Glasgow Math. J. **45** (2003) 281–291.
DOI: 10.1017/S0017089503001241. Printed in the United Kingdom

SOME REMARKS ON THE PROBABILITY OF GENERATING AN ALMOST SIMPLE GROUP

FRANCESCA DALLA VOLTA

Dipartimento di Matematica e Applicazioni, Università di Milano – Bicocca, Via Bicocca Degli Arcimboldi 8, 20126 Milano, Italy
e-mail: dallavolta@matapp.unimib.it

ANDREA LUCCHINI and FIORENZA MORINI

Dipartimento di Matematica, Università di Brescia, Via Valotti 9, 25133 Brescia, Italy
e-mail: lucchini@ing.unibs.it, morini@ing.unibs.it

(Received 7 March, 2002; accepted 8 August, 2002)

Abstract. We compare the probability of generating with a given number of random elements two almost simple groups with the same socle S. In particular we analyse the case $S = \mathrm{PSL}(2, p)$.

2000 *Mathematics Subject Classification.* 20P05, 20D06, 20D60.

1. Introduction. A finite nonabelian simple group S can be identified with a subgroup of its automorphism group $\mathrm{Aut}\, S$. In [**1**] it is proved that for any pair of elements g_1, g_2 in $\mathrm{Aut}\, S$, there exist s_1, s_2 in S such that $\langle g_1 s_1, g_2 s_2\rangle = \langle g_1, g_2, S\rangle$, i.e. the subgroup of $\mathrm{Aut}\, S$ generated by $g_1 s_1$, $g_2 s_2$ contains S. Given g_1, g_2 in $\mathrm{Aut}\, S$ we want to study the probability $P_{g_1,g_2}(S)$ that a pair of elements s_1, s_2 satisfies the condition $\langle g_1 s_1, g_2 s_2\rangle = \langle g_1, g_2, S\rangle$.

First we need to recall some definitions. For any finite group let $\phi_G(t)$ denote the number of ordered t-tuples $(g_1, \ldots, g_t)$ of elements of G that generate G. The number $P_G(t) = \frac{\phi_G(t)}{|G|^t}$ gives the probability that t randomly chosen elements of G generate G. Moreover if N is a normal subgroup of G, we define $P_{G,N}(t) = P_G(t)/P_{G/N}(t)$. This number is the probability that a t-tuple generates G, given that it generates G modulo N. In particular $P_{G,G}(t) = P_G(t)$. Note that $|N|^t P_{G,N}(t) = \frac{\phi_G(t)}{\phi_{G/N}(t)}$; moreover, by a remark due to Gaschütz [**4**], given t elements $(g_1, \ldots, g_t)$ generating G modulo N, $\frac{\phi_G(t)}{\phi_{G/N}(t)}$ is precisely the number of t-tuples $(n_1, \ldots, n_t) \in N^t$ such that $G = \langle g_1 n_1, \ldots, g_t n_t\rangle$. In our particular case $P_{g_1,g_2}(S) = P_{G,S}(2)$, where $G = \langle g_1, g_2, S\rangle$.

Now define $P(S)$ to be the probability that two randomly chosen elements of $\mathrm{Aut}\, S$ generate a subgroup containing S. We want to compare $P(S)$ with $P_S(2)$. Note that

$$P(S) = \sum_{(g_1,g_2)\in(\mathrm{Aut}\, S)^2} \frac{P_{g_1,g_2}(S)}{|\mathrm{Aut}\, S|^2},$$

i.e. $P(S)$ is the average of the numbers $P_{g_1,g_2}(S)$. So our question is how much the numbers $P_{g_1,g_2}(S)$, and in particular $P_S(2) = P_{1,1}(S)$, can differ from their average $P(S)$.

