Generating minimally transitive permutation groups

Tracey, Gareth

Citation for published version (Harvard):
Tracey, G 2016, 'Generating minimally transitive permutation groups', *Journal of Algebra*, vol. 460, pp. 380-386.

Generating minimally transitive permutation groups

Gareth M. Tracey*

Mathematics Institute, University of Warwick,
Coventry CV4 7AL, United Kingdom

June 13, 2015

Abstract

We improve the upper bounds (in terms of n) in [9] and [13] on the minimal number of elements required to generate a minimally transitive permutation group of degree n.

1 Introduction

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 a prime factorisation $n = \prod_{p \text{ prime}} p^{n(p)}$ of n, we will write $\omega(n) := \sum_p n(p)$ and $\mu(n) := \max\{n(p) : p \text{ prime}\}$.

The question of bounding $d(G)$ in terms of n was first considered by Shepperd and Wiegold in [13]; there, they prove that every minimally transitive group of degree n can be generated by $\omega(n)$ elements. It was then suggested by Pyber (see [12]) to investigate whether or not $\mu(n)+1$ elements would always suffice. A. Lucchini gave a partial answer to this question in [9], 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 $d(G) \leq \lfloor \log_2(\omega(n)-1)+3 \rfloor$.*

In this note, we offer a complete solution to the problem, proving

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 [9]. 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. The key step in this direction is Lemma 3.1, which we prove in Section 3. We use Section 2 to outline the method of *crown-based powers* due to Lucchini and F. Dalla Volta; this will serve as the basis for our arguments. Finally, we prove Theorem 1.1 in Section 4.

*Electronic address: `G.M.Tracey@warwick.ac.uk`

2 Crown-based powers

In this section, we outline an approach to study the minimal generation of finite groups, 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 N is abelian, then assume further that N is 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

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

Equivalently, $L_k := \mathrm{diag}(L^k)N^k$, where $\mathrm{diag}\,(L^k)$ 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 (**[2], Theorem 1.4**)**.** *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 $k \geq 2$, 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 d randomly chosen elements of G generate G, given that their images modulo M generate G/M.

Theorem 2.2 (**[9], Theorem 2.1 and [2], Theorem 2.7**)**.** *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 $d(L) \leq d$. Then*

(i) If N is abelian, then $d(L_k) \leq \max\{d(L), k+1\}$;

(ii) If N is nonabelian, then $d(L_k) \leq d$ if and only if $k \leq P_{L,N}(d)|N|^d/|C_{\mathrm{Aut}\,(N)}(L/N)|$.

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

Theorem 2.3 (**[4], Theorem 1.1**)**.** *Let L be a finite group, with a unique minimal normal subgroup N, which is nonabelian, and suppose that $d \geq d(L)$. Then $P_{L,N}(d) \geq 53/90$.*

3 Indices of proper subgroups in finite simple groups

Before stating and proving the main result of this section, we need some standard notation: for a positive integer m, $\pi(m)$ denotes the set of prime divisors of m. Our lemma can now be stated as follows.

Lemma 3.1. *Let S be a nonabelian simple group. Then there exists a set of primes $\Gamma = \Gamma(S)$ with the following properties:*

(i) $|\Gamma| \leq f(S)$, where $f(S) := r/2 + 1$ if S is an alternating group of degree r, and $f(S) := 4$ otherwise;

(ii) $\pi(|S : H|)$ intersects Γ nontrivially for every proper subgroup H of S.

Proof. If $S = L_2(p)$, for some prime p, then since every maximal subgroup M of S has index divisible by either p or $p+1$ (see [5], for example), the result is clear. If $S = L_2(8)$, $L_3(3)$, $U_3(3)$ or $Sp_4(8)$, then direct computation using MAGMA (or Tables 8.1 to 8.6 and Table 8.14 in [1]), implies that each maximal subgroup of S has index divisible by at least one of the primes in $\{2, 3\}$, $\{2, 13\}$, $\{3, 7\}$, and $\{2, 3\}$, respectively.

