Open access • Journal Article • DOI:10.1007/S11856-013-0034-7

The probability of generating a finite simple group — Source link

Nina Emma Menezes, Martyn Quick, Colva M. Roney-Dougal

Institutions: University of St Andrews

Published on: 01 Jul 2013 - Israel Journal of Mathematics (Springer US)

Topics: Simple group, Finite group, Profinite group, Simple (abstract algebra) and Conditional probability

ISRAEL JOURNAL OF MATHEMATICS **00** (XXXX), 1–21
DOI: 10.1007/s00000000000000000000000

THE PROBABILITY OF GENERATING A FINITE SIMPLE GROUP*

BY

Nina E. Menezes, Martyn Quick & Colva M. Roney-Dougal

School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, U.K.

ABSTRACT

We study the probability of generating a finite simple group, together with its generalisation $P_{G,\operatorname{soc} G}(d)$, the conditional probability of generating an almost simple finite group G by d elements, given that these elements generate $G/\operatorname{soc} G$. We prove that $P_{G,\operatorname{soc} G}(2) \geqslant 53/90$, with equality if and only if G is A_6 or S_6, and establish a similar result for $P_{G,\operatorname{soc} G}(3)$. Positive answers to longstanding questions of Wiegold on direct products, and of Mel′nikov on profinite groups, as well as to a conjecture of Holt and Stather, follow easily from our results.

1. Introduction

Results of Dixon [8], Kantor–Lubotzky [17] and Liebeck–Shalev [27] establish that the probability that two randomly chosen elements of a finite almost simple group G generate a subgroup containing $\operatorname{soc} G$ converges to 1 as $|G| \to \infty$. We obtain explicit lower bounds, and deduce several important consequences.

If G has a normal subgroup N, we write $P_{G,N}(d)$ to denote the conditional probability of generating G by d randomly chosen elements, given that these elements project onto a generating set for G/N. We write $d(G)$ to denote the minimum number of generators of G. Notice that $P_{G,G}(d) = P_G(d)$, where

* The authors would like to thank Andrea Lucchini and Eloisa Detomi for helpful discussions that greatly improved this paper. We would also like the anonymous referee for their insightful suggestions. We acknowledge the support of EPSRC grants EP/H011978/1 and EP/I03582X/1.

G	$P_{G,\mathrm{soc}\,G}(2)$	3 d.p.
A_5, S_5	19/30	0.633
A_6, S_6	53/90	0.588
A_7	229/315	0.726

G	$P_{G,\mathrm{soc}\,G}(2)$	3 d.p.
A_8	133/180	0.738
$L_2(7)$	19/28	0.678
$L_2(11)$	127/165	0.769

G	$\mathrm{PGL}_2(9)$	M_{10}	$A_6.2^2$	S_7	S_8	A_9
$P_{G,S}(2)$	0.866	0.866	0.866	0.817	0.815	0.848
G	S_9	A_{10}	S_{10}	A_{11}	S_{11}	$\mathrm{PGL}_2(7)$
$P_{G,S}(2)$	0.863	0.875	0.875	0.893	0.894	0.821
G	$L_2(8)$	$L_2(8).3$	$\mathrm{PGL}_2(11)$	$L_3(3)$	$L_3(4)$	$\mathrm{P\Sigma L}_3(4)$
$P_{G,S}(2)$	0.845	0.845	0.884	0.863	0.864	0.896
G	$S_4(3)$	$S_4(3).2$	M_{11}	M_{12}		
$P_{G,S}(2)$	0.887	0.887	0.817	0.813		

Table 1. The probability $p = P_{G,\mathrm{soc}\,G}(2)$ for those finite almost simple groups G for which $p \leqslant \frac{9}{10}$. Decimals are lower bounds, correct to 3 d.p.

$P_G(d)$ denotes the probability that d random elements of G generate G. We investigate $P_{G,\mathrm{soc}\,G}(d)$, where G is almost simple, and establish:

THEOREM 1.1: *Let G be a finite almost simple group with socle S such that $d(G/S) \leqslant 2$. Then*

$$P_{G,S}(2) \geqslant \tfrac{53}{90} = 0.58\dot{8},$$

with equality if and only if G is A_6 or S_6. If $P_{G,S}(2) \leqslant \frac{9}{10}$ then G and $P_{G,S}(2)$ are as stated in Table 1.

In [14], Holt and Stather conjectured that $P_S(2) \geqslant P_{A_6}(2) = 53/90$ for all finite simple groups S; Theorem 1.1 proves their conjecture.

It would be reasonably easy to generalise the proof of Theorem 1.1 to bound $P_{G,S}(d)$ for other values of d; we present only the case $d = 3$.

COROLLARY 1.2: *Let G be a finite almost simple group with socle S. Then*

$$P_{G,S}(3) \geqslant \gamma = \frac{139}{150} = 0.92\dot{6},$$

with equality if and only if $S = A_5$.

The *Eulerian function* $\phi_G(d)$ counts the ordered d-tuples of elements of a finite group G that generate G. By definition,

$$P_G(d) = \frac{\phi_G(d)}{|G|^d}.$$

Define $h_G(d)$ to be the largest integer h such that the direct product of h copies of G can be generated by d elements. Philip Hall [12] observed that if S is a non-abelian finite simple group, then

$$h_S(d) = \frac{\phi_S(d)}{|\mathrm{Aut}\, S|}$$

and consequently

$$h_S(d) = \frac{P_S(d)|S|^{d-1}}{|\mathrm{Out}\, S|}.$$

There has been much study, by Wiegold [45] and others, of the growth of $h_G(d)$ for various classes of groups G. Theorem 1.1 and Corollary 1.2 allow us to easily deduce a precise bound for $h_S(d)$, for S non-abelian simple. Throughout, all logarithms are to base 2.

THEOREM 1.3: *Let S be a non-abelian finite simple group. Then*

$$h_S(d) \geqslant \frac{\alpha|S|^{d-1}}{\log|S|}$$

for all $d \geqslant 2$, where $\alpha = \frac{121}{1680}\log 20160 > 1.029$. Moreover, equality holds if and only if $d = 2$ and $S = \mathrm{L}_3(4)$.

Proof. We deal first with $d = 2$. If $P_S(2) > 9/10$ then, by Lemma 2.1, $h_S(2) > \frac{9}{10}|S|/|\mathrm{Out}\, S| \geqslant \frac{21}{20}|S|/\log|S|$. We then verify the inequality for the groups S in Table 1, and use $P_{\mathrm{L}_3(4)}(2) = \frac{121}{140}$. For $d \geqslant 3$, use Corollary 1.2 to observe that $P_S(d) \geqslant P_S(3) \geqslant \gamma$ and hence, by Lemma 2.1, $h_S(d) \geqslant \frac{7}{6}\gamma|S|^{d-1}/\log|S|$. ∎

Theorem 1.3 is asymptotically optimal. Let $S_i = \mathrm{L}_2(2^i)$, then as $i \to \infty$

$$\frac{h_{S_i}(d)\log|S_i|}{|S_i|^{d-1}} = \frac{P_{S_i}(d)\log|S_i|}{|\mathrm{Out}\, S_i|} = P_{S_i}(d)\left(3 + \frac{\log(1-2^{-2i})}{i}\right) \to 3.$$

It is also possible, using additional data on $P_{G,S}(3)$ in [37], to produce the optimal constant for $h_S(3)$ in Theorem 1.3.

Wiegold asks (see [34, Problem 17.116]) for an explicit lower bound for $h_S(2)$ and, in particular, whether $h_S(2) > \sqrt{|S|}$ for every non-abelian finite simple group S. This was recently answered in the affirmative by Maróti–Tamburini [33],

showing that $h_S(2) > 2\sqrt{|S|}$. The Maróti–Tamburini bound follows immediately from Theorem 1.3 (with the exception of $S = \mathrm{A}_5$ where an additional calculation is required). We can now easily compute the largest possible constants for both this and another bound for $h_S(2)$.