In the particular case when $|\mathrm{Aut}\, S : S| = 2$ then $\langle g_1, g_2, S\rangle$ is either S or $\mathrm{Aut}\, S$; since $P_{\mathrm{Aut}\, S/S}(2) = 3/4$, we obtain

$$P(S) = \frac{P_{S,S}(2)}{4} + \frac{3P_{\mathrm{Aut}\, S,S}(2)}{4}.$$

Looking at two examples, Alt(5) and PSL(2, 7), we get the following numbers:

S	$P_{S,S}(2)$	$P_{\mathrm{Aut}\, S,S}(2)$	$P(S)$
Alt(5)	19/30	19/30	19/30
PSL(2, 7)	19/28	23/28	22/28

These examples show that in some cases the two numbers $P(S)$ and $P_S(2)$ coincide, in other cases they can be different. In this paper we try to explain these phenomena, and in particular we study the case when $S = \mathrm{PSL}(2, p)$ proving

THEOREM 1. *If p is a prime number, $p \geq 5$, and $S = PSL(2, p)$ then*

$$P(S) = P_S(2) + \frac{x}{|S|}$$

where

$$\begin{cases} x = 0 & \text{if either } p = 5 \text{ or } p \equiv \pm 2 \mod 5 \text{ and } p \equiv \pm 3 \mod 8; \\ x = 18 & \text{if } p \equiv \pm 2 \mod 5 \text{ and } p \equiv \pm 1 \mod 8; \\ x = 57 & \text{if } p \equiv \pm 1 \mod 5 \text{ and } p \equiv \pm 3 \mod 8; \\ x = 75 & \text{if } p \equiv \pm 1 \mod 5 \text{ and } p \equiv \pm 1 \mod 8. \end{cases}$$

A related question is the following: if $S \trianglelefteq G \leq \mathrm{Aut}\, S$ and S is a finite nonabelian simple group we define $\psi_G(u)$ as follows:

$$\psi_G(u) = \frac{\phi_G(u)}{\phi_{G/S}(u)} \frac{1}{|C_{\mathrm{Aut}\, S}(G/S)|}.$$

The interest in this number comes from the following remarks: for any positive integer t define

$$G_t = \{(g_1, \ldots, g_t) \in G^t \mid g_1 \equiv \cdots \equiv g_t \bmod S\}.$$

We want to study the growth sequence $\{d(G_t)\}_{t\in\mathbb{N}}$ of the minimal numbers of generators of groups G_t. By **[2]** Corollary 8, when $u \geq 2$ we have $d(G_t) \leq u$ if and only if $t \leq \psi_G(u)$. Suppose that $S \trianglelefteq X$, $Y \leq \mathrm{Aut}\, S$; if we want to compare the two growth sequences $\{d(X_t)\}_{t\in\mathbb{N}}$ and $\{d(Y_t)\}_{t\in\mathbb{N}}$ we need to compare the two functions ψ_X and ψ_Y; in the particular case when $\mathrm{Aut}\, S/S$ is cyclic of prime order we want to compare $\psi_S(u) = \frac{\phi_S(u)}{|\mathrm{Aut}\, S|}$ and $\psi_{\mathrm{Aut}\, S}(u) = \frac{\phi_{\mathrm{Aut}\, S}(u)}{\phi_{\mathrm{Aut}\, S/S}(u)|\mathrm{Aut}\, S|}$.

When $S = \mathrm{PSL}(2, p)$ and $G = \mathrm{Aut}\, \mathrm{PSL}(2, p)$ we will see in Section 2, Theorem 7, that there are only four possible behaviors for the difference $\psi_{\mathrm{Aut}\, S}(u) - \psi_S(u)$, depending, as in Theorem 1, on the congruence properties of the prime p modulo 5 and 8; in all the cases we find that $\psi_G(n) \geq \psi_S(n)$ for any positive integer n; this implies that $0 \leq d(S_t) - d(G_t) \leq 1$. For any n, $\psi_G(n) - \psi_S(n)$ is the cardinality of the

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

set $X_n = \{t \in \mathbb{N} \mid d(G_t) = n, d(S_t) = n+1\}$; for example the only possible values for $|X_2|$ are 0, 12, 38, 50 (again depending on the values of p modulo 5 and 8).