Next, assume that $S = A_r$ is an alternating group of degree r, and let p and q be the two largest primes not exceeding r, where $p > q$. If $r = p$, then we can take $\Gamma := \{r, q\}$, by Theorem 4 of [7]. So assume that $p < r$, and for each k in $p \leq k \leq r - 1$, choose a prime divisor q_k of $\binom{r}{k}$. Then set $\Gamma := \Gamma(A_r) = \{q_p, \ldots, q_{r-1}\} \cup \{p, q\}$. We claim that Γ satisfies (i) and (ii). To see this, note that $|\Gamma| \leq r - p + 2$, which is less than $r/2 + 2$ by Bertrand's postulate. This proves (i). To see that (ii) holds, let H be a proper subgroup of A_r. If p or q does not divide $|H|$ then we are done, so assume that pq divides $|H|$. Then $A_k \trianglelefteq H \leq S_k \times S_{r-k}$, for some k with $p \leq k \leq r - 1$, by Theorem 4 of [7]. Hence, H has index divisible by $\binom{r}{k}$, and (ii) follows.

So assume that S is not one of the simple groups considered in the first two paragraphs above, and let $\Pi = \Pi(S)$ be the set of prime divisors of $|S|$ discussed in Corollary 6 of [7], so that $|\Pi| \leq 3$. If S does not occur in the left hand column of Table 10.7 in [7], then $\Gamma := \Pi$ satisfies the conclusion of the lemma, by Corollary 6 of [7], so assume otherwise.

Then S is one of the simple groups in the left hand column of Table 10.7 in [7]; we need to prove that there exists a set Γ as in the statement of the lemma. If $H < S$ is not one of the exceptions listed in the middle column of Table 10.7, then $|S : H|$ intersects Π non-trivially. Thus, all we need to prove is that there exists a prime p such that, whenever H is one of these exceptional subgroups, then p divides $|S : H|$. Indeed, in this case, $\Gamma := \Pi \cup \{p\}$ gives us what we need.

So let H be one of these subgroups. We consider each of the possibilities from Table 10.7 of [7]:

1. $S = PSp_{2m}(q)$ (m, q even) or $P\Omega_{2m+1}(q)$ (m even, q odd), and $\Omega^-_{2m}(q) \trianglelefteq H$. Then $H \leq N_S(\Omega^-_{2m}(q))$, so $|S : N_S(\Omega^-_{2m}(q))|$ divides $|S : H|$. But $|N_S(\Omega^-_{2m}(q)) : \Omega^-_{2m}(q)| \leq 2$ using Corollary 2.10.4 part (i) and Table 2.1.D of [6] and, for each of the two choices of S, we have $|S : \Omega^-_{2m}(q)| = q^m(q^m - 1)$. Choosing p so that $q = p^f$ now works.

2. $S = P\Omega^+_{2m}(q)$ (m even, q odd), and $\Omega_{2m-1}(q) \trianglelefteq H$. As above, $H \leq N_S(\Omega_{2m-1}(q))$, and we use Corollary 2.10.4 part (i) and Table 2.1.D of [6] to conclude that $|N_S(\Omega_{2m-1}(q)) : \Omega_{2m-1}(q)| \leq 2$. It follows that $\frac{1}{2}q^{m-1}(q^m - 1) = |S : \Omega_{2m-1}(q)|$ divides $2|S : H|$. Since $m \geq 4$, choosing p so that $q = p^f$ again works.

3. $S = PSp_4(q)$ and $PSp_2(q^2) \trianglelefteq H$. Then $H \leq N_S(\Omega_{2m-1}(q))$, and Corollary 2.10.4 part (i) and Table 2.1.D of [6] gives $|N_S(PSp_2(q^2)) : PSp_2(q^2)| \leq 2$. It follows that $q^2(q^2-1) = |S : PSp_2(q^2)|$ divides $2|S : H|$. Again, the prime p satisfying $q = p^f$, for some f, gives us what we need.

4. In each of the remaining cases (see Table 10.7 in [6]), we are given a tuple $(S, Y_1, \ldots, Y_{t(S)})$, where $t(S) \leq 4$, S is one of $L_2(8)$, $L_3(3)$, $L_6(2)$, $U_3(3)$, $U_3(3)$, $U_3(5)$, $U_4(2)$, $U_4(3)$, $U_5(2)$, $U_6(2)$, $PSp_4(7)$, $PSp_4(8)$, $PSp_6(2)$, $P\Omega_8^+(2)$, $G_2(3)$, ${}^2F_4(2)'$, M_{11}, M_{12}, M_{24}, HS, M_cL, Co_2 or Co_3, $Y_i < S$ for each $1 \leq i \leq t(S)$, and H is contained in at least one of the groups Y_i. In each case, we can easily see that there is a prime p, with p dividing $|S : Y_i|$ for each i in $1 \leq i \leq t(S)$.

