International Journal of Statistics and Applied Mathematics 2021; 6(4): 23-24

International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2021; 6(4): 23-24

www.mathsjournal.com
Received: 06-05-2021
Accepted: 09-06-2021

Firoj Ahamad
Research Scholar, Department of Mathematics, J.P. Univ. Chapra, Bihar, India

Dr. Ashok Kumar
Associate Professor, Department of Mathematics, DAV PG College, Siwan, Bihar, India

Corresponding Author:
Firoj Ahamad
Research Scholar, Department of Mathematics, J.P. Univ. Chapra, Bihar, India

Analysis of generating minimally transitive permutation groups

Firoj Ahamad and Dr. Ashok Kumar

Abstract
A transitive permutation group $G \leq S_n$ is called minimally transitive if every proper subgroup of G is intransitive. In this paper, we consider the minimal number of elements d(G) required to generate such a group G, in terms of its degree n. For the prime factorization $n = \prod_{p \text{ prime}} p^{n(p)}$ of n, we will write $\omega(n) := \Sigma_p n(p)$ and $\mu(n) := \max\{n(p) : p \text{ prime}\}$.

Keywords: transitive permutation, minimally transitive, prime factorization

1. Introduction

The question of bounding d(G)in terms of n was first considered by Shepperd and Wiegold in [1]; there, they prove that every minimally transitive group of degree n can be generated by $\omega(n)$ elements. It was then suggested by Pyber [2] to investigate whether or not $\mu(n)+1$ elements would always suffice. A. Lucchini gave a partial answer to this question in [3], proving that: if G is a minimally transitive group of degree n, and $\mu(n)+1$ elements are not sufficient to generate G, then $\omega(n) \geq 2$ and $d(G) \leq [\log_2(\omega(n)-1)+3]$.
We improve the upper bounds (in terms of n) in [3] and [1] on the minimal number of elements required to generate a minimally transitive permutation group of degree n.

Theorem 1.1 Let G be a minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n)+1$.
Our approach follows along the same lines as Lucchini's proof of the main theorem in [3]. Indeed, his methods suffice to prove Theorem 1.1 in the case when a minimal normal subgroup of G is abelian. Thus, our main efforts will be concerned with the case when a minimal normal subgroup of G is a direct product of isomorphic nonabelian simple groups.

2. Crown-based powers

We outline an approach to study the question of finding the minimal number of elements required to generate a finite group, which is due to F. Dalla Volta and A. Lucchini. So let G be a finite group, with $d(G) = d > 2$, and let M be a normal subgroup of G, maximal with the property that $d(G/M) = d$. Then G/M needs more generators than any proper quotient of G/M, and hence, as we shall see below, G/M takes on a very particular structure.
We describe this structure as follows: let L be a finite group, with a unique minimal normal subgroup N. If Nis abelian, then assume further that Nis complemented in L. Now, for a positive integer k, set L_k to be the subgroup of the direct product L^k defined as follows

$$L_k := \{(x_1, x_2, ..., x_k) : x_i \in L, Nx_i = Nx_j \text{ for all } i, j\}$$

Equivalently, $L_k := \text{diag}(L^k)\, N^k$, where $\text{diag}(L^k)$denotes the diagonal subgroup of L^k. The group L_k is called the crown-based power of L of size k.
We can now state the theorem of Dalla Volta and Lucchini.

Theorem 2.1 Let G be a finite group, with $d(G) \geq 3$, which requires more generators than any of its proper quotients. Then there exists a finite group L, with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and a positive integer k≥2, such that $G \cong L_k$

It is clear that, for fixed L, $d(L_k)$increases with k. To use this result, however, we will need a bound on $d(L_k)$, in terms of k. This is provided by the next two theorems. Before giving the statements, we require some additional notation: for a group G and a normal subgroup M of G, let $P_{G,M}$ (d)denote the conditional probability that randomly chosen elements of G generate G, given that their images modulo M generate G/M.

Theorem 2.2 Let L be a finite group with a unique minimal normal subgroup N which is either nonabelian or complemented in L, and let k be a positive integer. Assume also that d(L) ≤d. Then

1. If N is abelian, then $d(L_k) \le \max\{d(L),k+1\}$;
2. If N is nonabelian, then $d(L_k) \le d$ if and only if $k \le P_{L,N}(d)|N|^d/|C_{Aut}N(L/N)|$.

We will also need an estimate for $P_{L,N}(d)$

Theorem 2.3 Let L be a finite group, with a unique minimal normal subgroup N, which is nonabelian, and suppose that d ≥d(L). Then $P_{L,N}(d) \ge 53/90$.

We need some standard notation: for a positive integer m, π(m)denotes the set of prime divisors of m. Our lemma can now be stated as follows.

3. The proof of Theorem 1.1

Before proceeding to the proof of Theorem 1.1, we need three lemmas.

Lemma 3.1 Let G be a transitive subgroup of S_n (n ≥1), let 1≠=M be a normal subgroup of G, and let Ω be the set of M-orbits. Then

1. Either M is transitive, or Ω forms a system of blocks for G. In particular, the size of an M-orbit divides n.
2. |Ω| =|G:AM|, where A is a point stabiliser in G.
3. If G is minimally transitive, then G^{Ω} acts minimally transitively on Ω.