COROLLARY 1.4: *Let S be a non-abelian finite simple group. Then*

(i) $h_S(2) \geqslant \beta\sqrt{|S|}$, *where* $\beta = 19/\sqrt{60} > 2.452$. *Moreover, equality holds if and only if* $S = \mathrm{A}_5$.

(ii) $h_S(2) \geqslant |S|^{\lambda}$, *where* $\lambda = \log 53/\log 360 > 0.674$. *Moreover, equality holds if and only if* $S = \mathrm{A}_6$.

Proof. (i) We observe that $|S|^{1/2}/\log|S|$ is an increasing function of $|S|$ so, from Theorem 1.3, $h_S(2) \geqslant \alpha|S|/\log|S| > \beta\sqrt{|S|}$ for $|S| \geqslant 437$. The inequality is verified directly for the remaining groups, namely A_5, A_6 and $\mathrm{L}_2(7)$.

(ii) Similarly, $|S|^{1-\lambda}/\log|S|$ increases with $|S|$, and so $\alpha|S|/\log|S| > |S|^{\lambda}$ for $|S| \geqslant 1125$. The inequality is verified computationally for the remaining groups, namely A_5, A_6, $\mathrm{L}_2(7)$, $\mathrm{L}_2(8)$, $\mathrm{L}_2(11)$ and $\mathrm{L}_2(13)$. ∎

Lucchini in [29] makes the nice observation that proving $P_S(2) \geqslant \frac{1}{2}$ would be sufficient to establish a conjecture of Fireman. In [9], Fireman shows that proving this conjecture would in turn resolve a 1978 problem of Mel′nikov [36]. We complete this work. If S is a finite simple group, then a *poly-S group* is a finite group with all composition factors isomorphic to S and a *pro-S group* is an inverse limit of poly-S groups. We deduce from Theorem 1.1 and [29, Theorem 1.2]:

THEOREM 1.5: *Let S be a non-abelian finite simple group. Then*

(i) *for every positive integer n, there exists a 2-generated poly-S group with a normal subgroup isomorphic to S^n;*

(ii) *every free pro-S group of finite rank has, for every positive integer n, a closed normal subgroup of S-rank n.*

LAYOUT OF PAPER: In Section 2 we establish some preliminary results, including proving a bound on the order of the outer automorphism group of an almost simple group. In the next four sections we prove Theorem 1.1, and along the way we collect additional data to enable us to prove Corollary 1.2. We deal with the families of simple groups starting with the most complicated (for us). Thus Section 3 proves Theorem 1.1 for the exceptional groups, Section 4 for

the classical groups, Section 5 for the alternating groups, and Section 6 for the sporadic groups. In Section 7 we prove Corollary 1.2.

We use ATLAS notation [5] for group names throughout.

2. Preliminary results

Let G be a group with normal subgroup N. Let $g_1, \ldots, g_d \in G$ be such that $G = \langle g_1, \ldots, g_d, N\rangle$. If $d(G) \leqslant d$, then, by Gaschütz [11, Satz 1], there exist elements $n_1, \ldots, n_d \in N$ such that $G = \langle g_1 n_1, \ldots, g_d n_d\rangle$. Define

$$\Omega_{g_1,\ldots,g_d} = \{\, (n_1, \ldots, n_d) \in N^d \mid \langle g_1 n_1, \ldots, g_d n_d\rangle = G \,\}.$$

As observed in the proof of the above result of Gaschütz, the size of $\Omega_{g_1,\ldots,g_d}$ is independent of the choice of $g_1, \ldots, g_d$. Then $P_{G,N}(d) = |\Omega_{g_1,\ldots,g_d}|/|N|^d$.

In the following, let $\mathcal{M}_1$ be the set of maximal subgroups of G that supplement N, let $\mathcal{M}$ be a set of representatives for the G-conjugacy classes of the elements of $\mathcal{M}_1$, and let $\mathcal{L}$ be a set of representatives for the N-conjugacy classes of subgroups of the form $M_1 = M \cap N$ where $M \in \mathcal{M}_1$. Then:

$$\begin{aligned} P_{G,N}(2) &\geqslant 1 - \sum_{M\in\mathcal{M}_1} \frac{1}{|G:M|^2} \geqslant 1 - \sum_{M\in\mathcal{M}} \frac{1}{|G:M|} \\ &= 1 - \sum_{M\in\mathcal{M}} \frac{1}{|N:M\cap N|} \\ &\geqslant 1 - \sum_{M_1\in\mathcal{L}} \frac{1}{|N:M_1|}. \end{aligned} \tag{1}$$

The following lemma is straightforward, but extremely useful.

LEMMA 2.1: *Let S be a non-abelian finite simple group. Then* $|\mathrm{Out}(S)| \leqslant \frac{6}{7}\log|S|$.

Proof. If S is alternating or sporadic then this is easy.

Let S be one of: $\mathrm{L}_n(q)$ with $n \geqslant 6$, $\mathrm{U}_n(q)$ with $n \geqslant 6$, $\mathrm{S}_n(2)$ with $n \geqslant 4$, $\mathrm{O}^\circ_n(q)$ with $n \geqslant 7$, $\mathrm{O}^+_n(q)$ with $n \geqslant 10$, $\mathrm{O}^-_n(q)$ with $n \geqslant 8$, or an exceptional group. Then one may swiftly check in, for example, [5, p *xvi*] that $|\mathrm{Out}(S)| \leqslant \frac{6}{7}\log_p|S|_p$, where $|G|_p$ denotes the p-part of $|G|$.

This leaves only $\mathrm{L}_n(q)$ for $2 \leqslant n \leqslant 5$, $\mathrm{U}_n(q)$ for $3 \leqslant n \leqslant 5$ and $\mathrm{O}^+_8(q)$, where a more detailed examination of the group orders proves the result. ∎

The group which is closest to attaining the bound in Lemma 2.1 is $\mathrm{L}_3(4)$.

3. Exceptional groups

In this section, we find estimates for the conditional probability $P_{G,S}(2)$, where G is almost simple with socle S an exceptional group. For exceptional groups of small rank, our strategy is similar to that of Kantor–Lubotzky [17], namely to use the classification of maximal subgroups of these (almost simple) groups that already exists in the literature. For some of the other exceptional groups, we use a refinement of the method of Liebeck–Shalev [27], but for certain groups more care is needed, and we handle these separately.

Small rank exceptional groups. If G is almost simple with socle $S = X(q)$ where $X \in \{{}^2\mathrm{B}_2, \mathrm{G}_2, {}^2\mathrm{G}_2, {}^3\mathrm{D}_4, {}^2\mathrm{F}_4\}$ and q is an appropriate prime-power, then the maximal subgroups of G are known up to conjugacy (see [41, Theorem 9] and [4], [6, Theorem 2.3] and [4], [19, Theorems A and B], [19, Theorem C], [18], and [31], respectively). From these results, we conclude that if M is a maximal subgroup of G that supplements S, then $M \cap S$ is conjugate in S to either $X(q_0)$, where $q = q_0^r$ for some prime r (and there are consequently at most $\log q$ such conjugacy classes), or to one of a known list of maximal subgroups, as summarised in Table 2. Consequently we deduce from Equation (1) that

$$P_{G,{}^2\mathrm{B}_2(q)}(2) > 1 - \frac{4}{q^2} - \frac{\log q}{q^3} > 0.93 \qquad \text{for } q \geqslant 8,$$

$$P_{G,\mathrm{G}_2(q)}(2) > 1 - \frac{5}{q^5} - \frac{\log q}{q^7} > 0.99 \qquad \text{for even } q \geqslant 8,$$

$$P_{G,\mathrm{G}_2(q)}(2) > 1 - \frac{11}{q^5} - \frac{\log q}{q^7} > 0.95 \qquad \text{for all odd } q,$$

$$P_{G,{}^2\mathrm{G}_2(q)}(2) > 1 - \frac{5}{q^3} - \frac{\log q}{q^4} > 0.99 \qquad \text{for } q \geqslant 27,$$

$$P_{G,{}^3\mathrm{D}_4(q)}(2) > 1 - \frac{10}{q^8} - \frac{\log q}{q^{13}} > 0.96 \qquad \text{for all } q,$$

$$P_{G,{}^2\mathrm{F}_4(q)}(2) > 1 - \frac{11}{q^{10}} - \frac{\log q}{q^{15}} > 0.99 \qquad \text{for } q \geqslant 8.$$

We verify from the Atlas [5] that if S is the Tits group ${}^2\mathrm{F}_4(2)'$, or $\mathrm{G}_2(4)$, then $P_{G,S}(2) > \gamma$, where γ is as in Corollary 1.2.