2. Some preliminaries. Let us recall that the Möbius function is defined by the rules: $\mu_G(G) = 1$ and $\sum_{H \le K} \mu_G(K) = 0$ for every proper subgroup H of G. A well known result, due to P. Hall **[5]**, says that, for any finite group G,

$$\phi_G(t) = \sum_{H \le G} \mu_G(H)|H|^t.$$

In a similar way $\phi_G(t)/\phi_{G/N}(t)$ can be computed.

LEMMA 2. *If N is a normal subgroup of a finite group G and G/N can be generated by t elements then*

$$\frac{\phi_G(t)}{\phi_{G/N}(t)} = \sum_{H \le G} \mu_G(H)\epsilon(H)|H \cap N|^t$$

where $\epsilon(H) = 1$ if $HN = G$, $\epsilon(H) = 0$ otherwise.

Proof. Choose $g_1, \dots, g_t$ generating G modulo N; for any $H \le G$ let m_H be the cardinality of the set $\{(n_1, \dots, n_t) \in N^t \mid \langle g_1 n_1, \dots, g_t n_t\rangle = H\}$. Note that $\sum_{K \le H} m_K$ is the cardinality of $\Omega = \{(n_1, \dots, n_t) \in N^t \mid \langle g_1 n_1, \dots, g_t n_t\rangle \le H\}$; it can be easily seen that Ω is empty if and only if $HN \ne G$; moreover $(n_1, \dots, n_t)$ and $(\bar{n}_1, \dots, \bar{n}_t)$ are both elements of Ω if and only if $n_i \bar{n}_i^{-1} \in H \cap N$ for $1 \le i \le t$; hence $\sum_{K \le H} m_K = \epsilon(H)|H \cap N|^t$. Therefore by Möbius inversion formula

$$\frac{\phi_G(t)}{\phi_{G/N}(t)} = m_G = \sum_{H \le G} \left(\mu_G(H) \sum_{K \le H} m_K \right) = \sum_{H \le G} \mu_G(H)\epsilon(H)|H \cap N|^t.$$

□

We want to apply the previous lemma when $S \trianglelefteq G \le \operatorname{Aut} S$, with S a finite nonabelian simple group. Our aim is to compare the values of $\phi_G(2)/\phi_{G/S}(2)$ for different choices of G. To do that it is useful to rewrite the previous formula in the form $\phi_G(t)/\phi_{G/N}(t) = \sum_{H \le N} a_H |H|^t$, for suitable coefficients a_H.

From the definition of the Möbius function, the following lemma can be easily deduced.

LEMMA 3. *If $H_1 \le H_2 < G$ then $\sum_{K \le G, K \cap H_2 = H_1} \mu_G(K) = 0$.*

Proof. Fix H_2. If $H_1 = H_2$ then the assertion holds. Now take H_1, and assume the result true for all subgroups of H_2 strictly containing H_1. Therefore

$$\sum_{H_1 < X \le H_2} \left(\sum_{K \le G, K \cap H_2 = X} \mu_G(K) \right) = 0.$$

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

Moreover

$$\sum_{K\leq G, K\cap H_2=H_1}\mu_G(K)+\sum_{H_1<X\leq H_2}\left(\sum_{K\leq G, K\cap H_2=X}\mu_G(K)\right)=\sum_{H_1\leq K}\mu_G(K)=0.$$

This proves the lemma. □

LEMMA 4. *If N is a normal subgroup of G then*

$$\frac{\phi_G(t)}{\phi_{G/N}(t)}=\sum_{H\leq N}\left(\sum_{K\cap N=H, KN=G}\mu_G(K)\right)|H|^t=\sum_{H\leq N}\left(-\sum_{K\cap N=H, KN\neq G}\mu_G(K)\right)|H|^t.$$

Proof. The first equality is a trivial consequence of Lemma 2, the second follows from Lemma 3. □

In the particular case when N is a maximal subgroup of G (i.e. G/N is cyclic of prime order), from the previous lemma we deduce.

