUPS

BY

ILAN ZISSER†

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Ramat-Aviv, 69978, Israel

ABSTRACT

The covering numbers (cn) and the extended covering numbers (ecn) of all the sporadic simple groups and some other large groups are computed, using "economical" methods. An example is found, namely $D_4(3)$, for which

$$ecn(D_4(3)) - cn(D_4(3)) = 2.$$

I. Introduction

Let G be a finite non-Abelian simple group. The covering number of G is the smallest integer n such that $C^n = G$ for all non-trivial conjugacy classes C of G. The extended covering number of G is the smallest integer r such that $D_1 \cdot D_2 \cdot \cdots \cdot D_r = G$ for every r (not necessarily distinct) non-trivial conjugacy classes $D_1, D_2, \ldots, D_r$ of G.

The object of this paper is to show how to calculate these numbers. Our method will use character theory. This method is an "economical" one, since it does not require a vast quantity of arithmetic operations even for large groups.

The C.D.C. 6600 computer of Tel Aviv University was used to calculate the above numbers for all sporadic groups and some other simple groups. The results are presented in the last section of this article.

II. Definitions and basic theorems

Let G be a finite group. We will denote the number of its conjugacy classes by k. We fix an ordering of the conjugacy classes of G and write:

† These results are part of the author's master's research written at the Tel Aviv University under the supervision of Professor M. Herzog.

Received September 23, 1988 and in revised form March 1, 1989

$$C_1 = \{1\}, C_2, C_3, \ldots, C_k.$$

A representative element of the class C_j will be denoted by g_j. Arbitrary classes of G will be denoted by $D_1, D_2, \ldots$ with representative elements $d_1, d_2, \ldots$ respectively. Finally we fix an ordering of the irreducible characters of G and write:

$$\chi_1 = \{1_G\}, \chi_2, \ldots, \chi_k.$$

Let $\phi \neq A \subseteq G$. In [AHS] it is proven that there exists a positive integer n such that $A^n \leqq G$ (i.e. A^n is a subgroup of G). If we take for A a non-central conjugacy class C of G we can conclude that there exists an n such that $1 \neq A^n \lhd G$. In particular, if G is a non-Abelian simple group, we get that for every conjugacy class $C \neq 1$ there is a natural n such that $C^n = G$.

From now on the term "simple group" will denote a non-Abelian simple group. Let G be a simple group. We define the covering number of G as the least natural number n, such that $C_i^n = G$ for $i = 2, 3, \ldots, k$. This number will be denoted by $cn(G)$. The extended covering number of G is the least natural, number r, such that $D_1 \cdot D_2 \cdot \cdots \cdot D_r = G$ for every r non-trivial conjugacy classes $D_1, D_2, \ldots, D_r$ of G. This r will be denoted by $ecn(G)$.

The next theorem serves as the key for handling products of conjugacy classes. Its proof may be found in [AHS].

THEOREM 1. *Let $D_1, D_2, \ldots, D_r$ be conjugacy classes of a finite group G. For every $j = 1, 2, \ldots, k$ we define*:

$$a_j = 1 + \sum_{n=2}^{k} \frac{\prod_{i=1}^{r} \chi_n(d_i)\overline{\chi_n(g_j)}}{\chi_n^{r-1}(1)}.$$

Then $C_j \subseteq D_1 D_2 \cdot \cdots \cdot D_r$ if and only if $a_j \neq 0$.

This theorem enables us to determine which classes appear in the product $D_1 \cdot D_2 \cdot \cdots \cdot D_r$. Since in large groups the number of possible products is vast, it will be impractical to use the theorem directly. We will show how to reduce the number of checkings.

Arad, Herzog and Stavi used Theorem 1 to prove $ecn(G) \leqq 4|G|^{1/2} \ln|G|$ [AHS]. It is possible to improve this result by a more careful analysis of the characters. The improved result is $ecn(G) \leqq 1.3|G|^{1/2} \ln|G|$ [Z]. These bounds for $ecn(G)$ are very weak, but no better general bounds for $cn(G)$ and $ecn(G)$ are known.

Karni [K] used Theorem 1 in order to calculate $cn(G)$ and $ecn(G)$ for some sporadic small-order groups and some simple groups of small order. His method is based upon checking all possible products, so it is not applicable to large groups.