Group $X(q)$	Index of maximal $X(q_0)$	Number of other maximals	Index of other maximals
${}^2\mathrm{B}_2(q)$	$> q^3$	4	$> q^2$
$\mathrm{G}_2(2^m)$, $m \geqslant 3$	$> q^7$	5	$> q^5$
$\mathrm{G}_2(q)$, q odd	$> q^7$	11	$> q^5$
${}^2\mathrm{G}_2(q)$, $q \geqslant 27$	$> q^4$	5	$> q^3$
${}^3\mathrm{D}_4(q)$	$> q^{13}$	10	$> q^8$
${}^2\mathrm{F}_4(q)$	$> q^{15}$	11	$> q^{10}$

Table 2. Data concerning small rank exceptional groups

LARGE RANK EXCEPTIONAL GROUPS (GENERAL CASE). Let G be almost simple with socle S one of $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$ for some prime-power $q = p^m$. Define $\mathcal{K}$ (the *known* groups) to be a set of S-conjugacy class representatives of maximal subgroups M of G that supplement S such that $M_1 = M \cap S$ satisfies either

(i) M_1 is not almost simple, or
(ii) $\operatorname{soc} M_1$ is a simple group of Lie type over a field of characteristic p and of untwisted Lie rank greater than half the rank of G.

Let $\mathcal{U}$ (the *unknown* groups) be a set of S-conjugacy class representatives of the remaining maximal subgroups of G that supplement S. Note that the groups in $\mathcal{K}$ are known up to S-conjugacy, whilst the groups in $\mathcal{U}$ are only known to within finitely many isomorphism types.

We work with the description from [26, Theorem 8] of the groups in $\mathcal{K}$, where they are divided into eight classes (we merge Classes (I)(d) and (IV), for conciseness). The maximal subgroups are defined up to (at most) inner and diagonal automorphisms, the number of diagonal automorphisms of groups $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$ being at most 1, 3, 3, 2 and 1, respectively. Thus the number of classes of each type of maximal subgroup M can be found in [26, Theorem 8] and the references therein as follows:

(i) parabolic (parametrised by nodes in the Dynkin diagram);
(ii) reductive of maximal rank: [24, Tables 5.1 & 5.2], up to S-conjugacy with listed exceptions;
(iii) $S = E_7(q)$, $p > 2$, and two possible $M \cap S$;
(iv) $S = E_8(q)$, $p > 5$, and two possible $M \cap S$, up to S-conjugacy;

Case	$\mathrm{F}_4(q)$	$\mathrm{E}_6(q)$	${}^2\mathrm{E}_6(q)$	$\mathrm{E}_7(q)$	$\mathrm{E}_8(q)$
(i)	4	6	6	7	8
(ii)	14	9	9	13	29
(iii)	0	0	0	4	0
(iv)	0	0	0	0	2
(v)	2	15	15	16	9
(vi)	$2\log q$	$6\log q$	$3\log q$	$2\log q$	$\log q$
(vii)	1	3	3	0	2

Table 3. Bounds for the number of S-classes of maximal $\mathcal{K}$-subgroups

(v) $M \cap S$ as given in [26, Table 3];
(vi) $M \cap S$ is of the same type as S (possibly twisted);
(vii) $M \cap S$ an exotic local subgroup.

The bounds obtained for each type of conjugacy class are summarised in Table 3, where the first column gives the case in the above description.

The smallest index of a proper subgroup of G is given in [42, 43, 44]. Putting this all together, we obtain the following estimates for all q:

$$\sum_{\substack{S=\mathrm{F}_4(q),\\ M\in\mathcal{K}}} \frac{1}{|G:M|} \leqslant \frac{21+2\log q}{q^{15}} < 0.0008$$

$$\sum_{\substack{S=E_6(q),\\ M\in\mathcal{K}}} \frac{1}{|G:M|} \leqslant \frac{33+6\log q}{q^{16}} < 0.001$$

$$\sum_{\substack{S={}^2\mathrm{E}_6(q),\\ M\in\mathcal{K}}} \frac{1}{|G:M|} \leqslant \frac{33+3\log q}{q^{20}} < 0.001$$

$$\sum_{\substack{S=E_7(q),\\ M\in\mathcal{K}}} \frac{1}{|G:M|} \leqslant \frac{40+2\log q}{q^{27}} < 0.001$$

$$\sum_{\substack{S=E_8(q),\\ M\in\mathcal{K}}} \frac{1}{|G:M|} \leqslant \frac{50+\log q}{q^{57}} < 0.001. \tag{2}$$

We now consider the class $\mathcal{U}$ of maximal subgroups not belonging to $\mathcal{K}$. We shall make use of the following lemma:

LEMMA 3.1: *Let G be an almost simple finite group with socle S. Let $\mathcal{V}$ be a set of representatives for some G-conjugacy classes of maximal subgroups that supplement S such that each $M \in \mathcal{V}$ is almost simple. Define $\mathcal{V}_1 = \{ M \cap S \mid M \in \mathcal{V} \}$. Let k be the maximum value taken by $|\mathrm{Aut}\, T||\mathrm{Out}\, T|$, where $M \in \mathcal{V}$ and $T = \mathrm{soc}\, M$, let m be an upper bound for the orders of subgroups in $\mathcal{V}_1$, and let $i(S)$ be the number of involutions in S. Then*

$$\text{(i)} \quad \sum_{M \in \mathcal{V}} \frac{1}{|G : M|} \leqslant \frac{i(S)k}{|S|} \qquad \text{and} \qquad \text{(ii)} \quad \sum_{M \in \mathcal{V}} \frac{1}{|G : M|} \leqslant \frac{6i(S)m \log m}{7|S|}.$$

Proof. Let $\mathcal{T}$ be the set of socles of the G-conjugates of M for $M \in \mathcal{V}$ and let $\mathcal{W}$ be the set of G-conjugates of such M. Note that $\mathrm{soc}\, M \leqslant M \cap S$, $\mathrm{N}_G(M) = M$ and $|G : M| = |S : M \cap S|$ for all $M \in \mathcal{V}$. Hence

$$\begin{aligned} \sum_{M \in \mathcal{V}} \frac{1}{|G : M|} &= \sum_{M \in \mathcal{W}} \frac{1}{|S : M \cap S|^2} \\ &\leqslant \frac{1}{|S|^2} \sum_{T \in \mathcal{T}} |\mathrm{Aut}\, T|^2 \leqslant \frac{k}{|S|^2} \sum_{T \in \mathcal{T}} |T| \leqslant \frac{i(S)k}{|S|}, \end{aligned}$$

using [27, Lemma 3.1(i)]. Inequality (ii) follows similarly since if T is a socle of the almost simple subgroup $M \in \mathcal{V}$, then $|T| \leqslant |M \cap S| \leqslant m$ and so $|\mathrm{Out}\, T| \leqslant \frac{6}{7} \log m$ by Lemma 2.1. ∎

PROPOSITION 3.2: *Let M be an almost simple maximal subgroup of G with $T = \mathrm{soc}\, M$ either not a Lie type group of characteristic p, or of untwisted Lie rank at most half that of $S = \mathrm{soc}\, G$. In addition, if $S = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ assume $q \neq 2$.*

If $S = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$, then $|M| < 4q^{20} \log q$, $4q^{28} \log q$, $4q^{28} \log q$, $9q^{30} \log q$, $12q^{56} \log q$, respectively.