LEMMA 5. *If N is a normal subgroup of G and G/N has prime order then*

$$\frac{\phi_G(t)}{\phi_{G/N}(t)}=-\sum_{H\leq N}\mu_G(H)|H|^t.$$

Proof. It follows immediately from the second equality in Lemma 4. Suppose that $H\leq N$, $K\cap N=H$ and $KN\neq G$; it must be $K\leq N$, hence $K=H$. □

COROLLARY 6. *If N is a normal subgroup of G and G/N has prime order then*

$$\phi_N(t)-\frac{\phi_G(t)}{\phi_{G/N}(t)}=\sum_{H\leq N}(\mu_N(H)+\mu_G(H))|H|^t.$$

3. PSL(2, *p*). In this section suppose that p is a prime, $p\geq 5$, $S=\mathrm{PSL}(2,p)$ and $G=\mathrm{Aut}\,S$. Since S and G are the only subgroups of $\mathrm{Aut}\,S$ containing S, our question about $P(S)$ reduces to comparing $\phi_S(2)$ and $\phi_{G/S}(2)$. This can be done using Corollary 6.

It was already known by P. Hall [**5**] that the values of the Möbius function μ_S on the subgroups of S only depend on the congruence properties of the prime p modulo 5 and 8. This remains true for the values of μ_G. Four cases must be distinguished:

a) either $p=5$ or $p\equiv\pm 2 \mod 5$ and $p\equiv\pm 3 \mod 8$;
b) $p\equiv\pm 2 \mod 5$ and $p\equiv\pm 1 \mod 8$;
c) $p\equiv\pm 1 \mod 5$ and $p\equiv\pm 3 \mod 8$;
d) $p\equiv\pm 1 \mod 5$ and $p\equiv\pm 1 \mod 8$.

For each of these cases we describe the values of $\mu_G(H)$ and $\mu_S(H)$ for $H\leq G$. More precisely we write a table in which any row corresponds to a subgroup H of S for which either $\mu_S(H)\neq 0$ or $\mu_G(H)\neq 0$; we give also the order of H and the number i_H of subgroups of S isomorphic to H. In this way all the information needed to apply Corollary 6 can be read from these tables. For convenience we write $\frac{1}{2}(p-1)=q$, $\frac{1}{2}(p+1)=r$, $g=2pqr=|S|$; moreover s is either q or r according as $p\equiv\pm 1 \mod 3$

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

and t is either q or r according as $p \equiv \pm 1 \bmod 4$. The notation for subgroups is quite standard. We just observe that M_{pq} is the semidirect product $[C_p]C_{\frac{p-1}{2}}$ and E_4 is the Vier group $C_2 \times C_2$.

a) either $p = 5$ or $p \equiv \pm 2 \mod 5$ and $p \equiv \pm 3 \mod 8$.

We have

H	$\mu_S(H)$	$\mu_G(H)$	$\lvert H\rvert$	i_H
S	1	-1	g	1
D_{2r}	-1	1	$2r$	pq
D_{2q} ($p \neq 5$)	-1	1	$2q$	pr
M_{pq}	-1	1	pq	$2r$
C_q ($p \neq 5$)	2	-2	q	pr
A_4	-1	1	12	$g/12$
E_4 ($p \neq 5$)	3	-3	4	$g/12$
C_3	$2s/3$	$-2s/3$	3	$g/2s$
C_2	t (4 if $p = 5$)	$-t$ (-4 if $p = 5$)	2	$g/2t$
1	$-g$	g	1	1

Note that $\mu_G(H) + \mu_S(H) = 0$ for any $H \leq G$; so in particular $\phi_S(2) = \phi_G(2)/\phi_{G/S}(2)$.

b) $p \equiv \pm 2 \mod 5$ and $p \equiv \pm 1 \mod 8$.

