Abstract

We prove that if $G$ is a transitive permutation group, then $d(G) \log |G|/n^2$ tends to 0 as $n$ tends to $\infty$.

1 Introduction and preliminary results

1.1 Introduction

The purpose of this note is to prove the following:

Theorem 1.1. Let $f(n)$ be the maximum of $d(G) \log |G|$ as $G$ runs over the transitive permutation groups of degree $n$. Then $f(n)/n^2$ tends to 0 as $n$ tends to $\infty$.

The notation $d(G)$ denotes the minimal number of generators for $G$. All logs are to the base 2 unless otherwise stated.

Our strategy for the proof of the theorem will be to bound $d(G) \log |G|$, for a fixed transitive group $G$, in terms of the degrees of a set of primitive components for $G$, and another invariant $bl_W(G)$ of $G$ (we define $bl_W(G)$, and the term primitive components in Section 1.3). The key result in this direction is Lemma 2.3, which we prove in Section 2. Section 1.2 and 1.3 contain required preliminary and elementary results, while Section 3 is reserved for the proof of Theorem 1.1.

1.2 Minimal generator numbers in transitive permutation groups

We begin with a bound on the minimal number of generators for a transitive permutation group of degree $n$. 

*Electronic address: G.M.Tracey@warwick.ac.uk
Theorem 1.2 ([6], Corollary 1.2). Let $G$ be a transitive permutation group of degree $n \geq 2$. Then $d(G) \leq \lfloor c_1n/\sqrt{\log n} \rfloor$, where $c_1 := 0.920584\ldots$.

When $G$ is primitive, the bound for $d(G)$ is much sharper:

Theorem 1.3 ([3], Theorem 1.1). Let $H$ be a subnormal subgroup of a primitive permutation group of degree $r$. Then $d(H) \leq \lfloor \log r \rfloor$, except that $d(H) = 2$ when $r = 3$ and $H \cong S_3$.

In order to prove Theorem 1.1, we will also need to improve the upper bound for $d(G)$ when $G$ is imprimitive. Before stating the results we need, we introduce a definition: for a finite group $R$, and a transitive permutation group $S \leq \text{Sym}(s)$, consider the wreath product $W = R \wr S$. Let $B := R_1 \times R_2 \times \ldots \times R_s$ be the base group of $W$, and let $\pi : W \to \text{Sym}(s)$ be the projection onto the top group. Also, since $N_W(R_i) \cong R_i \times (R \wr \text{Stab}(i))$, we may consider the projection maps $\rho_i : N_W(R_i) \to R_i$. Then say that a subgroup $G$ of $W$ is large if

1. $\pi(G) = S$, and;
2. $\rho_i(N_G(R_i)) = R_i$ for all $i$.

The results we need, both from [6], can now be stated as follows (here, $(t)_p$ denotes the $p$-part of the positive integer $t$):

Lemma 1.4 ([6], Lemma 4.1 part (ii)). Let $G$ be a finite group, $H$ a subgroup of $G$ of index $n \geq 2$, $F$ a field of characteristic $p > 0$, and $V$ a $H$-module of dimension $a$ over $F$. Also, let $T$ be a soluble subgroup of $G$, and let $t_i$, for $1 \leq i \leq m$, denote the lengths of the orbits of $T$ on the set of right cosets of $H$ in $G$. Let $S$ be a submodule of the induced module $V \uparrow^G$. Then $d_G(S) \leq a \sum_{i=1}^m (t_i)_p$.

Note that, for a finite group $R$, $a(R)$ denotes the composition length of $R$.

Proposition 1.5 ([6], Corollary 5.6). Let $R$ be a finite group, let $S$ be a transitive permutation group of degree $s \geq 2$, and let $G$ be a large subgroup in the wreath product $R \wr S$. Then

1. If $2 \leq s \leq 1260$, then $d(G) \leq \left\lfloor \frac{\tilde{c}a(R)s}{\log s} \right\rfloor + d(\pi(G))$, where $\tilde{c} := 2 \times 1.25506/\ln 2 = 3.621337\ldots$;
2. If $s \geq 1261$, then $d(G) \leq \left\lfloor \frac{a(R)b_1 s}{\sqrt{\log s}} \right\rfloor + d(\pi(G))$, where $b_1 := 2/\sqrt{\pi} = 1.2838\ldots$.

In order to use Proposition 1.5 we will also need an upper bound on the composition length of a primitive group, in terms of its degree. The bound we require is provided by the next theorem, which is stated slightly differently from how it is stated in [5].