Proof. For T a group of Lie type in characteristic p, this is immediate from [27, Theorem 1.2].

Theorem 1 of [25] describes which alternating groups, sporadic simple groups and Lie groups of cross-characteristic may exist as subgroups of an exceptional Lie type. We consult [22] to establish that Fi_{22} is not a subgroup of $\mathrm{E}_6(q)$ for $q \leqslant 4$ nor of $\mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$ for any q. The required inequalities can now be established for each remaining group, making use of the assumption that $q \geqslant 3$ when $S = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$. ∎

Finally, the conjugacy classes of involutions in S were determined in [15, 1]. In each case, there are at most five such conjugacy classes and the order of the centraliser for a conjugacy class of maximal size is listed in [27, Table II]. As a consequence, we estimate

$$i(S) \leqslant \begin{cases} 5|S|/|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)| & \text{if } S = \mathrm{F}_4(q) \\ 5(3,q-1)|S|/|\mathrm{SL}_2(q)||\mathrm{SL}_6(q)| & \text{if } S = \mathrm{E}_6(q) \\ 5(3,q+1)|S|/|\mathrm{SL}_2(q)||\mathrm{SU}_6(q)| & \text{if } S = {}^2\mathrm{E}_6(q) \\ 10|S|/|\mathrm{SL}_8(q)| & \text{if } S = \mathrm{E}_7(q) \\ 5|S|/(4,q^2-1)|\mathrm{O}_{16}^+(q)| & \text{if } S = \mathrm{E}_8(q). \end{cases} \tag{3}$$

Hence, Lemma 3.1(ii) enables us to conclude

$$\sum_{\substack{S=\mathrm{F}_4(q) \\ M\in\mathcal{U}}} \frac{1}{|G:M|} \leqslant \frac{120q^{20}(\log q)\log(4q^{20}\log q)}{7|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)|} < 0.0725 \qquad \text{for } q \geqslant 17;$$

$$\sum_{\substack{S=\mathrm{E}_6(q) \\ M\in\mathcal{U}}} \frac{1}{|G:M|} \leqslant \frac{120(3,q-1)q^{28}(\log q)\log(4q^{28}\log q)}{7|\mathrm{SL}_2(q)||\mathrm{SL}_6(q)|} < 0.029 \quad \text{for } q \geqslant 3;$$

$$\sum_{\substack{S={}^2\mathrm{E}_6(q) \\ M\in\mathcal{U}}} \frac{1}{|G:M|} \leqslant \frac{120(3,q+1)q^{28}(\log q)\log(4q^{28}\log q)}{7|\mathrm{SL}_2(q)||\mathrm{SU}_6(q)|} < 0.027 \quad \text{for } q \geqslant 3;$$

$$\sum_{\substack{S=\mathrm{E}_7(q) \\ M\in\mathcal{U}}} \frac{1}{|G:M|} \leqslant \frac{540q^{30}(\log q)\log(9q^{30}\log q)}{7|\mathrm{SL}_8(q)|} < 0.001 \qquad \text{for all } q;$$

$$\sum_{\substack{S=\mathrm{E}_8(q) \\ M\in\mathcal{U}}} \frac{1}{|G:M|} \leqslant \frac{360q^{56}(\log q)\log(12q^{56}\log q)}{7(4,q^2-1)|\mathrm{O}_{16}^+(q)|} < 0.001 \qquad \text{for all } q.$$

Combining the estimates for the classes $\mathcal{K}$ and $\mathcal{U}$ in Equation (1), we conclude that $P_{G,S}(2) > \gamma$ if $S = \mathrm{F}_4(q)$ with $q \geqslant 17$, or $S = \mathrm{E}_6(q)$ with $q \geqslant 3$, or $S = {}^2\mathrm{E}_6(q)$ with $q \geqslant 3$, or $S = \mathrm{E}_7(q)$ for any q, or $S = \mathrm{E}_8(q)$ for any q.

Large rank exceptional groups (special cases). The maximal subgroups of $\mathrm{F}_4(2)$ and $\mathrm{Aut}\,\mathrm{F}_4(2) = \mathrm{F}_4(2).2$ (see [39]), $\mathrm{E}_6(2)$ and $\mathrm{Aut}\,\mathrm{E}_6(2) = \mathrm{E}_6(2).2$ (see [21]), and all almost simple groups with socle ${}^2\mathrm{E}_6(2)$ (the list in

the original printing of the ATLAS is stated to be complete in the improvements section of the reprint [5]) are now known. Hence $P_{G,\operatorname{soc} G}(2) > \gamma$ when G is an almost simple group with socle $\mathrm{F}_4(2)$, $\mathrm{E}_6(2)$, or ${}^2\mathrm{E}_6(2)$.

We deal with the group $\mathrm{F}_4(q)$ for $q \in \{5, 7, 11, 13\}$ by making use of the work of Magaard in his Ph.D. thesis [30]. Note that if $q \in \{5, 7, 11, 13\}$ then $\mathrm{F}_4(q) = \operatorname{Aut} \mathrm{F}_4(q)$. For these q, we take $\mathcal{K}$ to be representatives for the maximal subgroups listed in [47, Theorem 4.4(i)–(xv)]. There are no maximal subgroups of the form $\mathrm{F}_4(q_0)$, since q is prime. Comparing with the information about conjugacy classes in [26] we see that there is at most one class of each type of maximal subgroup. There are 14 classes listed, and each subgroup has index at least q^{15}, so $\sum_{M\in\mathcal{K}} 1/|\mathrm{F}_4(q) : M| \leqslant 14/q^{15} < 0.001$ for $q \in \{5, 7, 11, 13\}$. The groups in the class $\mathcal{U}$ of "unknown" maximal subgroups are almost simple, with the largest possible almost simple group having socle ${}^3\mathrm{D}_4(2)$. Hence if $M \in \mathcal{U}$ with socle T, then $|\operatorname{Aut} T||\operatorname{Out} T| \leqslant k_0 = 3^2|{}^3\mathrm{D}_4(2)|$. Using Lemma 3.1 (i), and the same estimate for $i(S)$ as above, we conclude

$$\sum_{M\in\mathcal{U}} \frac{1}{|\mathrm{F}_4(q) : M|} < \frac{5k_0}{|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)|} < 0.001$$

for $q \in \{5, 7, 11, 13\}$. Hence

$$P_{\mathrm{F}_4(q)}(2) > \gamma \qquad \text{for } q \in \{5, 7, 11, 13\}.$$

It remains to deal with $\mathrm{F}_4(q)$ for $q \in \{3, 4, 8, 9, 16\}$. This is done by refinements of the arguments presented above. We describe the steps for $\mathrm{F}_4(3)$ in detail and summarise them for the other values of q.

$\boldsymbol{S = \mathrm{F}_4(3)}$: Note that $|\mathrm{F}_4(3)| = 2^{15} \cdot 3^{24} \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 41 \cdot 73$, and that $\mathrm{F}_4(3) = \operatorname{Aut} \mathrm{F}_4(3)$, so we only need determine $P_{\mathrm{F}_4(3)}(2)$. Using the fact that $\mathrm{F}_4(3)$ has a 25-dimensional faithful representation over a field of characteristic 3 (see [28]), whereas $\mathrm{O}_8^+(2)$ does not [16], and consideration of divisors of the group order to further refine the lists in [25, Table 1], we conclude that if $M \in \mathcal{U}$ (as defined earlier) and the socle S is not of Lie type of untwisted rank at most 2 and characteristic 3, then S is one of:

$$A_n \ (n \leqslant 10),\ \mathrm{J}_2,\ \mathrm{L}_2(7),\ \mathrm{L}_2(13),\ \mathrm{L}_2(25),\ \mathrm{L}_3(4),\ \mathrm{S}_6(2),\ {}^3\mathrm{D}_4(2).$$