One additional fact should be mentioned. Every group checked by Karni satisfied the relation $cn(G)+1=ecn(G)$. This relation holds also in some families of simple groups, see [D] and [ACM]. In this paper we will give an example of a group that does not satisfy this relation.

III. Calculation of the covering numbers

In this section we will show how to calculate $cn(G)$ and $ecn(G)$. We will start with $cn(G)$. Let C be a conjugacy class of G and let $g \in C$. If $m>1$ then $C^m = G$ if, and only if, for every $j=1,2,\ldots,k$ the following conditions holds:

$$\sum_{j=2}^{k} \frac{\chi_i^m(g)}{\chi_i^{m-1}(1)} \overline{\chi_i(g_j)} \neq -1.$$

Define now the following three class functions:

$$\alpha(g) = \max_{i=2,3,\ldots,k} \frac{|\chi_i(g)|}{\chi_i(1)}, \quad \beta(g) = \sum_{i=2}^{k} \frac{|\chi_i(g)|}{\chi_i(1)}, \quad \gamma(g) = \max_{2 \leq i \leq k} |\chi_i(g)|.$$

LEMMA 1. *If $\beta(g)\gamma^2(g) < 1$ then $C^3 = G$.*

PROOF.

$$\left| \sum_{i=2}^{k} \frac{\chi_i^3(g)}{\chi_i^2(1)} \overline{\chi_i(g_j)} \right| \leq \sum_{i=2}^{k} \frac{|\chi_i(g)|^3}{\chi_i(1)} \leq \max_{2 \leq i \leq k} |\chi_i(g)|^2 \sum_{i=2}^{k} \frac{|\chi_i(g)|}{\chi_i(1)} = \gamma^2(g)\beta(g) < 1.$$

LEMMA 2. *If $\alpha^{m-2}(g) < (|C(g)|-1)^{-1}$ then $C^m = G$.*

PROOF.

$$\begin{aligned}
\left| \sum_{i=2}^{k} \frac{\chi_i^m(g)}{\chi_i^{m-1}(1)} \overline{\chi_i(g_j)} \right| &\leq \sum_{i=2}^{k} |\chi_i(g)|^2 \left(\frac{|\chi_i(g)|}{\chi_i(1)} \right)^{m-2} \\
&\leq \max_{2 \leq i \leq k} \left(\frac{|\chi_i(g)|}{\chi_i(1)} \right)^{m-2} \sum_{i=2}^{k} |\chi_i(g)|^2 \\
&= \alpha^{m-2}(g)(|C(g)|-1) < 1.
\end{aligned}$$

The second orthogonality relation was used in the last equality.

LEMMA 3. *If* $\sum_{i=2}^{k} |\chi_i(g)/\chi_i(1)|^{m-2} |\chi_i^2(g)| < 1$ *then* $C^m = G$.

PROOF. Trivial.

The last three lemmas will be useful, especially when the values of the characters of the group are small relative to the degree of the character. This is the situation in a large number of simple groups. The process of finding $cn(G)$ can now be described as follows:

(1) Find a candidate m for $cn(G)$. We do this by selecting a class C for which the values of the functions α, β and γ are high. For this class we use Theorem 1 in order to find the smallest m such that $C^m = G$.

(2) We have to check that $C_j^m = G$ for every $j = 2, 3, \ldots, k$. The above lemmas can be used in order to verify this fact.

(3) For every class C for which the previous step was not successful, we use Theorem 1 in order to verify that $C_j^m = G$.

(4) If in step 3, a class C was found such that $C_j^m \neq G$ then m is not $cn(G)$ and $m + 1$ is our next candidate. We now go back to step 3 and check only the classes for which $C_j^m \neq G$.

We now turn to $ecn(G)$. The proof of the following lemma is simple.

LEMMA 4. *$ecn(G)$ is the least natural r such that $1 \in D_1 \cdot D_2 \cdot \cdots \cdot D_r$ for every r non-trivial conjugacy classes $D_1, D_2, \ldots, D_r$.*

Let r be a candidate for $ecn(G)$. In order to show that $ecn(G) = r$ we have to verify two facts:

(a) $1 \in D_1 \cdot D_2 \cdot \cdots \cdot D_r$ for every r non-trivial conjugacy classes $D_1, D_2, \ldots, D_r$.

(b) There exist $r - 1$ classes such that $1 \notin D_1 \cdot D_2 \cdot \cdots \cdot D_{r-1}$.

The main problem is the verification of (a). We will start with it.