Proof. Part (i) is clear, so we prove (ii): if M is transitive, then AM=G, so |Ω| =1 =|G:AM|. Otherwise, part (i) implies that the size of each M-orbit is |M:M∩A| =|AM:A|, so the number of M-orbits is n/|AM:A| =|G:AM|. Part (ii) follows. Finally, part (iii) is Theorem 3.4 in [4].

Lemma 3.2 Let L be a finite group with a unique minimal normal subgroup N, which is non abelian, and write N≅St, where Sis a non abelian simple group. Then $|C_{Aut(N)}(L/N)| \le t|S|^t|\,Out(S)|$.

Lemma 3.3 Let S be a non abelian finite simple group. Then | Out(S)| ≤|S|1/4.

The preparations are now complete

Proof of Theorem 1.1. Assume that the theorem is false, and let G be a counterexample of minimal degree. Also, let Abe the stabiliser in G of a point α, and let m :=μ(n) +1.

First, we claim that G needs more generators than any proper quotient of G. To this end, let M be a normal subgroup of G, and let K be the kernel of the action of G on the set of M-orbits. Then G/K is minimally transitive of degree s :=|G :AM|, by Lemma 3.1, and hence, since s divides n, the minimality of G implies that there exists elements $x_1, x_2,..., x_m$ in G such that $G = \langle x_1, x_2,..., x_m, K\rangle$. But then $H:= \langle x_1, x_2,..., x_m\rangle$ acts transitively on the set of M-orbits, so HM=G by minimal transitivity of G. Hence d(G/M) ≤m, which proves the claim.

Hence, by Theorem 2.1, $G \neq L_k$, for some k≥2, and some group L with a unique minimal normal subgroup N, which is either non abelian, or complemented in L. We now fix some notation: write $Soc(G)=N_1 \times N_2 \times ... \times N_k$, where each $N_i \cong N \cong S^t$, for some simple group S, and t ≥1, and set $X_i:=N_1 \times N_2 \times ... \times N_i$. We will also write $X_0:=1$, $H_{i+1}=N_{i+1} \cap X_iA$, and we denote by Δ_i the Xi-orbit containing α, for 0 ≤i ≤k. Then $|\Delta_i| =n|X_iA|/|G|$ by Lemma 3.1 part (ii), and hence

$$\frac{|\Delta_{i+1}|}{|\Delta_i|} = \frac{|X_{i+1}A|}{|X_iA|} = \frac{|N_{i+1}X_iA|}{|X_iA|} = |N_{i+1}:H_{i+1}|$$

Furthermore, it is shown in the proof of the main theorem in [3], that $|\Delta_{i+1}|/|\Delta_i| =|N_{i+1}:H_{i+1}|$ is greater than 1 for 0 ≤i ≤k−2, and also for i =k−1 if Nis abelian. Note also that G/ Soc(G)≅L/M is m-generated, by the previous paragraph; thus, L is m-generated [5].

So we now have a list of primes $p_1, p_2,..., p_{k-1}$, with each p_i in Γ, such that the product $\prod_{i=1}^{k-1} p_i$ divides $|\Delta_{k-1}|$. For each prime pin Γ, let $a_{(p)}$ be the number of times that p occurs in this product. Then, since $|\Delta_{k-1}|$ divides n by Lemma 3.1(i), $\prod_{p\in\Gamma} p^a(p)$ divides n. Since |Γ| ≤f(S), and $\Sigma_{p\in\Gamma} a_{(p)}=k-1$, we have $a_{(p)} \ge (k-1)/f(S)$for at least one prime pin Γ. Hence, (k−1)/f(S) ≤μ(n), and it follows that

$$k \le f(S)\mu(n) + 1 \le \frac{53|S|^{t\mu(n)}}{90t\,|Out(S)|} \quad (1)$$

$$\le \frac{53|N|^m}{90|C_{Aut(N)}(L/N)|} \text{ (by Lemma 3.2)} \quad (2)$$

$$\le \frac{P_{L,N}(m)|N|^m}{|C_{Aut(N)}(L/N)|} \text{ (by Theorem 2.3)} \quad (3)$$

The inequality at (1) above follows easily when Sis an alternating group of degree r, since |S| =r!/2, and | Out(S)| ≤4 in this case (also, | Out(S)| ≤ 2 if r≠6). It also follows easily when S is not an alternating group, using Lemma 3.3. Now, by Theorem 2.2 part (ii), the inequality at (3) contradicts our assumption that d(G) >m. This completes the proof.

References

1. Shepperd JAM, Wiegold J. Transitive groups and groups with finite derived groups, Math. Z 2018;81:279-285.
2. Pyber L. Asymptotic results for permutation groups, in: L. Finkelstein WM. Kantor (Eds.), Groups and Computation, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence 2019;11:197-219.
3. Lucchini A. Generating minimally transitive groups, in: A. Pasini (Ed.), Proceedings of the Con-ference on Groups and Geometries, Siena, September 1996, Birkhäuser, Basel 2018, 149-153.
4. Dalla Volta F, Siemons J. On solvable minimally transitive permutation groups, Des. Codes Cryp-togr 2007;44:143-150.
5. Lucchini A, Menegazzo F. Generators for finite groups with a unique minimal normal subgroup, Rend. Semin. Mat. Univ. Padova 2019;98:173-191.