J. Aust. Math. Soc. **103** (2017), 91–103
doi:10.1017/S1446788716000458

ON THE GENERATING GRAPH OF A SIMPLE GROUP

ANDREA LUCCHINI, ATTILA MARÓTI and COLVA M. RONEY-DOUGAL✉

(Received 24 November 2015; accepted 30 April 2016; first published online 26 September 2016)

Communicated by B. Martin

Abstract

The generating graph $\Gamma(H)$ of a finite group H is the graph defined on the elements of H, with an edge between two vertices if and only if they generate H. We show that if H is a sufficiently large simple group with $\Gamma(G) \cong \Gamma(H)$ for a finite group G, then $G \cong H$. We also prove that the generating graph of a symmetric group determines the group.

2010 *Mathematics subject classification*: primary 20D06; secondary 20P05.

Keywords and phrases: generating graph, finite group.

1. Introduction

The *generating graph* $\Gamma(H)$ of a finite group H is a graph whose vertices are the elements of H, where two vertices are adjacent if they generate H. Examples show that little information about H can be deduced from knowledge of $\Gamma(H)$ only, provided that $\Gamma(H)$ contains at least two isolated vertices. On the other hand, it seems that if $\Gamma(H)$ contains at most one isolated vertex then H is very restricted; for example it follows that H/N is cyclic for every nontrivial normal subgroup N of H. A conjecture (about spread) of Breuer *et al.* [3] states that the converse is also true. (There has been recent work on this problem by Guralnick [7] and by Burness and Guest [4].)

The *spread* of a group H is the maximal integer k such that for any k nonidentity elements $x_1, \ldots, x_k \in H$ there exists a $y \in H$ such that $\langle x_i, y\rangle = H$ for all i. Guralnick and Kantor [8] showed that any finite simple group H has spread at least 1. This motivated us to show the following result.

THEOREM 1.1. *If H is a sufficiently large simple group with $\Gamma(G) \cong \Gamma(H)$ for a finite group G, then $G \cong H$.*

The authors were supported by Università di Padova (Progetto di Ricerca di Ateneo: Invariable generation of groups). The second author was also supported by an Alexander von Humboldt Fellowship for Experienced Researchers, by OTKA grants K84233 and K115799, and by the MTA Rényi Lendület Groups and Graphs Research Group.

It was shown in [17] that the spread of the symmetric group S_n is at least 1 for $n \neq 4$.

THEOREM 1.2. *If H is a symmetric group with $\Gamma(G) \cong \Gamma(H)$ for a finite group G, then $G \cong H$.*

It is tempting to ask whether $\Gamma(H)$ determines H, provided that $\Gamma(H)$ contains at most one isolated vertex. In addition to the previous two theorems, we show in Proposition 5.1 that this is true if G is a sufficiently large soluble group. We also show in Theorem 7.4 that the generating graphs of all of the finite simple groups are pairwise distinct. However, distinct groups with the same socle can have quite similar generating graphs. For example, $\mathrm{PGL}_2(9) \ncong \mathrm{M}_{10}$, but $\Gamma(\mathrm{PGL}_2(9))$ and $\Gamma(\mathrm{M}_{10})$ have the same numbers of vertices and edges. They also have the same (second) minimal vertex degrees. However, the maximal vertex degrees differ in the two graphs.

Since the previous question seems likely to be difficult, we observe that it should be easier to approach a weaker question, namely: does $\Gamma(H)$ determine $\mathrm{soc}(H)$ provided that $\Gamma(H)$ contains at most one isolated vertex?

This paper is structured as follows. In Section 2 we justify our concentration on groups with spread at least 1. In Section 3 we present some elementary results concerning such groups, and fix some notation for them. In Section 4 we prove that for any given $n \geq 3$ there are fewer than $(\log_2 n)^2$ nonisomorphic generating graphs on n vertices, of which at most one is isolated. In Section 5 we show that if G is a sufficiently large group with spread at least 1, then $\Gamma(G)$ determines whether or not G is soluble, and if so determines G up to isomorphism. In Section 6 we then show that if H is a sufficiently large simple group, and $\Gamma(G) \cong \Gamma(H)$ for some finite G, then G is also simple. The proof of Theorem 1.1 is then completed in Section 7 by showing that the generating graphs of the finite simple groups are pairwise nonisomorphic. Finally, in Section 8 we prove Theorem 1.2.

2. Generating graphs with at least two isolated vertices

In this work we are interested in the question: what kind of group-theoretic information about H can be deduced from knowledge about $\Gamma(H)$ only? We are especially interested in when, if ever, $\Gamma(H)$ determines H up to isomorphism.

As an immediate observation, $\Gamma(H)$ determines the order of H. Secondly, $\Gamma(H)$ demonstrates whether or not H can be generated by two elements and whether or not H is cyclic. Our third observation is that if $\Gamma(G) \cong \Gamma(H)$ for some p-group H of order n, and $H/\Phi(H)$ is elementary abelian of rank 2 (where $\Phi(H)$ denotes the Frattini subgroup of H), then G is also a p-group of order n and $G/\Phi(G)$ is elementary abelian of rank 2, but can be any such by [1, (23.1)(2) and (23.2)]. In particular, G need not be isomorphic to H.