For every $i = 1, 2, \ldots, k$ we define:

$$\chi_{\max_i} = \max_{1 \neq g \in G} |\chi_i(g)|.$$

The proof of the next lemma is similar to the proofs of Lemmas 1 and 2.

LEMMA 5. *Let C be a conjugacy class of G, $g \in C$ and let e be a positive integer such that:*

$$\sum_{i=2}^{k} \frac{|\chi_i(g)|^e}{\chi_i^{r-2}(1)} \chi_{\max_i}^{r-e} < 1.$$

Then $1 \in C^e D_{e+1} \cdot \cdots \cdot D_r$ *for every* $r - e$ *non-trivial classes* $D_{e+1}, \ldots, D_r$ *of* G.

Let C be a non-trivial conjugacy class of the simple group G. Define $I(C)$ as follows:

$$I(C) = \min\{cn(G) - 1, e - 1\}$$

where e is the least integer satisfying the condition of Lemma 5. $I(C)$ is easy to compute and has the following property: if the class C appears in the product $D_1 \cdot D_2 \cdot \cdots \cdot D_r$ at least $I(C) + 1$ times then $1 \in D_1 \cdot D_2 \cdot \cdots \cdot D_r$.

In the simple groups checked by us, most of the classes (in each group) satisfied $I(C) \leqq 1$. Until now the ordering of the classes in the product $D_1 \cdot D_2 \cdot \cdots \cdot D_r$ was arbitrary. Since this product is commutative, we can arrange the classes in a way that will reduce the amount of calculations. Let ρ be a partition of the number r (i.e. ρ is a finite sequence of natural numbers $\gamma_1, \gamma_2, \ldots, \gamma_e$ such that $\gamma_1 \geqq \gamma_2 \geqq \cdots \geqq \gamma_e$ and $\gamma_1 + \gamma_2 + \cdots + \gamma_e = r$). It is enough to check the set of products $D_1^{\gamma_1} \cdot D_2^{\gamma_2} \cdot \cdots \cdot D_e^{\gamma_e}$ where the D_i's are distinct and the γ_i's are taken from the set of possible partitions of r.

Assume that the partition ρ is fixed. It follows from Lemma 5 that if D_i satisfies $I(D_i) < \gamma_i$ then $1 \in D_1^{\gamma_1} \cdot D_2^{\gamma_2} \cdot \cdots \cdot D_e^{\gamma_e}$. If $\gamma_e \geqq 2$ then we will check all the possible products. We have to examine only the classes for which $I(D_i) \geqq 2$, which are very few. Now consider the case $\gamma_e = 1$. Let χ_i be an irreducible character of G. According to this χ_i we will arrange the non-trivial conjugacy classes of G. The order will be:

$$C_{i,1}, C_{i,2}, \ldots, C_{i,k-1}$$

subject to the condition:

$$|\chi_i(c_{i,1})| \geqq |\chi_i(c_{i,2})| \geqq \cdots \geqq |\chi_i(c_{i,k-1})|$$

where $c_{i,j} \in C_{i,j}$ for $j = 1, 2, \ldots, k-1$.

Define now $\chi_{\max i,j} = |\chi_i(c_{i,j})|$. Since $\gamma_e = 1$ it suffices to show that $1 \in D_1^{\gamma_1} D_2^{\gamma_2} \cdot \cdots \cdot D_{e-1}^{\gamma_{e-1}} C_j$ for every $j = 1, 2, \ldots, k$. The proof of the next lemma is again trivial.

Lemma 6. *Let C be a conjugacy class of G and let $g \in C$. If*

$$\sum_{i=2}^{k} \frac{\chi_{\max i,1}^{\gamma_1} \chi_{\max i,2}^{\gamma_2} \cdots \chi_{\max i,e-1}^{\gamma_{e-1}} |\chi_i(g)|}{\chi_i^{r-2}(1)} < 1$$

then $1 \in D_1^{\gamma_1} D_2^{\gamma_2} \cdots D_{e-1}^{\gamma_{e-1}} C$ *for every set* $\{D_1, D_2, \ldots, D_{e-1}\}$ *of non-trivial conjugacy classes.*