The remaining maximal subgroups M have socle S that is of Lie type in characteristic 3 and Lie rank at most 2. For such a socle $X(3^t)$, we exploit the fact that $|M| < 4 \cdot 3^{20} \log 3$, by Proposition 3.2, and [26, Theorem 8 (VI)] to obtain for each possible X an upper bound for the value of t. Consideration of divisors

of $|\mathrm{F}_4(3)|$ then give further restrictions on t, and we conclude that such an S is one of:

$$\begin{array}{ll} \mathrm{L}_2(3^t) & \text{for } t \in \{2,3,4\}, \\ \mathrm{L}_3(3^t) & \text{for } t \in \{1,2\}, \\ \mathrm{U}_3(3^t) & \text{for } t \in \{1,2\}, \end{array} \qquad \begin{array}{ll} \mathrm{S}_4(3^t) & \text{for } t \in \{1,2\}, \\ \mathrm{G}_2(3), {}^2\mathrm{G}_2(3)'. & \end{array}$$

Define $\mathcal{U}_0$ to be the set of almost simple maximal subgroups M of $\mathrm{F}_4(3)$ such that the socle S lies in either of the above two lists but is not isomorphic to $\mathrm{S}_4(9)$. Define $\mathcal{U}_{\mathrm{S}_4(9)}$ to be the set of almost simple maximal subgroups M of G with socle isomorphic to $\mathrm{S}_4(9)$. Then $\mathcal{U} = \mathcal{U}_0 \cup \mathcal{U}_{\mathrm{S}_4(9)}$, while if $T = \operatorname{soc} M$ with $M \in \mathcal{U}_0$ then

$$|\operatorname{Aut} T||\operatorname{Out} T| \leqslant |\operatorname{Aut} {}^3\mathrm{D}_4(2)||\operatorname{Out} {}^3\mathrm{D}_4(2)| = k_0.$$

Hence, by Lemma 3.1(i) and Equation (3),

$$\sum_{M \in \mathcal{U}_0} \frac{1}{|G:M|} \leqslant \frac{5k_0}{|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|} < 0.044.$$

To estimate the sum over maximal subgroups in $\mathcal{U}_{\mathrm{S}_4(9)}$, we use the following lemma, which is established by a simple counting argument, to replace Lemma 3.1. When $T = \mathrm{S}_4(9)$, we shall determine an estimate for the value d that appears below via a sequence of MAGMA calculations [2].

LEMMA 3.3: *Let T be a non-abelian finite simple group that can be generated by an involution and an element of prime order p. Suppose that there are d pairs $(t,x) \in T \times T$ such that $o(t) = 2$, $o(x) = p$ and $\langle t, x\rangle = T$. If G is any group, let $i(G)$ and $i_p(G)$ denote the number of elements of order 2 and p, respectively, in G. Then the number of subgroups of G isomorphic to T is at most $i(G)i_p(G)/d$.*

We take $T = \mathrm{S}_4(9)$ and $p = 41$ in this lemma. Working in MAGMA, we calculate the conjugacy classes of T and fix an element x of order 41 in T. We determine there are 298 152 involutions $t \in T$ such that $\langle t, x\rangle = T$, and that $|\mathrm{C}_T(x)| = 41$. Consequently, we deduce $d \geqslant 7272|T|$ in this case. The largest divisor of $|G|$ congruent to 1 (mod 41) is $|G|/2^4 \cdot 41$, so $i_{41}(G) \leqslant 40|G|/2^4 \cdot 41$. Hence

$$\sum_{M \in \mathcal{U}_{\mathrm{S}_4(9)}} \frac{1}{|G:M|} \leqslant \frac{5 \cdot 40\,|\mathrm{S}_4(9)||\operatorname{Out} \mathrm{S}_4(9)|^2}{(2^4 \cdot 41) \cdot 7272\,|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|} < 0.001.$$

Putting this information together with Equation (2), we conclude that

$$P_{\mathrm{F}_4(3)}(2) \geqslant 1 - \sum_{M \in \mathcal{K} \cup \mathcal{U}} \frac{1}{|G:M|} > \gamma.$$

$\mathbf{F_4(4)}$: For G an almost simple group with socle $S = \mathrm{F}_4(4)$, we let $\mathcal{U}$ consist of those almost simple subgroups of S that are either groups of Lie type of untwisted rank at most 2 and characteristic 2, or are not groups of Lie type in characteristic 2. Using [25, Theorem 1] and [26, Theorem 8 (VI)], we observe that if $M \in \mathcal{U}$ and $T = \operatorname{soc} M$, then

$$|\operatorname{Aut} T||\operatorname{Out} T| \leqslant |\operatorname{Aut} \mathrm{L}_3(16)||\operatorname{Out} \mathrm{L}_3(16)| = k_0.$$

We shall use the bound $i(S) \leqslant 5|S|/4^{18}|\mathrm{SL}_2(4)|^2$ that follows from information for even q in [27, Table II]. Hence, by Lemma 3.1(i),

$$\sum_{M \in \mathcal{U}} \frac{1}{|G:M|} \leqslant \frac{i(S)k_0}{|S|} < 0.017$$

and, using (2), we conclude that $P_{G,\mathrm{F}_4(4)}(2) > \gamma$.

$\mathbf{F_4(q)}$, $\boldsymbol{q = 8, 16}$: For G an almost simple group with socle $S = \mathrm{F}_4(q)$ with $q \in \{8, 16\}$, we define $\mathcal{U}$ as before, and calculate that if $T = \operatorname{soc} M$ where $M \in \mathcal{U}$, then

$$|\operatorname{Aut} T||\operatorname{Out} T| \leqslant |\operatorname{Aut} \mathrm{G}_2(8)||\operatorname{Out} \mathrm{G}_2(8)| = k_0.$$

By [27, Table II], $i(S) \leqslant 5|S|/q^{18}|\mathrm{SL}_2(q)|^2$. Hence

$$\sum_{M \in \mathcal{U}} \frac{1}{|G:M|} \leqslant \frac{i(S)k_0}{|S|} < 0.001$$

and, using (2), we conclude that $P_{G,\mathrm{F}_4(q)}(2) > \gamma$.

$\mathbf{F_4(9)}$: For G an almost simple group with socle $S = \mathrm{F}_4(9)$, we proceed as in previous cases to conclude that if $T = \operatorname{soc} M$ where $M \in \mathcal{U}$, then

$$|\operatorname{Aut} T||\operatorname{Out} T| \leqslant |\operatorname{Aut} \mathrm{G}_2(9)||\operatorname{Out} \mathrm{G}_2(9)| = k_0.$$

Hence, by Lemma 3.1(i),

$$\sum_{M \in \mathcal{U}} \frac{1}{|G:M|} \leqslant \frac{i(S)k_0}{|S|} < 0.001$$

and, using (2), we conclude that $P_{G,\mathrm{F}_4(9)}(2) > \gamma$.

REMARK 3.4: *All exceptional finite almost simple groups G satisfy $d(G) = 2$, so in this section we have established that if G is almost simple with socle S, where S is a finite exceptional group that is not isomorphic to a classical group, then $P_{G,S}(2) > \gamma$.*

4. Classical groups

For almost simple classical groups G of small dimension we make use of the tables found in Bray–Holt–Roney-Dougal [4], which list all maximal subgroups of G that supplement the socle of G, together with the relevant Aschbacher class, for $\operatorname{soc} G$ one of $\mathrm{L}_n(q)$, $\mathrm{S}_n(q)$, $\mathrm{U}_n(q)$, $\mathrm{O}^\circ_n(q)$ and $\mathrm{O}^\pm_n(q)$ for $n \leqslant 12$. This data is also implemented in the MAGMA function `ClassicalMaximals`, so for individual cases we use this to estimate the bound of Equation (1). For larger dimensions, our method is essentially along the lines of Kantor–Lubotzky [17] but also making use of a result of Liebeck [23] to bound the size of an almost simple maximal subgroup. We calculate the probability $P_{G,\operatorname{soc} G}(2)$ precisely for the classical almost simple groups G that cannot be handled in these ways (most of which are displayed in Table 1).

Throughout this section, G is a simple classical group of dimension n over a field of order $q = p^k$ with p prime.