Thus it will be convenient to assume that our finite group H can be generated by two elements and its Frattini subgroup is trivial. But even these conditions on H appear to be too weak to determine H up to isomorphism.

Indeed, consider the following example. Let C be a cyclic group of order 5 generated by x. Define two actions of C on a vector space $V = \langle a, b \rangle \cong \mathbb{F}_{11}^2$. In the

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

first action x takes a to $3a$ and b to $4b$, and in the second action x takes a to $3a$ and b to $5b$. Then the semidirect product of C with V gives rise to two solvable groups, H_1 and H_2, both of order 605. It is easy to see that $H_1 \ncong H_2$, since in the first case every element of $\langle x \rangle$ has determinant 1 while this is not true in the second case. In both cases an element (c, d) in V is isolated if $cd = 0$ and it has degree 484 otherwise. The elements of order 5 are conjugate to elements in $\langle x \rangle$ and thus have degree 500. From this it can be seen that $\Gamma(H_1) \cong \Gamma(H_2)$.

3. Assumptions and notation

For the rest of the paper let us make the assumption that G is a finite group with $\Gamma(G)$ containing exactly one isolated vertex. In other words, we assume that G has spread at least 1. It is easy to see that G has the property that every proper quotient of G is cyclic.

This happens if G is cyclic or is an elementary abelian p-group of rank 2 for some prime p. For the rest of this section assume that G is different from these groups. Then G contains a unique minimal normal subgroup, which we denote by N.

If N is an elementary abelian p-group for some prime p, then the cyclic group G/N acts irreducibly and faithfully on N, and therefore it lies inside a Singer cycle acting on N. This implies that $|G/N|$ divides $|N| - 1$ and the extension splits. It also follows that there is a unique such group G up to isomorphism.

If N is not solvable, then N is isomorphic to $T_1 \times \cdots \times T_r$ for some positive integer r, where the T_i are isomorphic to a fixed nonabelian simple group T. In this case we shall write $|G/N| = r \cdot m$ for some integer m dividing $|\mathrm{Out}(T)|$.

4. On the number of generating graphs

In this section we show that for any given n there should be very few finite groups G with spread at least 1 and $|G| = n$.

Proposition 4.1. *There are fewer than* $(\log_2 n)^2$ *nonisomorphic generating graphs on* $n \geq 3$ *vertices of which at most one is isolated.*

Proof. It is sufficient to show that the number of groups G of order $n \geq 3$ with spread at least 1 is less than $(\log_2 n)^2$. We use the assumptions and notation of the previous section.

First let G be solvable. Then for every given $n \geq 3$ there are at most two possibilities for G: a cyclic group, and either a certain Frobenius group as described in Section 3 or an elementary abelian group of rank 2.

Let G be nonsolvable of order n. Let $(x_1, \ldots, x_r)s \in \mathrm{Aut}(T) \wr C_r$ be an element of G that projects onto a generator of G/N, where $x_i \in \mathrm{Aut}(T)$ for $1 \leq i \leq r$ and s is an r-cycle. By conjugating by a certain element of $(\mathrm{Aut}(T))^r$, we see that the image of $(x_1, \ldots, x_r)s$ is $(x, 1, \ldots, 1)s$, where x is an element of $\mathrm{Aut}(T)$ whose smallest power contained in T is x^m.

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

Let $m = 1$ or $m = 2$. Since $r < (\log_2 n)/(\log_2 |T|) < (\log_2 n)/5$, there are fewer than $(\log_2 n)/5$ choices for r. By [10, Theorem 6.1], for each r there are at most two choices for T. Finally, by [16, Lemma 2.1], if $m = 2$, then there are at most $(6/7)\log_2 |T| \leq (6/7)\log_2 n$ choices for x (any choice of x projecting to a fixed element of $\mathrm{Out}(T)$ gives rise to the same group G), and one if $m = 1$. Thus there are fewer than $(12/35)(\log_2 n)^2 + (2/5)\log_2 n$ possibilities for G. In fact, we can divide this bound by 2 by using the fact that if there exist two nonisomorphic simple groups of order $|T|$, then $|T| \geq 20\,160$.

Now let $m \geq 3$. Since $r \cdot m \leq (6/7) r \log_2 |T| \leq (6/7)\log_2 n$, there are fewer than $(6/7)\log_2 n$ choices for $r \cdot m$. By [10, Theorem 6.1], for each such choice of $r \cdot m$ there are at most two possibilities for T and r. Since $m \geq 3$, there are fewer than $(6/14)\log_2 n$ possibilities for x. Thus there are fewer than $(36/49)(\log_2 n)^2$ possibilities for G.

In total, for a given n, there are fewer than

$$2 + (6/35)(\log_2 n)^2 + (1/5)\log_2 n + (36/49)(\log_2 n)^2$$

possibilities for G. For $n \geq 64$ this is less than $(\log_2 n)^2$. Otherwise, if $n \leq 63$, there are at most three possibilities for G, which gives the result, unless $n = 3$, when there is just one group G. □

5. Determining solvability

In this section we show that if G is sufficiently large, then $\Gamma(G)$ determines whether or not G is solvable. Furthermore, if G is solvable, then G is determined up to isomorphism.

