J. Austral. Math. Soc. (*Series A*) 31 (1981), 374–375

GROWTH SEQUENCES OF FINITE GROUPS V

D. MEIER and JAMES WIEGOLD

(Received 3 November 1980)

Communicated by D. E. Taylor

Abstract

A short and easy proof that the minimum number of generators of the nth direct power of a non-trivial finite group of order s having automorphism group of order a is more than $\log_s n + \log_s a$, $n \geqslant 1$. On the other hand, for non-abelian simple G and large n, $d(G^n)$ is within $1 + \varepsilon$ of $\log_s n + \log_s a$.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 20 D 60.

In 4.4. of Wiegold (1974) there appears the following corollary of results of P. Hall (1936), which was later applied in Wiegold (1980) to the growth sequences of finite groups for which all simple images are two-generator. Let G be a non-abelian simple group of order s with automorphism group of order a. Then for sufficiently large n (whose meaning is made precise in Wiegold (1974) but is not important for us here),

$$(1)\qquad \log_s n + \log_s a - 1 + \theta(n) < d(G^n) \leqslant \log_s n + \log_s a + 1 + \psi(n),$$

where θ, ψ are sequences tending to 0 as $n \to \infty$. Thus for large n, $d(G^n)$ must take one of at most three values near $\log_s n + \log_s a$.

The object of this note is to give a very trivial proof of a strengthened version of the lower estimate for $d(G^n)$, valid for all finite G. Precisely, we show that

$$(2)\qquad \log_s n + \log_s a < d(G^n)$$

for every finite G and all $n \geqslant 1$, where $s = |G|$ and $a = |\mathrm{Aut}\, G|$ as before. It is then clear that, *for non-abelian simple* G, $d(G^n)$ is within $1 + \varepsilon$ of $\log_s n + \log_s a$ for large n. In other words, it is $\log_s n + \log_s a + 1$ in the unlikely event that this is an integer, or it is one of the two smallest integers greater than $\log_s n + \log_s a$ if not. A glance at powers of A_5 shows that both of these latter contingencies

The first author is supported by the Swiss National Science Foundation.

actually arise. Unlike in Wiegold (1980), we are not assuming anything here about $d(G)$; this article should be compared with that one.

Now for the proof of (2). Suppose that $s^r \leqslant an$ for positive integers r, n. What we want to prove is that $d(G^n) > r$ in this case, and to that end we look at any r elements

$$\begin{aligned} x_1 &= (g_{11}, g_{12}, \ldots, g_{1n}) \\ x_2 &= (g_{21}, g_{22}, \ldots, g_{2n}) \\ &\vdots \\ x_r &= (g_{r1}, g_{r2}, \ldots, g_{rn}) \end{aligned}$$

of G^n, written as strings of length n in the usual way. For $x_1, x_2, \ldots, x_r$ to have a chance of generating G^n, we must have $\langle g_{1i}, g_{2i}, \ldots, g_{ri} \rangle = G$ for each $i = 1, 2, \ldots, n$. Suppose that this is so. Say that two generating r-vectors $(u_1, u_2, \ldots, u_r)$ and $(v_1, v_2, \ldots, v_r)$ are in the same Aut G-class if there is an automorphism α of G such that $u_i^\alpha = v_i$, $i = 1, 2, \ldots, r$. (This idea originated with P. Hall (1936).) How many Aut G-classes of generating r-vectors are there? Certainly less than s^r/a, since Aut G permutes the generating r-vectors regularly, there are exactly s^r r-vectors altogether, and at least one is not generating, namely the trivial r-vector. Of course, many other r-vectors are not generating either if G is not of prime order; but this is of no importance here.

Since $s^r \leqslant an$, there must exist i, j, $i \neq j$, such that $(g_{1i}, g_{2i}, \ldots, g_{ri})$ and $(g_{1j}, g_{2j}, \ldots, g_{rj})$ are in the same Aut G-class. Then for a word w, $w(g_{1i}, \ldots, g_{ri}) = 1$ if and only if $w(g_{1j}, \ldots, g_{rj}) = 1$. It is now clear that x_1, $x_2, \ldots, x_r$ do not generate G^n, since they cannot produce an element which is 1 in the 1-th place and not 1 in the j-th place.

P. Hall (1936) gives a lovely exact formula for the number of generating r-vectors, and it is this which gives rise to the upper bound in (1). What is amusing here is that so easily-won a lower bound should actually be practically the correct answer for simple groups.

References

P. Hall (1936), 'The Eulerian functions of a group,' *Quart. J. Math. Oxford Ser.* **7**, 134–151.
James Wiegold (1974), 'Growth sequences of finite groups,' *J. Austral. Math. Soc.* **17**, 133–141.
James Wiegold (1980), 'Growth sequences of finite groups IV,' *J. Austral. Math. Soc. Ser. A* **29**, 14–16.

Mathematics Institute
University of Warwick
Coventry
England

University College
Cardiff
Wales