ASYMPTOTIC RESULTS
FOR TRANSITIVE PERMUTATION GROUPS

A. LUCCHINI, F. MENEGAZZO AND M. MORIGI

1. Introduction

In this paper we give answers to some open questions concerning generation and enumeration of finite transitive permutation groups. In [1], Bryant, Kovács and Robinson proved that there is a number $c'$ such that each soluble transitive permutation group of degree $n \geq 2$ can be generated by $[c'n/\sqrt{\log n}]$ elements, and later A. Lucchini [5] extended this result (with a different constant $c'$) to finite permutation groups containing a soluble transitive subgroup. We are now able to prove this theorem in full generality, and this solves the question of bounding the number of generators of a finite transitive permutation group in terms of its degree. The result obtained is the following.

**Theorem 1.** There exists a constant $c$ such that any transitive permutation group of finite degree $n \geq 2$ can be generated by $[cn/\sqrt{\log n}]$ elements.

Theorem 1 allows us to deal with the problem of enumerating finite transitive permutation groups.

Denote by $f(n)$ the number of subgroups of the symmetric group $\text{Sym}(n)$ of degree $n \geq 2$, and by $f_{\text{trans}}(n)$ the number of its transitive subgroups. The following result bounds $f_{\text{trans}}(n)$ in terms of the degree $n$.

**Theorem 2.** There exists a constant $b$ such that $f_{\text{trans}}(n) \leq 2^{bn^2/\sqrt{\log n}}$.

This result was proved by A. Lucchini [5] in the case of permutation groups of prime power degree, and actually his proof can be adapted in order to prove the general case.

As in [5], thanks to Theorem 2 it is possible to give a positive answer to a conjecture of Pyber [6], which says that $\text{Sym}(n)$ has 'few' transitive subgroups, meaning that $f_{\text{trans}}(n)/f(n)$ tends to 0 as $n$ tends to infinity. Namely, the following is true.

**Theorem 3.** The proportion of subgroups of $\text{Sym}(n)$ which are transitive tends to 0 as $n$ tends to infinity.

**Proof.** By Pyber [6, Theorem 4.2], $f(n) \geq 2^{\frac{1}{6}n^2 + o(1)n^2}$. So, by Theorem 2,

$$\lim_{n \to \infty} \frac{f_{\text{trans}}(n)}{f(n)} \leq \lim_{n \to \infty} \frac{2^{bn^2/\sqrt{\log n}}}{2^{\frac{1}{6}n^2 + o(1)n^2}} = 0.$$
To prove Theorem 1, we use a key lemma concerning induced modules, which might have some interest in its own right. It is the generalization of the following result, due to Bryant, Kovács and Robinson [1, Theorem 1.5]: there is a constant \( b \) such that, given a module of dimension \( a \) for a subgroup of index \( n \geq 2 \) in a finite soluble group, each submodule of the induced module can be generated by \( \lfloor abn/\sqrt{\log n} \rfloor \) elements.

Actually, we can remove the solvability hypothesis from that theorem, and the following result is true.

**Lemma 4.** There is a constant \( b' \) such that if \( H \) is a subgroup of index \( n \geq 2 \) in a finite group \( G \), \( F \) is a field (of arbitrary characteristic), and \( V \) is an \( H \)-module of dimension \( a \) over \( F \), then every submodule of the induced module \( W = V^G \) can be generated by \( \lfloor ab'n/\sqrt{\log n} \rfloor \) elements.

Once the lemma is proved, all three theorems can be deduced by following the proofs of the analogous theorems in [5], making suitable modifications in the arguments. Consequently, as in [5], all our theorems depend on the Classification of Finite Simple Groups.

The bound in Theorem 1 is ‘asymptotically best possible’. In fact [4], for each prime \( p \), there is a constant \( c_p \) such that whenever \( n \) is a power of \( p \), there is a transitive \( p \)-group of degree \( n \) which cannot be generated by \( \lfloor c_p n/\sqrt{\log n} \rfloor \) elements.