This is clear if G is cyclic or an elementary abelian p-group of rank 2 for some prime p. So let us exclude these cases. Also, the fact that once G is known to be solvable, G can be determined up to isomorphism follows from Section 3.

Let $n > 1$ be a natural number. The *contribution* of a prime p to n is the highest power of p dividing n. The *dominant prime* $p = p(n)$ in n is that prime whose contribution $Q = Q(n)$ to n is maximal. The *logarithmic proportion* $\lambda(n)$ of n is $\log_2 Q / \log_2 n$, where Q is the contribution to n of the dominant prime p.

Proposition 5.1. *Let Γ be a simple graph on n vertices, exactly one of which is isolated. Let G be a finite group with $\Gamma(G) \cong \Gamma$. Suppose that n is sufficiently large. Then G is solvable if and only if $\lambda(n) > 1/2$. In that case, n determines G up to isomorphism.*

Proof. The claims that if G is noncyclic and solvable, then $\lambda(|G|) > 1/2$, and that in this case n determines G, follow from Section 3.

For the converse, suppose that G is not solvable. Recall the notation of Section 3. We must show that if n is sufficiently large, then $\lambda(n) \leq 1/2$.

We clearly have

$$\lambda(n) < \lambda(|T|) + \frac{\log_2 m + \log_2 r}{r \log_2 |T|}.$$

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

First suppose that T is a sporadic group, an alternating group, or the Tits group. Then $m \leq 4$ and, since n goes to infinity, r or $|T|$ goes to infinity. In each case we see that

$$\frac{\log_2 m + \log_2 r}{r \log_2 |T|} < 0.01,$$

provided that n is large enough.

From [10], we see that $\lambda(|T|) < 0.49$ if T is not a classical group and $\lambda(|T|) < 1/2 - 1/(c_1 \cdot \ell)$ if T is a classical group, where $c_1 > 2$ is some absolute constant and ℓ is the Lie rank of T.

So let T be a finite simple group of Lie type of Lie rank ℓ defined over a field of size q. Write q in the form p^f, where p is a prime and f is an integer.

Suppose first that ℓ is bounded (from above) by some fixed constant. Then there exists a universal constant c_2 such that $m \leq |\mathrm{Out}(T)| \leq c_2 \cdot f$ (see [11, pages 170–171]). Since n goes to infinity, $|T|$ or r goes to infinity. In any case $(\log_2 r)/(r \log_2 |T|)$ goes to 0. But $\log_2(c_2 f)/(r \log_2 |T|)$ also goes to 0. Thus $\lambda(n) < 1/2$ for sufficiently large n.

Thus we may assume that T is a classical group and that ℓ goes to infinity. Then $\log_2 |T| > c_3 + (\ell^2/2) \log_2 q$ for some absolute constant c_3. Also, $m \leq |\mathrm{Out}(T)| \leq c_4 \cdot \ell \cdot f$ for some absolute constant c_4. Thus

$$\frac{\log_2 m + \log_2 r}{r \log_2 |T|} \leq \frac{\log_2 c_4 + \log_2 \ell + \log_2 f + \log_2 r}{r c_3 + r(\ell^2/2) \log_2 q} = O(\ell^{-3/2}).$$

This finishes the proof of the proposition. □

6. Determining simplicity

For a finite group X, let $P(X)$ denote the probability that two random elements from X generate X, and let $m(X)$ denote the minimal index of a proper subgroup in X.

Proposition 6.1. *Let H be a sufficiently large simple group. Suppose that $\Gamma(G) \cong \Gamma(H)$ for some finite group G. Then G is simple.*

Proof. We may assume that H is nonabelian. From [3], we know that $\Gamma(H)$ has exactly one isolated vertex, and so by Proposition 5.1 the group G is insoluble with all proper quotients cyclic.

Suppose, by way of contradiction, that G is not simple, and recall the definitions of T, m, and r from Section 3. It is elementary to see that $P(G) \leq 1 - 1/t^2$, where t is the smallest prime divisor of $m \cdot r$. On the other hand, it was proved in [13] that $1 - c_5/m(H) \leq P(H)$, where c_5 is some absolute constant. Thus $1 - c_5/m(H) \leq 1 - 1/t^2$, giving us $m(H) \leq c_5 \cdot t^2$. We claim that for sufficiently large H this is not the case.

To prove this, it suffices to show that if c_6 is any constant, then for sufficiently large H we can bound $c_6 \cdot (\log_2 |H|)^2 < m(H)$. Indeed, if $r = 1$, then $t \leq m$, otherwise $t \leq r$. By [16, Lemma 2.1], $m < (6/7) \log_2 |T| \leq (6/7r) \log_2 |H|$, which, if the claim holds, is less than $\sqrt{m(H)/c_5}$ for sufficiently large H. Thus we may assume that $t \leq r$. But then $c_5 \cdot r^2 \leq c_5 \cdot (\log_2 |H|)^2$, which is smaller than $m(H)$ for sufficiently large H.

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

Let H be different from an alternating group. Then

$$\log_2 |H| < (\log_2(m(H)) + 1) \cdot \log_2 m(H)$$

whenever $m(H) > 24$, by [14, Theorem 1.1], since H is simple. But then, for sufficiently large H, we clearly have $c_6 \cdot (\log_2 |H|)^2 < m(H)$.