SMALL DIMENSION CLASSICAL GROUPS. Only certain of the simple classical groups of dimension $n \leqslant 12$ need to be handled using the tables in [4]. The rest are dealt with by the general method. For $\mathrm{L}_2(q)$, a detailed analysis is required, whereas for other small dimension classical groups it is sufficient to bound the number of conjugacy classes of maximal subgroups.

$\mathbf{L_2(q)}$: Let $\mathcal{M}$ be a set of S-conjugacy class representatives of the maximal subgroups of $G \leqslant \operatorname{Aut} \mathrm{L}_2(q)$ that supplement $S = \operatorname{soc} G \cong \mathrm{L}_2(q)$, let $\mathcal{L} = \{ H \cap S \mid H \in \mathcal{M} \}$, and let $\mathcal{L}_0$ denote the corresponding subgroups of $\mathrm{SL}_2(q)$. Then by analysing the order, occurrence, and number of conjugacy classes of possible groups in $\mathcal{M}$ as stated in [4] we deduce that

$$\sum_{L \in \mathcal{L}_0} |L| \leqslant \begin{cases} q^2 + 3q + 336 & \text{if } k = 1, \\ q^2 + 3q + 2q^{1/2}(q-1) + 240 & \text{if } k = 2, \\ q^2 + 3q + 2q^{1/2}(q-1) + q^{1/3}(q^{2/3} - 1)\log q & \text{if } k \geqslant 3, \end{cases}$$

from which

$$\sum_{M\in\mathcal{L}} \frac{1}{|S:M|} \leqslant \frac{q^2+3q+336}{q(q^2-1)} < 0.06 \qquad \text{for } q=p\geqslant 29,$$

and similarly that the sum is at most 0.03 for $q=p^2\geqslant 49$, and at most 0.07 for $q=p^k\geqslant 27$ with $k\geqslant 3$. We conclude that

$$P_{G,\mathrm{L}_2(q)}(2) > \gamma \qquad \text{for } q\geqslant 27.$$

The values of $P_{G,\mathrm{L}_2(q)}(2)$ for $4\leqslant q\leqslant 25$ are computed precisely using the `EulerianFunction` and library of Table of Marks implemented in GAP [10, 38]. These values appear in Table 1 if they are at most $\frac{9}{10}$. The groups G such that $\frac{9}{10} < P_{G,S}(2) \leqslant \gamma$ are listed in Remark 4.1, below.

Other small dimension classical groups. Table 4 provides an upper bound c for the number of conjugacy classes of maximal subgroups of G that supplement $\operatorname{soc} G$, which can be read off the tables in [4], and a lower bound ρ for the index of those maximal subgroups, given in [17, Table 5.2.A], for the classical groups we now consider. Then $P_{G,S}(2)\geqslant 1-c/\rho$ and so $P_{G,S}(2)>\gamma$ for $S=\mathrm{L}_3(q)$ for $q\geqslant 17$, $\mathrm{L}_4(q)$ for $q\geqslant 8$, $\mathrm{U}_3(q)$ for $q\geqslant 7$, $\mathrm{U}_4(q)$ for $q\geqslant 5$, $\mathrm{U}_5(q)$ for $q\geqslant 3$, $\mathrm{U}_6(q)$ for $q\geqslant 3$, $\mathrm{S}_4(q)$ for $q\geqslant 5$, $\mathrm{S}_6(q)$ for $q\geqslant 3$, $\mathrm{O}_7(q)$ for all odd q, $\mathrm{O}_8^+(q)$ for $q\geqslant 4$ and $\mathrm{O}_8^-(q)$ for $q\geqslant 3$.

We use the Magma function `ClassicalMaximals` to check $P_{G,S}(2)>\gamma$ when S is one of $\mathrm{L}_3(q)$ for $5\leqslant q\leqslant 16$, $\mathrm{L}_4(q)$ for $4\leqslant q\leqslant 7$, $\mathrm{U}_3(4)$, $\mathrm{U}_4(q)$ for $q=3,4$, $\mathrm{U}_5(2)$, $\mathrm{U}_6(2)$, $\mathrm{S}_4(4)$, $\mathrm{O}_8^+(q)$ for $q=2,3$ and $\mathrm{O}_8^-(2)$. We calculate the probabilities for the remaining groups of these dimensions precisely and those with $P_{G,S}(2)\leqslant\frac{9}{10}$ are found in Table 1.

Larger dimension classical groups. We now assume that $n\geqslant 5$, and moreover that $n\geqslant 7,8,9$ if G is unitary, symplectic, or orthogonal, respectively. Theorem 4.1 of Liebeck [23] states that if M is a maximal subgroup of G that supplements $\operatorname{soc} G$ then one of the following holds:

(i) M is a "geometric maximal subgroup", that is, belongs to one of the Aschbacher classes $\mathscr{C}_1$–$\mathscr{C}_8$;
(ii) M is A_c or S_c embedded in G and $n\in\{c-1,c-2\}$;
(iii) $|M|<q^{3un}$, where $u=2$ if G is unitary, and $u=1$ otherwise.

We write $m_1(G)$ for the number of conjugacy classes of maximal subgroups of types (i) and (ii) in G and $m(G)$ for the total number of conjugacy classes of

S	c	Min. index
$\mathrm{L}_3(p^k)$, $k \leqslant 2$	16	q^2+q+1
$\mathrm{L}_3(p^k)$, $k \geqslant 3$	$10+3\log q$	q^2+q+1
$\mathrm{L}_4(q)$, $q \geqslant 3$	$24+4\log q$	q^3+q^2+q+1
$\mathrm{U}_3(q)$, $q \neq 5$	$13+3\log q$	q^3+1
$\mathrm{U}_4(q)$	$27+\log q$	q^4+q^3+q+1
$\mathrm{U}_5(q)$	$11+5\log q$	$(q^5+1)(q^2+1)$
$\mathrm{U}_6(q)$, $q \geqslant 3$	$34+6\log q$	$(q^5+1)(q^4+q^2+1)$
$\mathrm{S}_4(q)$, $q \geqslant 4$	$9+\log q$	q^3+q^2+q+1
$\mathrm{S}_6(q)$, $q \geqslant 3$	$21+\log q$	$(q^6-1)/(q-1)$
$\mathrm{O}_7(q)$	$14+\log q$	$(q^6-1)/(q-1)$ for $q \geqslant 5$, $3^3(3^3-1)/2$ for $q=3$
$\mathrm{O}_8^+(q)$, $q \geqslant 4$	$81+\log q$	$(q^4-1)(q^3+1)/(q-1)$
$\mathrm{O}_8^-(q)$	$12+\log q$	$(q^4+1)(q^2+q+1)$

Table 4. Data for small dimension classical groups

maximal subgroups. We use the bound

$$m(G) < 2n^{5.2} + n\log\log q$$

given by Häsä [13, Theorem 1.1] and this provides us with an upper bound for the number of conjugacy classes of maximal subgroups M of type (iii). We can use Tables 3.5.A–G in [20] to estimate the number of conjugacy classes of geometric maximal subgroups, and add in the groups with socle A_c as specified by Liebeck, getting

$$m_1(G) \leqslant 6n + \tfrac{1}{3}n\log n + n\log\log q$$

unless $G = \mathrm{O}_n^+(q)$ in which case

$$m_1(G) \leqslant \tfrac{5}{2}n + 12n^{1/2} + 9\log n + \log\log q + 12.$$

We then employ the estimate

$$P_{G,S}(2) > 1 - \frac{m_1(G)}{\rho(G)} - \frac{m(G)q^{3un}}{|S|}$$

where $\rho(G)$ is the bound for the index of a maximal subgroup given in [20, Table 5.2.A] together with corrections for $S = \mathrm{U}_n(2)$ for n even and $\geqslant 6$ and for $S = \mathrm{O}_n^+(3)$ (Bray [3]). Hence $P_{G,S}(2) > \gamma$ for all such G with the possible exception of the following socles:

$$\begin{aligned}
&\mathrm{L}_n(q), \quad (n,q) \in \{(5,2),(5,3),(5,4),(6,2),(6,3),(7,2),(8,2),(9,2)\},\\
&\mathrm{U}_n(q), \quad (n,q) \in \{(7,2),(7,3),(7,4),(7,5),(7,7),(7,8),(7,9),(8,2)\},\\
&\mathrm{S}_n(q), \quad (n,q) \in \{(8,2),(8,3),(10,2)\},\\
&\mathrm{O}_n^\circ(q), \quad (n,q) \in \{(9,3),(9,5)\},\\
&\mathrm{O}_n^-(q), \quad (n,q) \in \{(10,2),(10,3)\},\\
&\mathrm{O}_n^+(q), \quad (n,q) \in \{(10,2)\}.
\end{aligned}$$

These groups are all of sufficiently small dimension to be covered by the Bray–Holt–Roney-Dougal tables. If $S = \mathrm{L}_5(2)$ then we calculate the precise values of $P_{G,S}(2)$, and find that $P_{G,S}(2) > \gamma$. For the remaining groups we use the MAGMA function `ClassicalMaximals` to verify that $P_{G,S}(2) > \gamma$.