Theorem 1.6 ([5], Theorem 2.10). Let $R$ be a primitive permutation group of degree $r \geq 2$, and set $c_0 := \log_9 48 + \frac{1}{4} \log_9 24 = 2.24399\ldots$. Then $a(R) \leq (2 + c_0) \log r - (1/3) \log 24$.

Finally, we need the following theorem of Cameron, Solomon and Turull; note that we only give a simplified version of their result here.

Theorem 1.7 ([2], Theorem 1). Let $G$ be a permutation group of degree $n \geq 2$. Then $a(R) \leq \frac{3}{2} n$. 



2
1.3 Orders of transitive permutation groups

We now turn to bounds on the order of a transitive permutation group \( G \), of degree \( n \). First, we define a function \( \text{bl} \) on \( G \): If \( G \) is primitive, set \( R_1 := G \) and \( r_1 := n \). Otherwise, let \( r_1 \geq 2 \) denote the size of a minimal block for \( G \). Then \( G \) is a large subgroup of the wreath product \( R_1 \wr S_1 \), where \( R_1 \) is primitive of degree \( r_1 \), and \( S_1 \) is transitive of degree \( s_1 := n/r_1 \). We can also iterate this process: either \( S_1 \) is primitive, or \( S_1 \) is a large subgroup in a wreath product \( R_2 \wr S_2 \), where \( R_2 \) is primitive of degree \( r_2 \geq 2 \), and \( S_2 \) is transitive of degree \( s_2 := s_1/r_2 \). Continuing in this way, we see that \( G \) is a subgroup in the iterated wreath product \( R_1 \wr R_2 \wr \ldots \wr R_t \), where each \( R_i \) is primitive of degree \( r_i \) say, and \( \prod_i r_i = n \). We shall call \( W = R_1 \wr R_2 \wr \ldots \wr R_t \) a primitive decomposition of \( G \), and the groups \( R_i \) will be called the primitive components of \( G \) associated to \( W \). Furthermore, we will write \( \pi_i \) to denote the projection \( \pi_i : G \leq (R_1 \wr R_2 \wr \ldots \wr R_i)(R_{i+1} \wr \ldots \wr R_t) \rightarrow R_{i+1} \wr \ldots \wr R_t \) (for \( 1 \leq i \leq t - 1 \)).

For each \( i \), set \( d_i := r_i \) if \( R_i \geq \text{Alt}(r_i) \), and \( d_i := 1 \) otherwise. Now set \( d' := \max_i d_i \), and \( d := \max\{d', c_2\} \), where \( c_2 := 2^{\log{95040}} = 2.83489 \ldots \). Finally, we define \( \text{bl}_W(G) := d \).

Before proceeding to the main result of this subsection, we require the following theorem of Maroti:

**Theorem 1.8** ([4], Corollary 1.4). Let \( G \) be a primitive permutation group of degree \( r \), not containing \( \text{Alt}(r) \). Then \( |G| \leq c_2 r^{-1} \), where \( c_2 := 2^{\log{95040}} = 2.83489 \ldots \).

We can now prove the following:

**Proposition 1.9.** Let \( G \) be a transitive permutation group of degree \( n \), let \( W = R_1 \wr \ldots \wr R_t \) be a primitive decomposition of \( G \), where each \( R_i \) is primitive of degree \( r_i \). Also, let \( d := \text{bl}_W(G) \) be as defined prior to Theorem 1.8. Then \( |G| \leq d^n \).

**Proof.** Working by induction on \( n \), the claim follows when \( G \) is primitive, since either \( d = n \); or \( |G| \leq c_2 n \) (by Theorem 1.8). So assume that \( G \) is imprimitive, and let \( r := r_1 \), \( R := R_1 \), \( S := \pi_1(G) \). Then \( S \) is transitive of degree \( s := n/r \) (being a large subgroup of \( R_2 \wr \ldots \wr R_t \)), and \( G \) is a large subgroup of the wreath product \( R \wr S \). Suppose first that \( R \geq \text{Alt}(r) \). Then \( |R| \leq r^{r-1} \leq d'^{-1} \). Also, the inductive hypothesis implies that \( |S| \leq d^s \). Hence, \( |G| \leq d^{(r-1)s} d^s = d^{r s} \), as needed. So assume that \( R \) is not the alternating or symmetric group of degree \( r \). Then Theorem 1.8 implies that \( |R| \leq c_2 r^{-1} \leq d'^{-1} \). The claim now follows, as above, using the inductive hypothesis. \( \square \)

2 Bounding \( d(G) \) in terms of \( n \) and \( \text{bl}_W(G) \)

**Proposition 2.1.** Let \( n \) be a positive integer. Then the alternating group \( \text{Alt}(n) \) contains a soluble transitive subgroup.

