BULL. AUSTRAL. MATH. SOC. 20F05
VOL. 51 (1995) [495–499]

A NOTE ON GROWTH SEQUENCES OF FINITE SIMPLE GROUPS

AHMAD ERFANIAN AND JAMES WIEGOLD

The aim of this paper is to give a new precise formula for $h(n, A)$, where A is a finite non-abelian simple group, $h(n, A)$ is the maximum number such that $A^{h(n, A)}$ can be generated by n elements, and $n \geqslant 2$. P. Hall gave a formula for $h(n, A)$ in terms of the Möbius function of the subgroup lattice of A; the new formula involves a concept called cospread associated with that of spread as explained in Brenner and Wiegold (1975).

1. INTRODUCTION

For any finitely generated group A, the minimum number of generators of A is denoted by $d(A)$. The growth sequence is the integer sequence $\{d(A^n)\}$, where A^n stands for the nth direct power of A. The growth sequences of finite groups are known with great accuracy in terms of various parameters [**7, 8, 9, 10**], and quite a lot is known in the case of finitely generated infinite groups [**11**].

One of the main theoretical tools in the finite case is a result of P. Hall [**5**], showing that for a finite non-abelian simple group A, and $n \geqslant d(A)$,

$$d(A^k) \leqslant n \Leftrightarrow k \leqslant h(n, A) := \frac{1}{|\mathrm{Aut}\, A|} \sum_{H \leqslant A} \mu(H)\,|H|^n,$$

where μ is the Möbius function of the subgroup lattice of A. Of course, Möbius functions can be hard to calculate, even for quite small groups like the alternating group A_{10}.

The purpose of this note is to give a somewhat different formula for $h(n, A)$, the new ingredient being the concept of cospread, which grew out of a rich correspondence between Brenner and the second author. (See [**1**] for results on spread.)

DEFINITION: Let G be any group and H any subgroup of G. The *cospread* of H in G is

$$cs(H) = |\{g : g \in G \quad \text{and} \quad \langle H, g\rangle = G\}|.$$

Received 4 August 1994

https://doi.org/10.1017/S0004972700014337 Published online by Cambridge University Press

Clearly, $cs(H)$ is sometimes zero, but we believe it to be non-zero for every non-trivial subgroup of a finite simple group A. (Equivalently, A has spread one in the parlance of [1].)

The main result is essentially a systematisation of methods used in previous articles, more particularly [5] and [6].

Theorem 1. *Let A be a finite non-abelian simple group. Then, for every $n \geqslant 0$,*

$$h(n+1, A) = \sum_{(x_1,\dots,x_n)\in\Delta_n} \frac{cs(\langle x_1, \dots, x_n\rangle)}{|C_{\mathrm{Aut}\,A}(x_1, \dots, x_n)|}, \tag{1}$$

where, for each i, Δ_i is any set of representatives of the Aut A*-classes of ordered i-vectors of elements of A.*

One can imagine many variants of this result, for example the following. (We shall omit the proof.)

Theorem 2. *For any finite simple group A and integers m, n with $1 \leqslant m < n$,*

$$h(n, A) = \sum_{(x_1,x_2,\dots,x_m)\in\Delta_m} \frac{cs_{m,n-m}(\langle x_1, \dots, x_m\rangle)}{|C_{\mathrm{Aut}\,A}(x_1, x_2, \dots, x_m)|},$$

where, for any subgroup H,

$$cs_{m,n-m}(H) = |\{(x_1, \dots, x_{n-m}) : x_i \in A \quad \text{and} \quad \langle H, x_1, \dots, x_{n-m}\rangle = A\}|.$$

Some applications of Theorem 1 will be given in Section 3.