REMARK 4.1: *In this section, we have established that if G is almost simple with socle S, where S is isomorphic to a finite classical group, then Theorem 1.1 holds for G. In addition, $\frac{9}{10} < P_{G,S}(2) \leqslant \gamma$ if and only if one of the following holds: $S = \mathrm{L}_2(13)$; $S = \mathrm{L}_2(16)$; $G = \mathrm{L}_2(17)$; $G = \mathrm{L}_2(19)$; $G = \mathrm{L}_3(4).2$ (where the involution is the product of the field and duality automorphisms); $G = \mathrm{PGL}_3(4)$; $G = \mathrm{P\Gamma L}_3(4)$; $S = \mathrm{U}_3(3)$; or $G = \mathrm{S}_6(2)$.*

5. Alternating groups

In this section we obtain bounds on the probability $P_{G,\mathrm{A}_n}(2)$, where G is almost simple with socle A_n and $n \geqslant 5$.

For small values of n (namely $5 \leqslant n \leqslant 13$), a direct computation in GAP using the table of marks of G determines $P_{G,\mathrm{A}_n}(2)$. In particular, all such groups with $P_{G,\mathrm{A}_n}(2) \leqslant \frac{9}{10}$ are given with precise probabilities in Table 1.

For $14 \leqslant n \leqslant 21$, information on the conjugacy classes of maximal subgroups of A_n is stored in MAGMA. This enables us to compute an estimate for $P_{G,\mathrm{A}_n}(2)$ using Equation (1), and to conclude that $P_{G,\mathrm{A}_n}(2) > \frac{9}{10}$ for $14 \leqslant n \leqslant 21$, whilst $P_{G,\mathrm{A}_n}(2) > \gamma$ for $17 \leqslant n \leqslant 21$.

For $n \geqslant 22$ we use recent work of Maróti and Tamburini [32], where they prove that the probability that 2 random elements of A_n or S_n generate a subgroup containing A_n is at least $1 - 1/n - 13/n^2$. Examining their proofs shows that

if G is almost simple with socle $S = \mathrm{A}_n$ then $P_{G,S}(2) \geqslant 1 - 1/n - 13/n^2$. For $n \geqslant 22$ this is greater than γ.

REMARK 5.1: *In this section we have proved that Theorem 1.1 holds for almost simple groups with socle* A_n*, and also that if* $P_{G,\mathrm{A}_n}(2) \leqslant \gamma$ *then* $n \leqslant 16$.

6. Sporadic simple groups

Bounding the conditional probability of generating the almost simple sporadic groups is, on the whole, straightforward.

For the Mathieu groups M_{11}, M_{12} or $\mathrm{Aut}\,\mathrm{M}_{12} = \mathrm{M}_{12}.2$, a computation in GAP or MAGMA can be used to obtain the precise value of the conditional probability. Only the values of $P_{\mathrm{M}_{11}}(2)$ and $P_{\mathrm{M}_{12}}(2)$ are at most γ, and these are given in Table 1.

For all other sporadic almost simple groups G, except for the Monster, the conjugacy classes of maximal subgroups are known and listed in the ATLAS [5]. We compute an estimate for $P_{G,S}(2)$ using Equation (1) and conclude that $P_{G,S}(2) > \gamma$ for all such G.

The maximal subgroups of the Monster $\mathrm{M} = \mathrm{Aut}\,\mathrm{M}$ are not fully known, but sufficient information exists in the literature to bound the probability $P_{\mathrm{M}}(2)$. We express the set $\mathcal{M}$ of conjugacy class representatives of the maximal subgroups of M as a union of the three subsets $\mathcal{L}$, $\mathcal{P}$ and $\mathcal{U}$.

The set $\mathcal{L}$ consists of maximal subgroups L that are p-local for some prime p. A set containing the groups in $\mathcal{L}$ is known (see [35, 46]) and provides us with at most 39 conjugacy classes of maximal subgroups of index at least 10^{18}.

The set $\mathcal{P}$ consists of maximal subgroups L that are normalisers of a direct product of two or more isomorphic non-abelian simple groups. The list of these maximal subgroups given in the ATLAS is complete, and gives 9 conjugacy classes of maximal subgroups of index at least 10^{30}.

The set $\mathcal{U}$ consists of almost simple maximal subgroups L of M, and is determined up to a finite list of isomorphism types. Here we make use of Lemma 3.1. The possible simple socles of these subgroups of M are listed in [40, Table 2] (with the addition of $\mathrm{L}_2(41)$ [48]), and so if S is the socle of an almost simple maximal subgroup of M, then $|\mathrm{Aut}\,S||\mathrm{Out}\,S| \leqslant |\mathrm{Fi}_{23}|$. The character table of M in [5] determines that $i(\mathrm{M}) < 5.8 \times 10^{27}$.

Putting these together, we conclude that

$$\sum_{L\in\mathcal{M}} \frac{1}{|\mathrm{M}:L|} \leqslant \frac{39}{10^{18}} + \frac{9}{10^{30}} + \frac{i(\mathrm{M})|\mathrm{Fi}_{23}|}{|\mathrm{M}|} < 0.001.$$

REMARK 6.1: *In this section we have estabilised that if G is almost simple with sporadic socle S, then $P_{G,S}(2) \leqslant \gamma$ if and only if $G = \mathrm{M}_{11}, \mathrm{M}_{12}$.*

7. Proof of Corollary 1.2

By [7], $d(G/S) \leqslant 3$, with equality only if $S = \mathrm{L}_n(q)$ with $n \geqslant 4$ and q an even power of an odd prime, or $S = \mathrm{O}_n^+(q)$ with $n \geqslant 8$ and q as before. If $d(G) = 2$ then $P_{G,S}(3) > P_{G,S}(2)$.

If $S = \mathrm{A}_n$ and $P_{G,S}(2) \leqslant \gamma$, then it follows from Remark 5.1 that $n \leqslant 16$. For $n \geqslant 14$ we use knowledge of the maximal subgroups of G to show that $P_{G,S}(3) > \gamma$, whilst for $5 \leqslant n \leqslant 13$ we calculate exact bounds using `EulerianFunction` in GAP. If S is a classical group and $d(G) = 2$, then we note in Remark 4.1 that $P_{G,S}(2) > \gamma$ except for the groups in Table 1, and certain G with socles $\mathrm{L}_2(q)$ (with $q \leqslant 19$), $\mathrm{L}_3(4)$, $\mathrm{U}_3(3)$, or $\mathrm{S}_6(2)$. It is straightforward to verify these cases computationally using MAGMA. If S is an exceptional group then $d(G) = 2$, and we note in Remark 3.4 that $P_{G,S}(2) > \gamma$. Finally, if S is sporadic then we note in Remark 3.4 that $P_{G,S}(2) > \gamma$ unless G is in Table 1, and we check these computationally.