The same cannot be said of the bound in Theorem 2. In this case, the lower bound is provided by [6, Proposition 4.3], where it is proved that for each prime \( p \), there exists a constant \( a_p \) such that if \( n \) is a power of \( p \), then \( f_{\text{trans}}(n) \geq 2^{a_p n/\log n} \). So there is still a gap between this number and the upper bound \( 2^{bn/\sqrt{\log n}} \) given by our Theorem 2.

Throughout this paper, ‘log’ means logarithm to the base 2.

2. **Induced modules**

The aim of this section is to prove Lemma 4. We first introduce the following.

**Definition.** For every integer \( n > 0 \), the leading prime power \( \text{lpp} n \) of \( n \) is the greatest prime power which divides \( n \).

For every \( k \), there is only a finite number of positive integers \( n \) such that \( \text{lpp} n \leq k \), so \( \lim_{n \to \infty} \text{lpp} n = \infty \). Moreover, we note that \( \text{lpp} n \geq c' \log n \) for some constant \( c' \) and every positive integer \( n \). Assume that a prime power \( k \) is the leading prime power of some positive integer \( n \). Then \( n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \) with \( k = p_1^{\alpha_1} \). Denote by \( \pi(k) \) the number of primes which are less than or equal to \( k \). Then, by the Prime Number Theorem [3, p. 165], \( \lim_{n \to \infty} (\pi(k) \ln k)/k = 1 \), so that \( k = (k/\ln k) \log k \) is asymptotically a constant multiple of \( \pi(k) \log k \). Now \( n \leq k^{\pi(k)} \) and \( \log n \leq \pi(k) \log k \), therefore there exists some constant \( c' \) such that \( k \geq c' \log n \), as required.

**Proof of Lemma 4.** The result clearly holds in the semisimple case, so we may assume that the characteristic of \( F \) is a prime divisor of \( |G| \). Let \( Q \) be a subgroup of \( G \), and let \( X = \{x_1, \ldots, x_m\} \) be a full set of \((H, Q)\)-double coset representatives of \( G \).
By Mackey’s Theorem [2, Proposition 6.20], we have that

\[ W_Q = (V^+ Q)_Q = \bigoplus_{i=1}^m W_{x_i}, \]

where \( W_{x_i} \) is isomorphic to the induced module \((V \otimes x_i)|^Q_{H^x \cap Q}\). (The action of \( H^x \cap Q \) on \( V \otimes x_i \) is given by

\[ (v \otimes x_i)^{h_i} = v^h \otimes x_i, \]

for each \( h_i \) in \( H^x \cap Q \).) Moreover, if \( n_{x_i} = |Q : H^x \cap Q| \) for \( i = 1, \ldots, m \), then

\[ \dim_F W = n \dim_F V = \sum_{i=1}^m n_{x_i} \dim_F (V \otimes x_i) = \sum_{i=1}^m n_{x_i} \dim_F V, \]

so \( n = \sum_{i=1}^m n_{x_i} \).

We may consider in \( W \), as \( Q \)-module, the following chain of \( Q \)-submodules:

\[ 0 \leq W_{x_1} \leq W_{x_1} \oplus W_{x_2} \leq \cdots \leq W_{x_1} \oplus \cdots \oplus W_{x_m} = W. \]

Let \( A \) be any \( Q \)-submodule of \( W \). Defining \( A_i = A \cap (W_{x_1} \oplus \cdots \oplus W_{x_i}) \), we obtain a chain \( 0 = A_0 \leq A_1 \leq \cdots \leq A_m = A \) of \( Q \)-submodules of \( A \) such that \( A_i/A_{i-1} \) is isomorphic to a \( Q \)-submodule of \( W_{x_i} \), for \( i = 1, \ldots, m \). Therefore, if \( A \) is a \( G \)-submodule of \( W \), then

\[ d_G(A) \leq d_Q(A) \leq \sum_{i=1}^m d_Q(A_i/A_{i-1}). \]

Now let \( p \) be the characteristic of \( F \), and let \( t = |G : H|_p \) be the greatest power of \( p \) dividing \( n \). There are two cases.