We have

H	$\mu_S(H)$	$\mu_G(H)$	$\lvert H\rvert$	i_H
S	1	-1	g	1
D_{2r} ($p \neq 7$)	-1	1	$2r$	pq
D_{2q} ($p \neq 7$)	-1	1	$2q$	pr
M_{pq}	-1	1	pq	$2r$
C_q	2	-2	q	pr
S_4	-1	0	24	$g/12$
D_8	2 (1 if $p = 7$)	0 (1 if $p = 7$)	8	$g/8$
S_3	2 (1 if $p = 7$)	0 (1 if $p = 7$)	6	$g/6$
C_2	$-t$	$-t$	2	$g/2t$

In particular, in all cases, we deduce

$$\begin{aligned}\phi_S(2) - \frac{\phi_G(2)}{\phi_{G/S}(2)} &= \sum_{H \leq S} (\mu_S(H) + \mu_G(H))|H|^2 \\ &= -1|S_4|^2 \frac{g}{12} + 2|D_8|^2 \frac{g}{8} + 2|S_3|^2 \frac{g}{6} - 2t|C_2|^2 \frac{g}{2t} \\ &= (-48 + 16 + 12 - 4)g = -24g.\end{aligned}$$

c) $p \equiv \pm 1 \mod 5$ and $p \equiv \pm 3 \mod 8$.

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

We have

H	$\mu_S(H)$	$\mu_G(H)$	$\lvert H\rvert$	i_H
S	1	-1	g	1
D_{2r}	-1	1	$2r$	pq
D_{2q} $(p \neq 11)$	-1	1	$2q$	pr
M_{pq}	-1	1	pq	$2r$
C_q	2	-2	q	pr
A_5	-1	0	60	$g/30$
A_4	1	1	12	$g/12$
D_{10}	2 (1 if $p = 11$)	0 (1 if $p = 11$)	10	$g/10$
S_3	2	0	6	$g/6$
E_4	3	-3	4	$g/12$
C_3	$-2s/3$	$-2s/3$	3	$g/2s$
C_2	$-3t$	$-t$	2	$g/2t$
1	g	g	1	1

In particular, in all cases, we deduce

$$\begin{aligned}\phi_S(2) - \frac{\phi_G(2)}{\phi_{G/S}(2)} &= \sum_{H \leq S} (\mu_S(H) + \mu_G(H))|H|^2 \\ &= -1|A_5|^2\frac{g}{30} + 2|A_4|^2\frac{g}{12} + 2|D_{10}|^2\frac{g}{10} + 2|S_3|^2\frac{g}{6} + \\ &\quad - 4t|C_2|^2\frac{g}{2t} - \frac{4s}{3}|C_3|^2\frac{g}{2s} + 2g \\ &= g(-120 + 24 + 20 + 12 - 8 - 6 + 2) = -76g.\end{aligned}$$

d) $p \equiv \pm 1 \mod 5$ and $p \equiv \pm 1 \mod 8$.

H	$\mu_S(H)$	$\mu_G(H)$	$\lvert H\rvert$	i_H
S	1	-1	g	1
D_{2r}	-1	1	$2r$	pq
D_{2q}	-1	1	$2q$	pr
M_{pq}	-1	1	pq	$2r$
C_q	2	-2	q	pr
A_5	-1	0	60	$g/30$
S_4	-1	0	24	$g/12$
A_4	2	0	12	$g/12$
D_{10}	2	0	10	$g/10$
D_8	2	0	8	$g/8$
S_3	4	0	6	$g/6$
C_3	$-4s/3$	0	3	$g/2s$
C_2	$-5t$	$-t$	2	$g/2t$
1	$2g$	0	1	1

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

In particular we deduce

$$\begin{aligned}\phi_S(2) - \frac{\phi_G(2)}{\phi_{G/S}(2)} &= \sum_{H \le S} (\mu_S(H) + \mu_G(H))|H|^2 \\ &= -1|A_5|^2\frac{g}{30} - 1|S_4|^2\frac{g}{12} + 2|A_4|^2\frac{g}{12} + 2|D_{10}|^2\frac{g}{10} \\ &\quad + 2|D_8|^2\frac{g}{8} + 4|S_3|^2\frac{g}{6} - \frac{4s}{3}|C_3|^2\frac{g}{2s} - 6t|C_2|^2\frac{g}{2t} + 2g \\ &= g(-120 - 48 + 24 + 20 + 16 + 24 - 6 - 12 + 2) = -100g.\end{aligned}$$