**Proof.** If \( n \) is odd, then the group generated by an \( n \)-cycle suffices, so assume that \( n \) is even, and write \( n = 2^k r \), with \( r \) odd. Let \( P \) be a Sylow 2-subgroup of \( \text{Alt}(2^k) \), and let \( x \) be an \( r \)-cycle

3
in \( \text{Alt}(r) \). Then \( P \) is transitive, and the wreath product \( P \wr \langle x \rangle \) (in its imprimitive action) is a soluble transitive subgroup of \( \text{Alt}(n) \).

\( \square \)

**Proposition 2.2.** Let \( H \) be a finite group with a subgroup \( H_1 \) of index \( u \geq 2 \), let \( V \) be a \( H_1 \)-module of dimension \( a \) over a field \( \mathbb{F} \) of characteristic \( p > 0 \), and let \( U \leq \text{Sym}(u) \) be the image of the induced action of \( H \) on the set of right cosets of \( H_1 \). If \( U \in \{ \text{Alt}(u), \text{Sym}(u) \} \), then each submodule of the induced module \( \uparrow^H_{H_1} \) can be generated by \( 2a \) elements.

**Proof.** We claim that \( U \) contains a soluble subgroup \( T \) which has at most two orbits, and each orbit has \( p^2 \)-length. To see this, assume first that \( p = 2 \). Then since \( n \) is either odd, or a sum of two odd numbers, we can take \( T := \langle x_1x_2 \rangle \), where \( x_1 \) is a cycle of odd length, either \( x_2 = 1 \) or \( x_2 \) is a cycle of odd length, and \( n \) is the sum of the orders (i.e. lengths) of \( x_1 \) and \( x_2 \).

So assume that \( p > 2 \), and write \( n = tp + k \), where \( 0 \leq k \leq p - 1 \). If \( k \neq p - 1 \), then take \( T_1 \) to be a soluble transitive subgroup of \( \text{Alt}(tp-1) \), and take \( T_2 \) to be a soluble transitive subgroup of \( \text{Alt}(k+1) \) (the existence of these groups is guaranteed by Proposition 2.1). If \( k = p - 1 \), then take \( T_1 \) to be a soluble transitive subgroup of \( \text{Alt}(tp+1) \), and take \( T_2 \) to be a soluble transitive subgroup of \( \text{Alt}(k-1) \) (note that \( k - 1 > 0 \) since \( p > 2 \)). Finally, taking \( T := T_1 \times T_2 \leq \text{Alt}(n) \) give us what we need, and proves the claim.

The result now follows immediately from Lemma 1.3.

\( \square \)

**Lemma 2.3.** Let \( R \) be a finite group, let \( U \) and \( V \) be permutation groups of degree \( u \) and \( v \) respectively, and let \( S \) be a large subgroup of the wreath product \( U \wr V \). Also, let \( G \) be a large subgroup of the wreath product \( W := R \wr S \). If \( U \in \{ \text{Alt}(u), \text{Sym}(u) \} \), then \( d(G) \leq 2a(R)v + d(S) \).

**Proof.** Clearly we may assume that \( R \) is nontrivial. Let \( B \) denote the base group of \( W \), so that \( G \cong R^w \). Since \( G/G \cap B \cong S \leq U \wr V \), we may choose subgroups \( H_1 \leq H \) of \( G \), containing \( G \cap B \), such that \( H_1/G \cap B \) is a point stabiliser in \( S \), and \( H/G \cap B \) is the stabiliser of a block \( \Delta \) of size \( u \) in \( S \). Hence, \( |G:H_1| = uv \) and \( |G:H| = v \).

Since \( G/G \cap B \cong S \leq U \wr V \) is large, \( H^\Delta \cong U \). Note also that the permutation action of \( S \) corresponds to the action of \( S \) on \( B \) (by permutation of the direct factors in \( B \cong R^w \)); hence, since \( H/G \cap B \) stabilises a block of size \( u \), \( H \) normalises a subgroup \( B_1 \cong R^u \leq B \). In the same way, \( H_1 \) normalises one of the direct factors in \( B \cong R^w \): identify \( R \) with this direct factor.