This completes the proof. □

4 The proof of Theorem 1.1

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

Lemma 4.1. *Let G be a transitive subgroup of S_n $(n \geq 1)$, let $1 \neq M$ be a normal subgroup of G, and let Ω be the set of M-orbits. Then*

(i) Either M is transitive, or Ω forms a system of blocks for G. In particular, the size of an M-orbit divides n.

(ii) $|\Omega| = |G : AM|$, where A is a point stabiliser in G.

(iii) 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 $|\Omega| = 1 = |G : AM|$. Otherwise, part (i) implies that the size of each M-orbit is $|M : M \cap A| = |AM : A|$, so the number of M-orbits is $n/|AM : A| = |G : AM|$. Part (ii) follows. Finally, part (iii) is Theorem 2.4 in [3]. □

Lemma 4.2 (**[11], Proof of Lemma 3**)**.** *Let L be a finite group with a unique minimal normal subgroup N, which is nonabelian, and write $N \cong S^t$, where S is a nonabelian simple group. Then $|C_{\mathrm{Aut}\,(N)}(L/N)| \leq t|S|^t|\,\mathrm{Out}\,(S)|$.*

Lemma 4.3 (**[8], Proposition 4.4**)**.** *Let S be a nonabelian finite simple group. Then $|\,\mathrm{Out}\,(S)| \leq |S|^{1/4}$.*

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 A be the stabiliser in G of a point α, and let $m := \mu(n) + 1$.

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 4.1, and hence, since s divides n, the minimality of G implies that there exists elements $x_1, x_2, \ldots, x_m$ in G such that $G = \langle x_1, x_2, \ldots, x_m, K\rangle$. But then $H := \langle x_1, x_2, \ldots, x_m\rangle$ acts transitively on the set of M-orbits, so $HM = G$ by minimal transitivity of G. Hence $d(G/M) \leq m$, which proves the claim.

Hence, by Theorem 2.1, $G \cong L_k$, for some $k \geq 2$, and some group L with a unique minimal normal subgroup N, which is either nonabelian, or complemented in L. We now fix some notation: write $\mathrm{Soc}\,(G) = N_1 \times N_2 \times \ldots \times N_k$, where each $N_i \cong N \cong S^t$, for some simple group S, and $t \geq 1$, and set $X_i := N_1 \times N_2 \times \ldots \times N_i$. We will also write $X_0 := 1$, $H_{i+1} = N_{i+1} \cap X_i A$, and we denote by Δ_i the X_i-orbit containing α, for $0 \leq i \leq k$. Then $|\Delta_i| = n|X_i A|/|G|$ by Lemma 4.1 part (ii), and hence

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

Furthermore, it is shown in the proof of the main theorem in [9], that $|\Delta_{i+1}|/|\Delta_i| = |N_{i+1} : H_{i+1}|$ is greater than 1 for $0 \leq i \leq k-2$, and also for $i = k-1$ if N is abelian. Note also that $G/\,\mathrm{Soc}\,(G) \cong L/M$ is m-generated, by the previous paragraph; thus, L is m-generated (see [10]).

We now separate the cases of N being abelian or nonabelian. If N is abelian, then $N \cong C_p^t$, for some prime p, so by the previous paragraph, p divides $|N_{i+1} : H_{i+1}| = |\Delta_{i+1}|/|\Delta_i|$ for each $0 \leq i \leq k-1$. Thus, p^k divides $|\Delta_k|$, and hence divides n, by Lemma 4.1 part (i). It follows that $k \leq \mu(n)$, which, by Theorem 2.2 part (i), contradicts our assumption that $d(G) > \mu(n) + 1$.

Thus, N is nonabelian. Hence, by the third paragraph, for each i in $0 \leq i \leq k-2$, N_{i+1} has a direct factor S_{i+1} ($S_{i+1} \cong S$), with $|S_{i+1} : S_{i+1} \cap H_{i+1}| > 1$. Let $\Gamma = \Gamma(S)$ be the set of primes in Lemma 3.1, so that $|\Gamma| \leq f(S)$, where $f(S)$ is as defined in Lemma 3.1. Then Lemma 3.1 implies that for each $0 \leq i \leq k-2$, the index $|S_{i+1} : S_{i+1} \cap H_{i+1}|$, and hence $|\Delta_{i+1}|/|\Delta_i| = |N_{i+1} : H_{i+1}|$, is divisible by some prime p_{i+1} in Γ.