Proof of Theorem 1. We have seen that

$$\frac{\phi_G(2)}{\phi_{G/S}(2)} = \phi_S(2) + y|S|,$$

with $y = 0$ in case a), $y = 24$ in case b), $y = 76$ in case c), $y = 100$ in case d). Therefore

$$\begin{aligned}P(S) &= \frac{P_{S,S}(2)}{4} + \frac{3P_{\mathrm{Aut}\,S,S}(2)}{4} = \frac{\phi_S(2) + 3\phi_G(2)/\phi_{G/S}(2)}{4|S|^2} \\ &= \frac{\phi_S(2) + 3(\phi_S(2) + y|S|)}{4|S|^2} = \frac{4\phi_S(2) + 3y|S|}{4|S|^2} = P_S(2) + \frac{3}{4}\frac{y}{|S|}.\end{aligned}$$

□

THEOREM 7. *For any integer n, $\psi_{\mathrm{Aut}\,\mathrm{PSL}(2,p)}(n) \ge \psi_{\mathrm{PSL}(2,p)}(n)$. Moreover the function $f(n) = \psi_{\mathrm{Aut}\,\mathrm{PSL}(2,p)}(n) - \psi_{\mathrm{PSL}(2,p)}(n)$ depends only on the congruence properties of the prime p modulo 5 and 8. More precisely $f = f_a, f_b, f_c$ or f_d in case a, b, c, d where*

$$\begin{aligned}f_a(n) &= 0, \\ f_b(n) &= 24^{n-1} - 8^{n-1} - 6^{n-1} + 2^{n-1}, \\ f_c(n) &= 60^{n-1} - 12^{n-1} - 10^{n-1} - 6^{n-1} + 3^{n-1} + 2 \cdot 2^{n-1} - 1, \\ f_d(n) &= 60^{n-1} + 24^{n-1} - 12^{n-1} - 10^{n-1} - 8^{n-1} - 2 \cdot 6^{n-1} + 3^{n-1} + 3 \cdot 2^{n-1} - 1.\end{aligned}$$

Proof. By Corollary 6

$$\begin{aligned}f(n) &= \psi_{\mathrm{Aut}\,\mathrm{PSL}(2,p)}(n) - \psi_{\mathrm{PSL}(2,p)}(n) \\ &= \frac{1}{|\mathrm{Aut}\,\mathrm{PSL}(2,p)|}\left(\frac{\phi_{\mathrm{Aut}\,\mathrm{PSL}(2,p)}(n)}{\phi_{\mathrm{Aut}\,\mathrm{PSL}(2,p)/\mathrm{PSL}(2,p)}(n)} - \phi_{\mathrm{PSL}(2,p)}(n)\right) \\ &= \frac{1}{|\mathrm{Aut}\,\mathrm{PSL}(2,p)|}\left(-\sum_{H \le \mathrm{PSL}(2,p)} \left(\mu_{\mathrm{PSL}(2,p)}(H) + \mu_{\mathrm{Aut}\,\mathrm{PSL}(2,p)}(H)\right)|H|^n\right)\end{aligned}$$

so the conclusion follows from the previous tables. □

A curious and unexpected fact is that $f_d = f_b + f_c$; we will try to explain this phenomenon and more generally the behavior of these functions in the next section, but first we want to look at some other examples.

4. Other simple groups. We have seen in the previous section that if $S = \mathrm{PSL}(2, p)$ then $\psi_S(n) \le \psi_{\mathrm{Aut}\,S}(n)$ for any n; this is true for many other simple groups. In the following tables we compare the values of $\psi_S(2)$ and $\psi_{\mathrm{Aut}\,S}(2)$ in some examples (these numbers may be found using GAP [**3**]):

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

n	$\psi_{\mathrm{Alt}(n)}(2)$	$\psi_{\mathrm{Sym}(n)}(2)$
5	19	19
6	53	53
7	916	1030
8	7748	8222
9	77015	78293
10	793827	793827
11	8918988	8925974

S	$\psi_S(2)$	$\psi_{\mathrm{Aut}\,S}(2)$
PSL(2, 8)	142	142
PSL(2, 16)	939	939
PSU(4, 2)	11505	11505
M_{12}	38664	46578
M_{22}	206294	208088
J_2	296579	296591
J_3	25103957	25107135