TABLE 1

G	k	$cn(G)$	$ecn(G)$
M11	10	3	4
M12	15	4	5
M22	12	3	4
M23	17	3	4
M24	26	3	4
J1	15	2	3
J2	21	4	5
J3	21	3	4
J4	62	3	4
HS	24	4	5
SUZ	43	4	5
MCL	24	3	4
RU	36	3	4
HE	33	4	5
LY	53	3	4
ON	30	3	4
C1	101	4	5
C2	60	4	5
C3	42	4	5
F22	65	6	7
F23	98	6	7
F24C	108	3	4
TH	48	3	4
HA	54	4	5
M	194	3	4
BM	184	4	5

TABLE 2

G	k	$cn(G)$	$ecn(G)$
PSL(3,8)	72	3	4
PSL(4.3)	29	4	5
PSU(3,8)	28	3	4
PSU(4,3)	20	4	5
PSU(5,2)	47	6	7
PSP(6,2)	30	6	7
PSU(6,2)	46	6	7
O7F2	30	6	7
$D_4(3)$	114	4	6

Lemma 6 turns out to be a very efficient tool.

Denote now by m the number of 1's in the partition ρ, and by m_1 the number of classes for which Lemma 6 was not successful. In many cases $m_1 < m$. If this is the case, then $1 \in D_1^{\gamma_1} \cdot \cdots \cdot D_e^{\gamma_e}$ for every combination of different classes $D_1, \ldots, D_e$. If $m_1 \geqq m$ then we have no choice and we will use Theorem 1 in order to verify that $1 \in D_1^{\gamma_1} D_2^{\gamma_2} \cdot \cdots \cdot D_{e-1}^{\gamma_{e-1}} C$ for every C. Only D_i for which $I(D_i) \geqq \gamma_i$ need to be checked. Moreover, if $\gamma_e = 1$ then we need only to check the classes for which Lemma 6 was not useful. Therefore, we have got a small number of checkings to do.

Our complete method of determining $ecn(G)$ is as follows:

(1) Our first candidate for $ecn(G)$ is $r = cn(G) + 1$ (as mentioned at the end of Section 2).

(2) Using the above method we check if $1 \in D_1 \cdot D_2 \cdot \cdots \cdot D_r$ for every r non-trivial classes. If not, we will increase r by 1 and repeat the process.

(3) After completion of (2), we know that $r \geqq ecn(G)$. The same process will show us that $r - 1$ is not $ecn(G)$. However, if we will not find $r - 1$ classes for which $1 \notin D_1 \cdot D_2 \cdot \cdots \cdot D_{r-1}$ then $ecn(G) \leqq r - 1$, and so on.

IV. Results

The above methods were used in order to calculate the covering numbers of the simple sporadic groups. The character tables were taken from CAS [N], which was kindly supplied to us by the University of Aachen.

The results appear in Table 1.

It can be seen that for every sporadic group we have $ecn(G) = cn(G) + 1$. We used the same method in computing some additional covering numbers of some other simple groups. The results appear in Table 2.

It can be seen that only one group (among those we have checked) does not satisfy $cn(G) + 1 = ecn(G)$. This group is $D_4(3)$ or O8P3 in CAS notations. It satisfies $ecn(G) = 6$, $cn(G) = 4$. It is the only presently known example of such a group.

References

[ACM] Z. Arad, D. Chillag and G. Moran, *Groups with a small covering number*, in *Products of Conjugacy Classes In Groups*, Lecture Notes in Mathematics, Vol. 1112, Springer-Verlag, Berlin, 1985, pp. 222–224.

[AHS] Z. Arad, M. Herzog and J. Stavi, *Powers and products of conjugacy classes in groups*, in *Products of Conjugacy Classes in Groups*, Lecture Notes in Mathematics, Vol. 1112, Springer-Verlag, Berlin, 1985, pp. 6–51.

[D] Y. Dvir, *Covering properties of permutation groups*, in *Products of Conjugacy Classes in Groups*, Lecture Notes in Mathematics, Vol. 1112, Springer-Verlag, Berlin, 1985, pp. 52–196.

[K] S. Karni, *Covering numbers of groups of small order and sporadic groups*, in *Products of Conjugacy Classes in Groups*, Lecture Notes in Mathematics, Vol. Springer-Verlag, Berlin, 1985, pp. 52–196.

[N] J. Neübuser, *Character tables of the sporadic simple groups*, CAS, Aachen, 1983.

[Z] I. Zisser, *The covering numbers of the spordic simple groups and some other simple groups*, M.Sc. thesis, Tel Aviv University, 1986 (in Hebrew).