Next, let \( L \) be a minimal normal subgroup of \( R \), and, viewing \( L \) as a subgroup of \( B \leq R \), let \( K \) be the direct product of the distinct \( G \)-conjugates of \( L \). Also, let \( K_1 := K \cap B_1 \cong L^u \). If \( L \) is nonabelian, then \( G \cap K \) is either trivial or a minimal normal subgroup of \( G \) (see [6] proof of Lemma 5.1]), so \( d(G) \leq 1 + d(G/G \cap K) \leq a(L) + d(G/G \cap K) \).

Assume now that \( L \) is elementary abelian, of order \( p^s \) say. Then \( K_1 \) is a \( H \)-module, generated by the \( H_1 \)-module \( L \), and \( \dim K_1 = u \dim L = |H:H_1| \dim L \). Thus, by [11] Corollary 3, page 56], \( K_1 \) is isomorphic to the \( H \)-module induced from the \( H_1 \)-module \( L \). By a similar argument, \( K \), as a \( G \)-module, is isomorphic to the \( G \)-module induced from the \( H \)-module \( K_1 \). Hence, since each \( H \)-submodule of \( K_1 \) can be generated by \( 2a \) elements by Proposition 2.2 it follows
that each $G$-submodule of $K \cong K_1 \uparrow^G_H$ can be generated by $2|G : H|a = 2\nu a$ elements. Thus, 
\[ d(G) \leq d_G(G \cap K) + d(G/G \cap K) \leq 2\nu a(L) + d(G/G \cap K). \]

We are now ready to prove the lemma by induction on $R$: by the previous two paragraphs, in each of the cases of $L$ being abelian or nonabelian we have, in particular, $d(G) \leq 2\nu a(L) + d(G/G \cap K)$. If $R = L$ then the result follows, and this can serve as the base step for induction. So assume that $R > L$. Note that $G/G \cap K$ is a large subgroup of the wreath product $R/L \wr S$ satisfying the hypothesis of the lemma, so the inductive hypothesis implies that $d(G/G \cap K) \leq 2\nu a(R/L) + d(S)$. The proof is now complete, since $a(R) = a(R/L) + a(L)$. 

3 Proof of Theorem 1.1

We are now ready to prove Theorem 1.1.

**Proof of Theorem 1.1.** Let $G$ be a transitive permutation group of degree $n$, and let $W = R_1 \wr R_2 \wr \ldots \wr R_t$ be a primitive decomposition of $G$, where each $R_i$ is primitive of degree $r_i$ say. Also, let $d = b_1W(G)$. If $G$ is primitive, then since $d(\text{Alt}(n)) \leq d(\text{Sym}(n)) \leq 2$, Theorems 1.3 and 1.5 imply that $f(n)/n^2 \leq 2n \log n/n^2$, which tends to 0 as $n$ tends to $\infty$.

So we may assume that $G$ is imprimitive. Note that if we set $r' = \prod_{j \leq k} r_j$ and $s' = \prod_{j > k} r_j$, for some $1 \leq k \leq t - 1$, then Proposition 1.9 implies that

\[ \log |G| \leq r's' \log d \quad (3.1) \]

Clearly we may also assume that $n \geq 51(> 4c^2)$.

Before proceeding, we fix some notation: let $R = R_1$, $S = \pi_1(G) \leq R_2 \wr \ldots \wr R_t$, $r = r_1$, and $s = n/r$, so that $S$ is transitive of degree $s$. Also, if one of the $R_j$ for $j \geq 2$, say $R_{i}$, is an alternating or symmetric group of degree $d$, then set $\tilde{R} := R_1 \wr R_2 \wr \ldots \wr R_{i-1}$, $\tilde{S} := \pi_{i-1}(G) \leq R_1 \wr \ldots \wr R_{i}$, $\tilde{r} := \prod_{j < i} r_j$, and $\tilde{s} := n/\tilde{r}$. Otherwise, set $\tilde{R} := R$, $\tilde{S} := S$, $\tilde{r} := r$, and $\tilde{s} := s$. Finally, let $C := c_0 + 2$, where $c_0$ is as in Theorem 1.6.