(a) \( t = p^\beta \geq \sqrt{\bar{n}} \). Let \( Q \) be a Sylow \( p \)-subgroup of \( G \). As \( |Q| = p^{\alpha + \gamma} \) with \( p^\alpha = |H|_p \), we have \( |H^x \cap Q| \leq p^\gamma \) and thus \( n_x \geq p^\beta \geq \sqrt{\bar{n}} \). It follows that

\[ d_G(A) \leq d_Q(A) \leq \sum_{i=1}^m d_Q(A_i/A_{i-1}) \leq \sum_{i=1}^m \frac{abn_{x_i}}{\log n_{x_i}} \leq \sum_{i=1}^m \frac{abn_{x_i}}{\log \sqrt{n}} = \frac{ab}{\log \sqrt{n}} \frac{\sqrt{abn}}{\sqrt{\log n}}, \]

where we have applied the theorem of Bryant, Kovács and Robinson [1, Theorem 1.5] to the \( Q \)-submodules of \( W_{x_i} \) isomorphic to \( A_i/A_{i-1} \), for \( i = 1, \ldots, m \).

(b) \( u = n/t \geq \sqrt{\bar{n}} \). Let \( q^\delta = \text{lpp } u \), and consider a Sylow \( q \)-subgroup \( Q \) of \( G \). We have \( |Q| = q^{\gamma + \beta} \) with \( q^\gamma = |H|_q \), so \( |H^x \cap Q| \leq q^\gamma \) and \( n_x \geq q^\delta = \text{lpp } u \). As \( q \neq p \), every \( W_{x_i} \) is a semisimple \( FQ \)-module, so \( d_Q(A_i) \leq d_Q(W_{x_i}) \leq \alpha \). Moreover, as \( n = n_{x_1} + \cdots + n_{x_m} \) and \( n_{x_i} \geq \text{lpp } u \), we have \( m \leq n/\text{lpp } u \). It follows that

\[ d_G(A) \leq d_Q(A) \leq \sum_{i=1}^m d_Q(A_i/A_{i-1}) \leq ma \leq \frac{an}{\text{lpp } u} \leq \frac{an}{u \log u} \leq \frac{2an}{c' \log \sqrt{n}} \leq \frac{2an}{c' \log n}. \]

Taking \( b' = \max\{\sqrt{3}b, 2/c'\} \), we have what we wanted.
3. The main theorems

The proofs of the theorems are basically the same as those in [5], so we shall often refer to that paper, in order not to repeat all the steps of the arguments.

Proof of Theorem 1. The proof is as in [5], simply using Lemma 4 in place of Theorem 1.5 of [1]. More precisely, all the results which appear in Section 2 of [5] are left unchanged, with the exception of Lemmas 2.5 and 2.7, where the solvability hypothesis can be removed, and the constant $b$ is substituted by $b'$ (then $c_1$ of Lemma 2.7 is, of course, different, and consequently the same happens for the constant $c$).

Proof of Theorem 2. There are two non-trivial changes to be made: one in Lemma 3.5, and one in the last part of the proof of Theorem 3.1. For the sake of brevity, we shall not repeat all the proofs, but we shall assume that the reader has the paper [5] at hand. The changes to be made affect only the constant considered.