Assume now that H is an alternating group A_k for $k \geq 5$. We claim that $r = 1$. Assume, by way of contradiction, that $r > 1$. If k is large enough, then there exist two primes q and p with $k/2 < q < p < k$. In particular p and q divide $|G| = |H|$ with multiplicity exactly 1; they cannot divide $|T|$ so they divide $|G/N|$. Let $K = N_G(T_1)$. If q does not divide $|K|$, then q divides r; in particular $|G|_2 \geq |T|_2{}^r \geq |T|_2{}^q \geq 4^q \geq 2^k$. However, $|H|_2 < 2^k$. Hence q (and for the same reason p) divides $|K|$. This implies that $p \cdot q$ divides $|\mathrm{Out}\, T|$. But then $k^2/4 < p \cdot q < |\mathrm{Out}\, T| < (6/7)\log_2 |T| \leq (6/7)\log_2 k!$ (see [16, Lemma 2.1]), which is false if k is large enough.

We remain with the case when G is almost simple, with $\mathrm{soc}(G) = T$. If T is alternating or sporadic, then $|G| = k!/2$ implies that $T = \mathrm{A}_k$, so we may assume that T is of Lie type. In [10], it is noticed (line 5 in the proof of Theorem 5.1) that if $k \neq 9$, then 2 is the dominant prime for A_k; moreover (see [10, Table L.4]) $\lambda(k!/2) < 0.232$ if $n > 40$. On the other hand if T is a group of Lie type, then $\lambda(|T|) \geq 1/3$ (see again [10]). Let p be the dominant prime of $|T|$, P a Sylow p-subgroup of G, and Q a Sylow p-subgroup of T. We have that

$$0.232 > \lambda(|G|) \geq \frac{\log_2 |P|}{\log_2 |G|} \geq \frac{\log_2 |Q|}{\log_2 |T| + \log_2 |\mathrm{Out}\, T|}.$$

When k is large, $|T|$ must be large, so $\log_2 |\mathrm{Out}\, T|$ is negligible. This gives

$$\frac{\log_2 |Q|}{\log_2 |T| + \log_2 |\mathrm{Out}\, T|} \sim \frac{\log_2 |Q|}{\log_2 |T|} = \lambda(|T|) \geq 1/3,$$

which is a contradiction. □

7. Distinguishing the simple groups

In this section we shall show that the generating graphs of the finite simple groups are pairwise nonisomorphic. This will complete the proof of Theorem 1.1. In this section we write P_k for the stabilizer in a simple classical group of a totally singular k-space.

Lemma 7.1. *Let q be odd and $n \geq 12$ be even. Then*

$$P(\mathrm{PSp}_n(q)) > 1 - \left(\frac{q-1}{q^n-1} + \frac{q^{n-8}(q-1)(q^2-1)}{(q^n-1)(q^{n-2}-1)} + \frac{1}{q^{n^2-3n-2}}\right).$$

Proof. We divide the conjugacy classes of maximal subgroups of $\mathrm{PSp}_n(q)$ into three families. The first family contains only P_1, which has index $(q^n-1)/(q-1)$. The second contains all other geometric maximal subgroups, together with any absolutely

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

irreducible representations of A_c or S_c that arise, where $c \in \{n-1, n-2\}$. The third contains all groups in Aschbacher class $\mathcal{S}$ except for A_c and S_c as before.

A short calculation using [2, Table 2.3] shows that the index of P_k in $\mathrm{PSp}_n(q)$ is

$$\frac{(q^n-1)(q^{n-2}-1)\cdots(q^{n-2k+2}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Since $n \geq 12$, this takes its second smallest value when $k=2$. A straightforward calculation shows that the stabilizer of a nondegenerate 2-space has index $q^{n-2}(q^n-1)/(q^2-1)$, which is larger by a factor of around q than the index of P_2, and it is clear that the remaining geometric maximal subgroups are smaller than this. We can bound the order of S_c by $n! < n^n < (q^{\log_3 n})^n < q^{n^2/4}$, so S_c is smaller than every parabolic subgroup. By [15, Theorems 5.1.10 and 5.1.11], we may bound the number of conjugacy classes of groups in this family by $2n + 2\log_2 n + 2\log_2\log_2 q + 4$, which, since $n \geq 12$ and $q \geq 3$, we bound above by q^{n-8}. Thus the probability that two random elements of $\mathrm{PSp}_n(q)$ lie in a group in this family is less than

$$q^{n-8} \cdot \frac{(q^2-1)(q-1)}{(q^n-1)(q^{n-2}-1)}.$$

This leaves only the third family, namely the remaining groups in Class $\mathcal{S}$. By [12], the order of each such group is at most q^{3n}, and by [9] the number of conjugacy classes of such groups is at most $2n^{5.2} + n\log_2\log_2 q$. Now $q^{3n} \leq q^{n^2/4}$ since $n \geq 12$, whilst we have the inequality $(2n^{5.2} + n\log_2\log_2 q) < 2q^n + qn < q^{n+1}$. Thus the probability that two random elements of $\mathrm{PSp}_n(q)$ lie in a group in this family is less than