We split the remainder of the proof into two cases: suppose first that either $d = r$ or $d \leq \max \{\log \tilde{r}, \log \tilde{s}\}$. Then, from the definitions of $r$, $s$, $\tilde{r}$ and $\tilde{s}$, we see that either $d = r$, or $d \neq r$ and one of the following holds:

(a) $d \leq \log \tilde{s} \leq \log s$, or;
(b) $\log \tilde{s} < d \leq \log \tilde{r}$. In this case, either $\tilde{r} \leq s$, in which case $d \leq \log s$; or $\tilde{r} > s$, in which case $r > \tilde{s}$. Since either $\tilde{s} > d$ or $d = c_2$ and $s = \tilde{s} = 2$ (recall that $d \neq r$), it follows that $\tilde{r} > s$ implies that $r > d$.

Now, using Proposition 1.5 there exists a constant $b'_1$ such that

\[ d(G) \leq \frac{a(R)b'_1 \tilde{s}}{\sqrt{\log \tilde{s}}} + d(\pi(G)) \]
Combining this with Theorems 1.2 and 1.6 and the inequality at (3.1), we get
\[ \frac{d(G) \log |G|}{n^2} \leq \frac{\left( Cb'_1 \log r + c_1 \right) s r s \log d}{r^{2} s^{2}} \]
\[ = \frac{\left( Cb'_1 \log r + c_1 \right) \log d}{r \sqrt{\log s}} \]

Since either \( d \leq r \) or \( d \leq \log s \) (see (a), (b) and the preceding comment above), this goes to 0 if either \( r \) or \( s \) is increasing, which gives us what we need.

Finally, assume that \( d > \max \{ \log \tilde{r}, \log \tilde{s} \} \), and that \( d \neq r \). Since \( n = \tilde{r} \tilde{s} \) and \( n > 4^{c_2} \), we have \( d > c_2 \), so one of the \( R_j \) for \( j \geq 2 \), must be an alternating or symmetric group of degree \( d \).
Thus, by definition we have \( \tilde{R} := R_1 \wr R_2 \cdots \wr R_{i-1}, \tilde{S} := \pi_{i-1}(G) \leq R_i \cdots \wr R_t \), and \( \tilde{r} := \prod_{j<i} r_j \).
Then, by Lemma 2.3 and Theorems 1.2 and 1.7, we have
\[ d(G) \leq \frac{a(\tilde{R})\tilde{s}}{d} + d(\tilde{S}) \quad \text{(by Lemma 2.3)} \]
\[ \leq \frac{a(\tilde{R})\tilde{s}}{d} + \frac{(2b'_1 + c_1)\tilde{s}}{\sqrt{\log \tilde{s}}} \quad \text{(by Proposition 1.5 and Theorem 1.2)} \]
\[ \leq \frac{3\tilde{r}\tilde{s}}{d} + \frac{(2b'_1 + c_1)\tilde{s}}{\sqrt{\log \tilde{s}}} \quad \text{(by Theorem 1.7)} \]

We make a further comment: the second inequality above follows from Proposition 1.5 since \( a(R_i) \leq 2 \). Combining the last inequality above with the upper bound at (3.1), we have
\[ \frac{d(G) \log |G|}{n^2} \leq \left[ \frac{3\tilde{r}\tilde{s}}{d} + \frac{(2b'_1 + c_1)\tilde{s}}{\sqrt{\log \tilde{s}}} \right] \frac{\tilde{r}s \log d}{r^{2} s^{2}} \]
\[ \leq \frac{3}{\tilde{r}d} \frac{\log d}{\sqrt{\log \tilde{s}}} + \frac{(2b'_1 + c_1) \log d}{\tilde{r} \log \tilde{s}} \]

Since \( d > \max \{ \log \tilde{r}, \log \tilde{s} \} \), \( d \leq \tilde{s} \) and \( n = \tilde{r} \tilde{s} \), the result now follows. \( \square \)

References

[1] Alperin, J.L. Local Representation Theory. Cambridge University Press, Cambridge, 1986.

[2] Cameron, P.J.; Solomon, R.G.; Turull, A. Chains of subgroups in symmetric groups. J. Algebra 127 (1989) 340-352.

[3] Holt, D.F.; Roney-Dougal, C.M. Minimal and random generation of permutation and matrix groups. J. Algebra 387 (2013) 195-223.

[4] Maroti, A. On the orders of primitive groups. J. Algebra 258 (2) (2002) 631-640.

[5] Pyber, L. Asymptotic results for permutation groups. Groups and Computation DIMACS Ser. Discrete Math. Theoret. Computer Sci. 11 (ed. Finkelstein, L. and Kantor, W.M., Amer. Math. Soc., Providence, 1993) 197-219.
[6] Tracey, G.M. Minimal generation of transitive permutation groups. *preprint*, available from http://arxiv.org/abs/1504.07506v2