In particular, in Lemma 3.5 we have $\bar{\varepsilon} = 2c + 2$. In fact, if $r = 6$ in case (b), then it is no longer true that all the automorphisms of $\text{Alt}(6)$ are induced by conjugation by a suitable element of $\text{Sym}(6)$. But we can fix $\tau \in \text{Aut}(\text{Alt}(6)) \setminus \text{Sym}(6)$, and changing $G$ with a suitable conjugate in $(\text{Sym}(6))^m \triangleleft \text{Sym}(n)$, we may assume that there exists a imprimitive system $I_1, \ldots, I_l$ for the action of $K$ on the set $\{1, \ldots, s\}$ such that $S = D_1 \times \cdots \times D_l$, where $D_i$ is very near to being a diagonal subgroup. That is, there exists a subset $J_i$ of $I_i$ such that $D_i$ is the subgroup of $\prod_{j \in I_i} A_j$ consisting of all elements $(x_1, \ldots, x_s)$ with $x_z = 1$ if $z \notin I_i$, $x_u = x_v$ for each $u, v \in I_i$, and $x_h = x_t = x_{\tau}$ for each $h, t \in I_i \setminus J_i$ and each $v \in J_i$. So, once $I_1$ is chosen, we have at most $2^{2s}$ choices for $J_1$. It follows that there are at most $2^{2s}$ possibilities for $S$. In the final inequalities we thus have

\[
(r!)^m 2^{2s} \leq (2^{r \log r})^m 2^{2s} \leq 2^{2cm \log r / \sqrt{\log s} + 2s} \leq 2^{2\sqrt{cm \log r / \sqrt{\log s}}} \leq 2^{2(2c+2)m / \sqrt{\log m}},
\]

as required.

We now proceed to analyse the final part of the proof of Theorem 3.1 in [5]. First, we note that we can find a constant $\bar{\eta}$ such that

\[
n h(n) 2^{2c \sqrt{\log n} / \sqrt{\log 2n}} \leq n^{(c - 2) \log n \sqrt{2^{2c \log n}}} \leq 2^{\bar{\eta} n^2 / \sqrt{\log n}},
\]

where $\bar{\varepsilon} = 2c + 2$, as above. Let $\bar{\delta} = 2\bar{\eta}$, and let $\tilde{f}_{\text{trans}}(n)$ (respectively $\tilde{f}_{\text{prim}}(n)$) denote the number, up to permutation isomorphism, of transitive (respectively primitive) permutation groups of degree $n$. The number of proper divisors of $n$ is at most $n - 1$. Among them, choose $s$ such that $\tilde{f}_{\text{trans}}(s)$ is maximum. Then

\[
\sum_{s|n, 1 \leq s < n} \tilde{f}_{\text{trans}}(s) < n \tilde{f}_{\text{trans}}(s).
\]
Now let $m$ be a multiple of $\bar{s}$ such that $n = pm$ with $p$ a prime. To conclude, we compute the following:

\[
g(n) \leq 1 + \sum_{m|n, \ 1 < m} \left( \sum_{r|m, \ 1 < r} \tilde{f}_{\text{prim}}(r) \tilde{f}_{\text{trans}} \left( \frac{m}{r} \right) \right) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq 1 + \sum_{m|n, \ 1 < m} \left( \sum_{r|m, \ 1 < r} \tilde{f}_{\text{prim}}(r) \tilde{f}_{\text{trans}} \left( \frac{m}{r} \right) \right) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq \left( \sum_{r|m, \ 1 < r} \tilde{f}_{\text{prim}}(r) \right) \left( \sum_{s|n, \ 1 < s} \tilde{f}_{\text{trans}}(s) \right) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq h(n) n \tilde{f}_{\text{trans}}(\bar{s}) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq h(n) n g(m) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq h(n) n g(n/p) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq g(n/p) 2^{\tilde{a}_n / \sqrt{\log n}}
\]

\[
\leq 2^{\tilde{a}_n / \sqrt{\log n}} 2^{\tilde{a}_p^2}
\]

\[
= 2^{\tilde{a}_n^2 \left( \frac{\tilde{a}_p^2}{\sqrt{\log n}} + \frac{1}{2} \right)}
\]

\[
\leq 2^{\tilde{a}_n^2 / \sqrt{\log n}}.
\]

References


Lucchini

Dipartimento di Elettronica per l’Automazione
Università di Brescia
Via Branze 25123
Italy

Menegazzo & Morigi

Dipartimento di Matematica Pura ed Applicata
Università di Padova
Via Belzoni n.7 35131
Padova
Italy