$$q^{n+1}/((q^n-1)(q^{n-2}-1)\cdots(q^2-1)) < 1/q^{n^2-3n-2}. \qquad \square$$

Lemma 7.2. *Let q be odd. Then*

$$P(\mathrm{PSp}_6(q)) > 1 - \left(\frac{q-1}{q^6-1} + \frac{1}{(q^3+1)(q^2+1)(q+1)} + \frac{q-1}{(q^2+1)(q^6-1)} + \frac{6}{q^8}\right),$$
$$P(\mathrm{PSp}_8(q) > 1 - \left(\frac{q-1}{q^8-1} + \frac{2}{(q^4+1)(q^3+1)(q+1)} + \frac{1}{q^{20}}\right),$$
$$P(\mathrm{PSp}_{10}(q)) > 1 - \left(\frac{q-1}{q^{10}-1} + \frac{2}{(q^5+1)(q^4+1)(q^3+1)(q+1)} + \frac{2}{q^{31}}\right).$$

Proof. We take information about the maximal subgroups of $\mathrm{PSp}_n(q)$ from [2, Tables 8.28, 8.29, 8.48, 8.49, 8.64 and 8.65]. For these n, the two largest maximal subgroups are P_1, of index $(q^n-1)/(q-1)$, and $P_{n/2}$, of index $(q^{n/2}+1)(q^{n/2-1}+1)\cdots(q+1)$.

In $\mathrm{PSp}_6(q)$, the third largest maximal subgroup is P_2, of index $(q^6-1)(q^4-1)/(q^2-1)(q-1)$, which contributes the third bracketed term above. The final reducible maximal subgroup has order less than q^{13}. Each of the remaining geometric maximal subgroups has order at most q^{11}, and there are at most $\log_p q + 5$ of them, so we can bound the sum of the orders of all geometric maximal subgroups other than P_1, P_2, and P_3 by $(4/3)q^{13}$.

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

Now consider the maximal subgroups of $\mathrm{PSp}_6(q)$ in Class $\mathcal{S}$, and assume for now that $q \geq 7$. There are at most two classes of extensions of A_5, each of size at most $|\mathrm{S}_5|$, so the sum of their orders is at most 240. Similarly, we get a contribution of at most $1344 + 2184 + 24\,192 + 1\,209\,600$ from covers of $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(13)$, A_7, $\mathrm{PSU}_3(3)$, and J_2. Thus the total contribution from groups in Class $\mathcal{S}$ is at most $1\,237\,560 + |\mathrm{PSL}_2(q)|$, which is less than q^8 for $q \geq 7$. Describing more precisely the groups occurring when $q = 3, 5$ bounds the total in all cases by q^9. Since $(4/3)q^{13} + q^9 < 2q^{13}$ and $|\mathrm{PSp}_6(q)| > q^{21}/3$, the result for $\mathrm{PSp}_6(q)$ follows.

We now consider $n \in \{8, 10\}$, where the arguments are simpler. We bound the number of geometric subgroups other than P_1 by $12 + \log_p q < 2q^2$, and their order by $|P_{n/2}|$.

For $n = 8$, there are at most eight maximal subgroups in Class $\mathcal{S}$, and at most three when $q \leq 9$, so we bound the number by q. They have order at most q^{11}, and hence index at least $q^5(q^8 - 1)(q^6 - 1)(q^4 - 1)(q^2 - 1) > q^{21}$.

For $n = 10$, there are at most $11 < 2q^2$ conjugacy classes of maximal subgroups in Class $\mathcal{S}$. They have order at most q^{17}, and hence index at least q^{33}. □

Lemma 7.3. *Let q be odd and n be even. Then*

$$P(\mathrm{P}\Omega_{n+1}(q)) < 1 - \left(\frac{q-1}{q^n-1} + \frac{2}{q^{n/2}(q^{n/2}-1)}\right) + \frac{3}{2q^{2n-4}}.$$

Proof. We use [2, Table 2.3], and consider only two of the largest maximal subgroups, namely P_1, which has index $(q^n - 1)/(q - 1)$, and the stabilizer of a minus type n-space, which has index $q^{n/2}(q^{n/2} - 1)/2$. If two elements of $\mathrm{P}\Omega_{n+1}(q)$ lie together in a subgroup of either of these types, then they fail to generate $\mathrm{P}\Omega_{n+1}(q)$: we now bound the sum of the probabilities of lying in the various pairwise intersections. Let β denote the symmetric bilinear form.

There are only two ways in which distinct stabilizers of totally singular points can intersect: either the two points span a nondegenerate 2-space (which must be of +-type), or they span a totally singular 2-space.