2. Proof of Theorem 1

Firstly, we recall [6] that the ordered m-vectors

$$\begin{gathered}(a_{11}, a_{12}, \dots, a_{1m})\\ \vdots\\ (a_{n1}, a_{n2}, \dots, a_{nm})\end{gathered}$$

of elements of A generate A^m if and only if $A = \langle a_{1i}, \dots, a_{ni}\rangle$ for each i and the m column vectors $(a_{1i}, \dots, a_{ni})'$ are inequivalent under the action of Aut A.

Let t denote the number on the right-hand side of (1). We shall display t Aut A-inequivalent generating $(n+1)$-vectors for A, and show that every generating $(n+1)$-vector is equivalent to one of them. This will be enough for our purposes. Suppose that Δ_n consists of n-vectors

$$\begin{bmatrix} x_{11}\\ \vdots\\ x_{1n}\end{bmatrix}, \dots, \begin{bmatrix} x_{r1}\\ \vdots\\ x_{rn}\end{bmatrix},$$

https://doi.org/10.1017/S0004972700014337 Published online by Cambridge University Press

so that $|\Delta_n| = r$. Clearly, every generating $(n+1)$-vector of A is Aut A-equivalent to one of the form

$$\begin{bmatrix} x_{i1} \\ \vdots \\ x_{in} \\ g \end{bmatrix}$$

for suitable $g \in A$ and suitable i; let us denote that vector by $v(i, g)$ for short. Two vectors $v(i, g)$ and $v(j, h)$ are Aut A-equivalent if and only if $i = j$ and there is an α in Aut A with $x_{is}^{\alpha} = x_{is}$ for $s = 1, 2, \ldots, n$ and $g^{\alpha} = h$. Also, for each i, the number of g such that $v(i, g)$ is a generating $(n+1)$-vector is $cs(\langle x_{i1}, \ldots, x_{in}\rangle)$; finally, for fixed i the number of Aut A-inequivalent $v(i, g)$ is

$$\frac{cs(\langle x_{i1}, \ldots, x_{in}\rangle)}{|C_{\mathrm{Aut}\,A}(x_{i1}, \ldots, x_{in})|}.$$

Thus, there are in all $t_1 + \ldots + t_r = t$ inequivalent generating $(n+1)$-vectors of the form $v(i, g)$, and every generating $(n+1)$-vector is equivalent to one of them. This completes the proof of Theorem 1. □

3. Applications

From Theorem 1 we get, for non-abelian simple group A,

$$h(2, A) = \sum_{l=1}^{r} \frac{cs(x_i)}{|C_{\mathrm{Aut}\,A}(x_i)|},$$

where $\{x_1, \ldots, x_r\}$ is a complete set of representatives of the Aut A-classes of elements of A. (In fact this number is $1/(|\mathrm{Aut}\,A|) \sum_{x \in A} cs(x)$, of course; however, the formula obtained here makes calculations easier). For example, for A_5 we have four Aut A_5-classes, represented by 1, $x_2 = (1, 2, 3, 4, 5)$, $x_3 = (1, 2, 3)$, $x_4 = (1, 2)(3, 4)$; and it is easy to check by hand that $cs(x_1) = 0$

$$\begin{aligned} cs(x_2) &= 50, & |C_{\mathrm{Aut}\,A_5}(x_2)| &= 5, \\ cs(x_3) &= 36, & |C_{\mathrm{Aut}\,A_5}(x_3)| &= 6, \\ cs(x_4) &= 24, & |C_{\mathrm{Aut}\,A_5}(x_4)| &= 8 \end{aligned}$$

so that we recover the famous value [5] for $h(2, A_5)$:

$$h(2, A_5) = 50/5 + 36/6 + 24/8 = 19.$$

https://doi.org/10.1017/S0004972700014337 Published online by Cambridge University Press

Hall's method depends on knowing the Möbius functions of the subgroup lattices, a rare phenomenom. Using a computer to check cospreads, we have made the following new evaluations (among others):

$$h(2, A_7) = 916, \qquad h(2, A_8) = 7,448,$$
$$h(2, A_9) = 77,015, \qquad h(2, A_{10}) = 793,827,$$
$$h(2, M_{11}) = 6,478.$$