So we now have a list of primes $p_1, p_2, \ldots, p_{k-1}$, with each p_i in Γ, such that the product $\prod_{i=1}^{k-1} p_i$ divides $|\Delta_{k-1}|$. For each prime p in Γ, let $a_{(p)}$ be the number of times that p occurs in this product. Then, since $|\Delta_{k-1}|$ divides n by Lemma 4.1 (i), $\prod_{p\in\Gamma} p^{a_{(p)}}$ divides n. Since $|\Gamma| \leq f(S)$, and $\sum_{p\in\Gamma} a_{(p)} = k-1$, we have $a_{(p)} \geq (k-1)/f(S)$ for at least one prime p in Γ. Hence, $(k-1)/f(S) \leq \mu(n)$, and it follows that

$$k \leq f(S)\mu(n) + 1 \leq \frac{53|S|^{t\mu(n)}}{90t|\,\mathrm{Out}\,(S)|} \tag{4.1}$$

$$\leq \frac{53|N|^m}{90|C_{\mathrm{Aut}\,(N)}(L/N)|} \qquad \text{(by Lemma 4.2)} \tag{4.2}$$

$$\leq \frac{P_{L,N}(m)|N|^m}{|C_{\mathrm{Aut}\,(N)}(L/N)|} \qquad \text{(by Theorem 2.3)} \tag{4.3}$$

The inequality at (4.1) above follows easily when S is an alternating group of degree r, since $|S| = r!/2$, and $|\,\mathrm{Out}(S)| \leq 4$ in this case (also, $|\,\mathrm{Out}(S)| \leq 2$ if $r \neq 6$). It also follows easily when S is not an alternating group, using Lemma 4.3. Now, by Theorem 2.2 part (ii), the inequality at (4.3) contradicts our assumption that $d(G) > m$. This completes the proof. $\square$

Acknowledgments: The author is hugely grateful to his supervisor Professor D.F. Holt for his careful reading of the paper, and to the Engineering and Physical Sciences Research Council for their continued support.

References

[1] Bray, J.N.; Holt, D.F.; Roney-Dougal, C.M. *The maximal subgroups of the low-dimensional finite classical groups.* London Math. Soc., Lecture Note Series 407, Cambridge, 2013.

[2] Dalla Volta, F.; Lucchini, A. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc.* (Series A) **64** (1998) 82-91.

[3] Dalla Volta, F.; Siemons, J. On solvable minimally transitive permutation groups. *Des. Codes Cryptogr.* **44** (2007) 143-150.

[4] Detomi, E.; Lucchini, A. Probabilistic generation of finite groups with a unique minimal normal subgroup. *J. London Math. Soc.* **87(3)** (2013) 689-706.

[5] Dickson, L.E. *Linear groups: With an exposition of the Galois field theory.* Dover Publications Inc., New York, 1958.

[6] Kleidman, P.; Liebeck, M.W. *The subgroup structure of the finite classical groups.* CUP, Cambridge, 1990.

[7] Liebeck, M.W.; Praeger, C.E.; Saxl, J. Transitive subgroups of primitive permutation groups. *J. Algebra* **234** (2000) 291-361.

[8] Liebeck, M.W; Pyber, L.; Shalev, A. On a conjecture of G.E. Wall. *J. Algebra* **317** (2007) 184-197.

[9] Lucchini, A. Generating minimally transitive groups. *Proceedings of the Conference on Groups and Geometries, Siena, September 1996* (ed. A. Pasini, Birkhauser, Basel) (1998) 149-153.

[10] Lucchini, A.; Menegazzo, F. Generators for finite groups with a unique minimal normal subgroup *Rend. Sem. Math. Univ. Padova* **98** (1997) 173-191.

[11] Lucchini, A.; Morigi, M. Recognizing the prime divisors of the index of a proper subgroup. *J. Algebra* **337** (2011) 335-344.

[12] 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.

[13] Shepperd, J.A.M.; Wiegold, J. Transitive groups and groups with finite derived groups. *Math. Z.* **81** (1963) 279-285.