By [18, page 141], there are $q^{n-1}(q^n - 1)$ ordered pairs of totally singular vectors (u, v) with $\beta(u, v) = 1$, so there are $(q - 1)q^{n-1}(q^n - 1)$ ordered pairs of totally singular vectors (u, v) with $\beta(u, v) \neq 0$, and hence $q^{n-1}(q^{n-1} - 1)/2(q - 1)$ unordered pairs of totally singular 1-spaces which span a hyperbolic line. The intersection of the stabilizers of these lines has index $q^{n-1}(q^n - 1)/(q - 1)$, so the probability that two random elements of $\mathrm{P}\Omega_{n+1}(q)$ lie in one of these intersections is

$$\frac{q^{n-1}(q^n-1)}{2(q-1)}\left(\frac{(q-1)}{q^{n-1}(q^n-1)}\right)^2 = \frac{(q-1)}{2q^{n-1}(q^n-1)} < \frac{1}{2q^{2n-2}}.$$

Since any two distinct nonzero totally singular vectors span a 1-space, a hyperbolic line, or a totally singular 2-space, given a totally singular vector v the number of vectors u with which it spans a totally singular 2-space is $q^n - (q - 1)q^{n-1} - q = q(q^{n-2} - 1)$. Thus the total number of unordered pairs of totally singular 1-spaces

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

spanning a totally singular 2-space is $q(q^n-1)(q^{n-2}-1)/2(q-1)^2$. The stabilizer of such an ordered pair has index $q(q^n-1)(q^{n-2}-1)/(q-1)^2$, so the probability that two random elements of $\mathrm{P}\Omega_7(q)$ lie in one of these intersections is

$$\frac{q(q^n-1)(q^{n-2}-1)}{2(q-1)^2}\left(\frac{(q-1)^2}{q(q^n-1)(q^{n-2}-1)}\right)^2 = \frac{(q-1)^2}{2q(q^n-1)(q^{n-2}-1)} < \frac{1}{2q^{2n-3}}.$$

The remaining intersections are of a stabilizer of a nondegenerate n-space of minus type with either another such space or a totally singular 1-space. The stabilizer of the n-space is $\Omega_n^-(q).2$, and the minimal index of an ordinary maximal subgroup of $\Omega_n^-(q).2$ is $(q^{n/2}+1)(q^{n/2-1}-1)/(q-1)$. Since the intersection of two stabilizers of n-spaces is contained in an ordinary maximal subgroup of both of them, it has index at least

$$\frac{q^{n/2}(q^{n/2}-1)}{2}\cdot\frac{(q^{n/2}+1)(q^{n/2-1}-1)}{q-1} = \frac{q^{n/2}(q^n-1)(q^{n/2-1}-1)}{2(q-1)}$$

in $\mathrm{P}\Omega_{n+1}(q)$. There are $q^{n/2}(q^{n/2}-1)/2$ minus-type n-spaces, so the contributions of these intersections of this type to the probability is less than

$$\frac{q^n(q^{n/2}-1)^2}{8}\cdot\frac{4(q-1)^2}{q^n(q^n-1)^2(q^{n/2-1}-1)^2} = \frac{(q-1)^2}{2(q^{n/2}+1)^2(q^{n/2-1}-1)^2} < \frac{1}{2q^{2n-4}}.$$

The intersection of the stabilizer of an n-space of minus type and a totally singular 1-space also has index at least $q^{n/2}(q^n-1)(q^{n/2-1}-1)/2(q-1)$ in $\mathrm{P}\Omega_7(q)$. Thus the contribution of the intersections of this type to the probability is at most

$$\frac{(q^n-1)}{q-1}\frac{q^{n/2}(q^{n/2}-1)}{2}\cdot\frac{4(q-1)^2}{q^n(q^n-1)^2(q^{n/2-1}-1)^2} = \frac{2(q-1)}{q^{n/2}(q^{n/2}+1)(q^{n/2-1}-1)^2} < \frac{2}{q^{2n-3}}.$$

Finally, we note that

$$\frac{1}{2q^{2n-2}}+\frac{1}{2q^{2n-3}}+\frac{1}{2q^{2n-4}}+\frac{2}{q^{2n-3}} < \frac{3}{2q^{2n-4}}. \qquad \square$$

THEOREM 7.4. *Let S_1 and S_2 be nonisomorphic finite simple groups. Then $\Gamma(S_1) \ncong \Gamma(S_2)$.*

PROOF. We may assume that S_1 and S_2 have the same order. For A_8 and $\mathrm{PSL}_3(4)$, it follows from [16, Table 1] that $\Gamma(\mathrm{A}_8)$ and $\Gamma(\mathrm{PSL}_3(4))$ have different numbers of edges.

We therefore need to distinguish only between $\mathrm{PSp}_n(q)$ and $\mathrm{P}\Omega_{n+1}(q)$, where q is odd and $n \geq 6$ is even, since all other finite simple groups have distinct orders.

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

Note that for a nonabelian finite simple group S the probability $P(S)$ is precisely the number of edges in $\Gamma(S)$ divided by $|S|^2/2$. Thus $\Gamma(S_1) \cong \Gamma(S_2)$ only if $P(S_1) = P(S_2)$.

For $n \geq 12$, subtracting the upper bound in Lemma 7.3 from the lower bound in Lemma 7.1 yields

$$\frac{2}{q^n - q^{n/2}} - \frac{3}{2q^{2n-4}} - \frac{q^{n-8}}{q^{n-1}q^{n-4}} - \frac{1}{q^{n^2-3n-2}},$$

which is greater than 0 for all q.

For $n = 6$, Lemmas 7.2 and 7.3 yield

$$\frac{2}{q^3(q^3-1)} - \frac{1}{(q+1)(q^2+1)(q^3+1)} - \frac{1}{(q^2+1)(q^5+q^4+\cdots+1)} - \frac{3}{2q^8}$$
$$> \frac{1}{q^3(q^3-1)} - \frac{1}{(q+1)(q^2+1)(q^3+1)} - \frac{1}{(q^2+1)(q^5+q^4+\cdots+1)} > 0.$$

The calculations for $n = 8$ and $n = 10$ are similar but easier. □

This finishes the proof of Theorem 1.1.