It remains to consider the groups G with $d(G/S) = 3$. When we proved Theorem 1.1 for groups H with $d(H/S) \leqslant 2$, we bounded $\sum_{M\in\mathcal{M}} 1/|H:M|$ for $\mathcal{M}$ a set of conjugacy class representatives of maximal subgroup of H that do not contain S. When doing so, we in fact check that this holds for *all* groups G with socle S, and so in particular the bounds that we establish cover the 3-generator groups G. This completes the proof.

References

[1] M. Aschbacher & G.M. Seitz, "Involutions in Chevalley groups over finite fields of even order," *Nagoya Math. J.* **63** (1976) 1–91; correction, *ibid.* **72** (1978) 135–136.

[2] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.* **24** (1997) 235–265.

[3] J.N. Bray, personal communication.

[4] J.N. Bray, D.F. Holt & C.M. Roney-Dougal, *The maximal subgroups of the low dimensional finite classical groups*, LMS Lecture Notes Ser., CUP, to appear.

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker & R.A. Wilson, ATLAS *of Finite Groups*, OUP, Oxford, reprinted 2003 with corrections.
[6] B.N. Cooperstein, "Maximal subgroups of $G_2(2^n)$", *J. Algebra* **70** (1981) 23–36.
[7] F. Dalla Volta & A. Lucchini, "Generation of almost simple groups," *J. Algebra* **178** (1995) 194–223.
[8] J.D. Dixon, "The probability of generating the symmetric group," *Math. Z.* **110** (1969) 199–205.
[9] L. Fireman, "On pro-S groups," *J. Group Theory* **13** (2010) 759–767.
[10] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12, 2008. (`http://www.gap-system.org`)
[11] W. Gaschütz, "Zu einem von B.H. und H. Neumann gestellten Problem," *Math. Nachr.* **14** (1955) 249–252.
[12] P. Hall, "The Eulerian function of a group," *Quart. J. Math. Oxford* **7** (1936) 134–151.
[13] J. Häsä, "Growth of cross-characteristic representations of finite quasisimple groups of Lie type", arXiv:1112.3941v1, Dec 2011.
[14] D.F. Holt and M.J. Stather, "Computing a chief series and the soluble radical of a matrix group over a finite field", *London Math. Soc. J. Comput. Math.* **11** (2008), 223 – 251.
[15] N. Iwahori, "Centralizers of involutions in finite Chevalley groups," in *Seminar on Algebraic Groups and Related Finite Groups*, Lecture Notes Math. **131**, Springer, Berlin, 1970, pp. 267–295.
[16] C. Jansen, K. Lux, R. Parker & R. Wilson, *An Atlas of Brauer Characters*, LMS Monographs, New Ser. **11**, OUP, New York, 1995.
[17] W.M. Kantor & A. Lubotzky, "The probability of generating a finite classical group," *Geom. Dedicata* **36** (1990) 67–87.
[18] P.B. Kleidman, "The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups," *J. Algebra* **115** (1988) 182–199.
[19] P.B. Kleidman, "The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree Groups ${}^2G_2(q)$, and their automorphism groups," *J. Algebra* **117** (1988) 30–71.
[20] P. Kleidman & M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, LMS Lecture Note Ser. **129**, CUP, Cambridge, 1990.
[21] P.B. Kleidman & R.A. Wilson, "The maximal subgroups of $E_6(2)$ and $\mathrm{Aut}(E_6(2))$," *Proc. London Math. Soc. (3)* **60** (1990) 266–294.
[22] P.B. Kleidman & R.A. Wilson, "Sporadic simple subgroups of finite exceptional groups of Lie type," *J. Algebra* **157** (1993) 316–330.
[23] M.W. Liebeck, "On the orders of maximal subgroups of the finite classical groups," *Proc. London Math. Soc. (3)* **50** (1985) 426–446.
[24] M.W. Liebeck, J. Saxl & G.M. Seitz, "Subgroups of maximal rank in finite exceptional groups of Lie type," *Proc. London Math. Soc. (3)* **65** (1992) 297–325.
[25] M.W. Liebeck & G.M. Seitz, "On finite subgroups of exceptional algebraic groups," *J. Reine Angew. Math.* **515** (1999) 25–72.
[26] M.W. Liebeck & G.M. Seitz, "A survey of maximal subgroups of exceptional groups of Lie type," in *Groups, combinatorics & geometry (Durham, 2001)*, 139–146, World Sci. Publ., River Edge, NJ, 2003.

[27] M.W. Liebeck & A. Shalev, "The probability of generating a finite simple group," *Geom. Dedicata* **56** (1995) 103–113.

[28] F. Lübeck, "Small degree representations of finite Chevalley groups in defining characteristic," *London Math. Soc. J. Comput. Math.* **4** (2001) 135–169.

[29] A. Lucchini, "Closed normal subgroups of free pro-S-groups of finite rank," *J. Group Theory* **14** (2011) 819–823.

[30] K. Magaard, *The maximal subgroups of the Chevalley groups* $\mathrm{F}_4(F)$ *where* F *is a finite or algebraically closed field of characteristic* $\neq 2, 3$, Ph.D. thesis, Calif. Inst. Tech., 1990.

[31] G. Malle, "The maximal subgroups of ${}^2\mathrm{F}_4(q^2)$," *J. Algebra* **139** (1991) 52–69.

[32] A. Maróti & M.C. Tamburini, "Bounds for the probability of generating the symmetric and alternating groups," *Arch. Math.* **96** (2011) 115–121.

[33] A. Maróti & M.C. Tamburini, "A solution to a problem of Wiegold," preprint, 2011.

[34] V.D. Mazurov & E.I. Khukhro (eds.), *The Kourovka Notebook, No. 17*, Russian Acad. Sciences, Institute Math., Novosibirsk, 2010.

[35] U. Meierfrankenfeld & S. Shpectorov, "Maximal 2-local subgroups of the Monster and Baby Monster, I & II," preprints, 2002 & 2003, (`http://www.math.msu.edu/~meier/Preprints/2monster/abstract.html`)

[36] O.V. Mel′nikov, "Normal divisors of free profinite groups (Russian)", *Izv. Akad. Nauk SSSR Ser. Mat.* **42** (1978) 3–25, 214. English translation: *Math. USSR-Izv.* **12** (1978) 1–20 (1979).

[37] N.E. Menezes, *Random generation and chief length of finite groups*, Ph.D. thesis, University of St Andrews (in preparation).

[38] L. Naughton & G. Pfeiffer, Tomlib, Version 1.2.1, GAP package, 2011, (`http://schmidt.nuigalway.ie/tomlib`).

[39] S.P. Norton & R.A. Wilson, "The maximal subgroups of $\mathrm{F}_4(2)$ and its automorphism group," *Comm. Algebra* **17** (1989) 2809–2824.

[40] S.P. Norton & R.A. Wilson, "Anatomy of the Monster: II," *Proc. London Math. Soc. (3)* **84** (2002) 581–598.

[41] M. Suzuki, "On a class of doubly transitive groups," *Ann. Math.* **75** (1962) 105–145.

[42] A.V. Vasilyev, "Minimal permutation representations of finite simple exceptional groups of types G_2 and F_4," *Algebra Logic* **35** (1996) 371–383.

[43] A.V. Vasilyev, "Minimal permutation representations of finite simple exceptional groups of types E_6, E_7 and E_8," *Algebra Logic* **36** (1997) 302–310.

[44] A.V. Vasilyev, "Minimal permutation representations of finite simple exceptional groups of twisted type," *Algebra Logic* **37** (1998) 9–20.

[45] J. Wiegold, "Growth sequences of finite groups, " *J. Austral. Math. Soc.* **17** (1974) 133–141.

[46] R.A. Wilson, "The odd-local subgroups of the Monster," *J. Austral. Math. Soc. Ser. A* **44** (1988) 1–16.

[47] R.A. Wilson, *The Finite Simple Groups*, Grad. Texts Math. **251**, Springer-Verlag, London, 2009.

[48] R.A. Wilson, personal communication.