Finally, it is probable that cospread calculations can be used in conjunction with the classification theorem to show that $h(2, A) \to \infty$ as $|A| \to \infty$ and A runs over finite non-abelian simple groups. Indeed, all that needs confirmation is that every such group has spread one; that is, for every $a \in A \setminus 1$ there exists $b \in A$ such that $A = \langle a, b \rangle$. This is known for projective special linear groups [**1**], alternating groups [**1, 2**], the Mathieu groups M_{11} and M_{12} [**3**] and the Suzuki groups [**4**].

We begin with a simple result.

Lemma. *Let A be a finite 2-generator group, say $\langle a, b \rangle$. Then $cs(a) \geqslant |C_{\mathrm{Aut}\,A}(a)|$.*

Proof: For $\alpha \in C_{\mathrm{Aut}\,A}(a)$ we have $A = \langle a, b \rangle^\alpha = \langle a, b^\alpha \rangle$. On the other hand the b^α with $\alpha \in C_{\mathrm{Aut}\,A}(a)$ are all different; if $b^\alpha = b^\beta$ for $\alpha, \beta \in C_{\mathrm{Aut}\,A}(a)$, then $\alpha\beta^{-1}$ fixes a and b and thus is the identity of A.

Of course, one expects $cs(a)$ to be much larger than $|C_{\mathrm{Aut}\,A}(a)|$ in general. However, the lemma is sufficient to enable us to estabish our final result. □

Theorem 5. *Let $\{A_\alpha\}_{\alpha \in J}$ be an infinite set of finite non-abelian simple groups of spread one. Then $h(2, A_\alpha) \to \infty$ as $|A_\alpha| \to \infty$.*

Proof: This result is a very elementary consequence of the Lemma, Theorem 1 and the fact that the exponent of A_α tends to infinity with $|A_\alpha|$, the last being a consequence of the classification theorem. All we have to note is that $h(2, A) \geqslant r$ for a non-abelian simple group A of spread one (r being the number of Aut A-classes of elements), and that elements of different orders are Aut A-inequivalent. □

References

[1] J.L. Brenner and J. Wiegold, 'Two generator groups I', *Michigan Math. J.* **22** (1975), 53–64.

[2] J.L. Brenner and J. Wiegold, 'Two generator groups II', *Bull. Austral. Math. Soc.* **22** (1980), 113–124.

[3] J.L. Brenner, R.M. Guralnick and James Wiegold, 'Two generator groups III', *Contemp. Math.* **33** (1984), 82–89.

[4] M.J. Evans, 'A note on two-generator groups', *Rocky Mountain J. Math.* **17** (1987), 887–889.

[5] P. Hall, 'The Eulerian functions of a group', *Quart. J. Math. Oxford* **7** (1936), 134–151.

[6] D. Meier and J. Wiegold, 'Growth sequences of finite groups V', *J. Austral. Math. Soc. Ser. A* **31** (1981), 374–375.

[7] J. Wiegold, 'Growth sequences of finite groups', *J. Austral. Math. Soc.* **17** (1974), 133–141.

[8] J. Wiegold, 'Growth sequences of finite groups II', *J. Austral. Math. Soc.* **20** (1975), 225–229.

[9] J. Wiegold, 'Growth sequences of finite groups III', *J. Austral. Math. Soc.* **25** (1978), 142–144.

[10] J. Wiegold, 'Growth sequences of finite groups IV', *J. Austral. Math. Soc.* **29** (1980), 14–16.

[11] James Wiegold and J.S. Wilson, 'Growth sequences of finitely generated groups', *Arch. Math.* **30** (1978), 337–343.

School of Mathematics
University of Wales
College of Cardiff
Senghennydd Road
Cardiff CF2 4YH
Wales
United Kingdom