8. Symmetric groups

In this section we prove Theorem 1.2.

Let S_n be the symmetric group of degree $n \geq 1$. Using GAP [6], it is easy to check that $\Gamma(\mathrm{S}_n)$ determines S_n for $n \leq 5$. Thus we may assume that $n \geq 6$.

Let G be a finite group with $\Gamma(G) \cong \Gamma(\mathrm{S}_n)$. It is shown in [17] that the spread of the symmetric group S_n is at least 1 for $n \neq 4$; thus $\Gamma(G)$ contains exactly one isolated vertex and so G has the structure described in Section 3, and is not cyclic.

First let G be solvable. By our assumptions on G, and the observations on the structure of G in Section 3, G has an elementary abelian normal subgroup P such that $|G|$ divides $|P|(|P| - 1)$. Since a Sylow subgroup of S_n has size at most 2^{n-1}, we must have $n! < 4^{n-1}$, which forces $n = 6$. But even in this case we arrive at a contradiction. Thus G is not solvable.

Using the notation from Section 3, the group G has order $|T|^r \cdot m \cdot r = n!$.

If $n = 6$, then, by order considerations, G is forced to be almost simple. Using [6], we see that the numbers of generating pairs in S_6 and in G coincide only if $G \cong \mathrm{S}_6$. Thus, from now on, we may assume that $n \geq 7$.

Lemma 8.1. *Let p and q be the largest and second largest prime divisors of $n!$ for $n \geq 7$. If m is divisible by neither p nor q, then $r = 1$.*

Proof. Assume for a contradiction that $r > 1$. By Chebyschev's theorem, we know that $p \geq n/2$ occurs exactly once in the prime factorization of $n!$. By our condition on m, this implies that p divides r. By Chebyschev's theorem again, $q \geq n/4$ occurs at most three times in the prime factorization of $n!$. Since $3 < p \leq r$ and q does not divide m, we see that q also divides r. Thus $r \geq pq \geq n^2/8$, which implies that $r \geq n$. But then the prime 2 occurs more than $n - 1$ times in the prime factorization of $|G|$, which is impossible. □

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

A consequence of the previous lemma is the following result.

LEMMA 8.2. *We may assume that T is a simple group of Lie type with $|T| > 10^6$.*

PROOF. Suppose that T is not a simple group of Lie type. Then m is not divisible by the second largest nor the largest prime factor of $n!$ and so Lemma 8.1 implies that $r = 1$. By simple order considerations, we must have $G \cong S_n$. Thus we may indeed assume that T is a simple group of Lie type.

To show that $|T| > 10^6$ (and thus $n \geq 10$), we may use the list of simple groups T of Lie type of orders less than 10^6 found in [5]. All but one of these groups have outer automorphism groups of order divisible only by the primes 2 or 3. The exception is $T = \mathrm{PSL}_2(32)$. However, even in this case $m = 5$, and we can conclude in all cases that $r = 1$, again by the use of Lemma 8.1.

By considering the orders of the various groups of Lie type T (with $|T| < 10^6$) and the numbers m, together with the condition that $r = 1$, we see that $|G|$ is never of the form $n!$, unless $G \cong \mathrm{S}_n$ or $n = 8$ and $T \cong \mathrm{PSL}_3(4)$. However, [16, Table 1] reveals that the generating graphs of S_8 and G are different when $|G| = 8!$ and $T \cong \mathrm{PSL}_3(4)$. This is because the conditional probabilities $P_{\mathrm{S}_8,\mathrm{A}_8} = (4/3)P(\mathrm{S}_8)$ and $P_{G,T} = (4/3)P(\mathrm{PSL}_3(4))$ can be determined from the generating graphs of S_8 and G, and these are different. □

LEMMA 8.3. *We may assume that $10 \leq n \leq 24$.*

PROOF. By Lemma 8.2, we know that T is a simple group of Lie type with $|T| > 10^6$. This implies that $n \geq 10$. Since $\log_2 m < \log_2 \log_2 |T|$ from [16, Lemma 2.1], we have the inequality $\log_2 m + \log_2 r \leq (1/4)r \log_2 |T|$. This implies that

$$\lambda(|G|) \geq \frac{r \log_2 Q(|T|)}{r \log_2 |T| + \log_2 m + \log_2 r} \geq \frac{r \log_2 Q(|T|)}{(5/4)r \log_2 |T|} \geq \frac{4}{15},$$

since $\log_2 Q(|T|)/\log_2 |T| \geq 1/3$. For $n \geq 25$, the dominant prime of $n!$ is 2 and $\lambda(n!) < 4/15$. Thus $n \leq 24$. □

LEMMA 8.4. *We may assume that G is almost simple.*

PROOF. Suppose that $r > 1$. From $|T| > 10^6$ and $n \leq 24$, we see that $2 \leq r \leq 3$. Furthermore, from $|T| > 10^6$ and $r \geq 2$, we deduce that $n \geq 15$. Now the two largest primes dividing $n!$ both divide m, since they only appear with multiplicity 1 in the prime factorization of $n!$. However, $m < \log_2 |T| < (1/2)\log_2 n!$. This is a contradiction for all n with $15 \leq n \leq 24$. Thus $r = 1$ and G is almost simple, by Lemma 8.3. □

In [5, pages 239–242], there is a list of simple groups S with $|S| < 10^{25}$. By going through this list, we see that the only groups that can appear as T, the socle of G, are $\mathrm{PSL}_2(q)$ with $|T| > 10^6$; $\mathrm{PSL}_3(q)$ with $|T| > 10^{12}$; $\mathrm{PSU}_3(q)$ with $|T| > 10^{12}$; $\mathrm{PSL}_4(q)$ with $|T| > 10^{16}$; $\mathrm{PSU}_4(q)$ with $|T| > 10^{16}$; $\mathrm{PSp}_4(q)$ with $|T| > 10^{16}$; and $\mathrm{G}_2(q)$ with $|T| > 10^{20}$.

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

Lemma 8.5. *We may assume that* $|T| < 10^{16}$ *and* $10 \leq n \leq 19$.

Proof. For otherwise $\log_2 m < 0.11 \log_2 |T|$, by using [16, Lemma 2.1], and $n \geq 19$. By refining the argument in the proof of Lemma 8.3, we get $\lambda(|G|) \geq (1/1.11)(1/3) > 0.3$. But $\lambda(n!) < 0.3$ for $19 \leq n \leq 24$, which is a contradiction. Thus $|T| < 10^{16}$ and so $10 \leq n \leq 19$ by use of [16, Lemma 2.1] once again. □

If $T = \mathrm{PSL}_2(q)$ with $|T| > 10^6$, then $|G|$ differs from $n!$ for $10 \leq n \leq 19$. This can be checked by [6]. Thus $|T| > 10^{12}$ and so $15 \leq n \leq 19$. Finally, if $T = \mathrm{PSL}_3(q)$ with $|T| > 10^{12}$ or if $T = \mathrm{PSU}_3(q)$ with $|T| > 10^{12}$, then $|G|$ differs from $n!$ for $15 \leq n \leq 19$. These two statements were also checked by [6].

This completes the proof of Theorem 1.2.

References

[1] M. Aschbacher, *Finite Group Theory*, Cambridge Studies in Advanced Mathematics, 10 (Cambridge University Press, Cambridge, 1986).

[2] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Mathematical Society Lecture Note Series, 407 (Cambridge University Press, Cambridge, 2013).

[3] T. Breuer, R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups. II', *J. Algebra* **320**(2) (2008), 443–494.

[4] T. C. Burness and S. Guest, 'On the uniform spread of almost simple linear groups', *Nagoya Math. J.* **209** (2013), 35–109.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An ATLAS of Finite Groups* (Clarendon Press, Oxford, 1985), reprinted with corrections 2003.

[6] The GAP Group, GAP – 'Groups, Algorithms, and Programming', Version 4.7.7, 2015. http://www.gap-system.org.

[7] R. M. Guralnick, 'The spread of finite groups', in preparation.

[8] R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups. Special issue in honor of Helmut Wielandt', *J. Algebra* **234**(2) (2000), 743–792.

[9] J. Häsä, 'Growth of cross-characteristic representations of finite quasisimple groups of Lie type', *J. Algebra* **407** (2014), 275–306.

[10] W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague, 'Composition factors from the group ring and Artin's theorem on orders of simple groups', *Proc. Lond. Math. Soc.* (3) **60** (1990), 89–122.

[11] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series, 129 (Cambridge University Press, Cambridge, 1990).

[12] M. W. Liebeck, 'On the orders of maximal subgroups of the finite classical groups', *Proc. Lond. Math. Soc.* (3) **50** (1985), 426–446.

[13] M. W. Liebeck and A. Shalev, 'Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky', *J. Algebra* **184**(1) (1996), 31–57.

[14] A. Maróti, 'On the orders of primitive groups', *J. Algebra* **258**(2) (2002), 631–640.

[15] N. E. Menezes, 'Random generation and chief length of finite groups', PhD Thesis, University of St Andrews, 2013.

[16] N. E. Menezes, M. Quick and C. M. Roney-Dougal, 'The probability of generating a finite simple group', *Israel J. Math.* **198**(1) (2013), 371–392.

[17] S. Piccard, 'Sur les bases du groupe symétrique et du groupe alternant', *Math. Ann.* **116**(1) (1939), 752–767.

[18] D. E. Taylor, *The Geometry of the Classical Groups* (Heldermann, Berlin, 1992).

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press

ANDREA LUCCHINI, Dipartimento di Matematica,
Università degli studi di Padova, Via Trieste 63, 35121 Padova, Italy
e-mail: lucchini@math.unipd.it

ATTILA MARÓTI, MTA Alfréd Rényi Institute of Mathematics,
Reáltanoda utca 13–15, H-1053, Budapest, Hungary
e-mail: maroti.attila@renyi.mta.hu

COLVA M. RONEY-DOUGAL, Mathematical Institute,
University of St Andrews, St Andrews, Fife KY16 9SS, UK
e-mail: colva.roney-dougal@st-andrews.ac.uk

https://doi.org/10.1017/S1446788716000458 Published online by Cambridge University Press