The previous examples lead one to conjecture that $\psi_S(n) \leq \psi_{\mathrm{Aut}\,S}(n)$ for any finite nonabelian simple group S, or at least for the simple groups S satisfying $|\mathrm{Aut}\,S : S| = 2$. But this is false; namely we have

S	$\psi_S(2)$	$\psi_{\mathrm{Aut}\,S}(2)$
PSU(3, 3)	2784	2772

In particular this implies $2 = d(\mathrm{PSU}(3,3)_{2773}) < d(\mathrm{Aut}\,\mathrm{PSU}(3,3)_{2773}) = 3$.

Many questions are suggested from the previous tables; for example

- For which values of n does one obtain

$$P_{\mathrm{Sym}(n),\mathrm{Alt}(n)}(u) = P_{\mathrm{Alt}(n)}(u)?$$

- Find conditions on S and $\mathrm{Aut}\,S$ in order that $P_S(u) = P_{\mathrm{Aut}\,S,S}(u)$.
- Can we find $S \leq Y_1, Y_2 \leq \mathrm{Aut}\,S$, $u_1, u_2 \in \mathbb{N}$ with $\psi_{Y_1}(u_1) > \psi_{Y_2}(u_1)$ and $\psi_{Y_1}(u_2) < \psi_{Y_2}(u_2)$?

We have no answers for these questions, but we want to give some remarks related to them.

If S is a nonabelian simple group, $S \leq G \leq \mathrm{Aut}\,S$ and G/S has prime order then, by Corollary 6

$$(P_S(u) - P_{G,S}(u))|S|^u = \sum_{H \leq S} (\mu_S(H) + \mu_G(H))|H|^u. \tag{4.1}$$

In particular we have

COROLLARY 8. *Suppose that S is a nonabelian simple group, $S \leq G \leq \mathrm{Aut}\,S$ and G/S has prime order; then $P_S(u) = P_{G,S}(u)$ if $\mu_S(H) + \mu_G(H) = 0$ for any $H \leq S$.*

It is difficult to say in which cases $\mu_S(H) + \mu_G(H) = 0$ for any $H \leq S$; however some remarks about this question can be deduced from the following lemma.

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

LEMMA 9. *Let X be a proper subgroup of a finite group Y.*

1) *Then $\mu_Y(X) \neq 0$ only if X is an intersection of maximal subgroups of Y.*
2) *Suppose that $\{M_1, \ldots, M_n\}$ is the set of maximal subgroups of Y containing X and that $X = M_1 \cap \cdots \cap M_n$. For $1 \leq i \leq n$ define $\lambda_{i,Y}(X)$ as the cardinality of the set $A_{i,Y}(X) = \{(M_{j_1}, \ldots, M_{j_i}) \mid j_1 < \cdots < j_i \text{ and } X = M_{j_1} \cap \cdots \cap M_{j_i}\}$. Then $\mu_Y(X) = \sum_{1 \leq i \leq n} (-1)^i \lambda_{i,Y}(X)$.*

Proof. 1) See [**5**]. 2) Let us consider the function defined by $\nu_Y(Y) = 1$ and

$$\nu_Y(X) = \sum_{1 \leq i \leq n} (-1)^i \lambda_{i,Y}(X),$$

if X is a proper subgroup of Y. We show that $\nu_Y(X) = \mu_Y(X)$; since by definition, $\nu_Y(Y) = 1$, we just have to prove that

$$\sum_{K \geq X} \nu_Y(K) = 1 + \sum_{1 \leq i \leq n} (-1)^i \left(\sum_{K > X} \lambda_{i,Y}(K) \right) = 0, \qquad (*)$$

for $X < Y$. Let $A = \{M_1, \ldots, M_n\}$ be the set of maximal subgroups of Y containing X so that $X = M_1 \cap \cdots \cap M_n$. We observe that, for each $i \in \{1, \ldots, n\}$, the intersection of i subgroups in A is a subgroup $K \geq X$, and each subgroup of Y containing X is obtained in this way. So the summands in $(*)$ are exactly the elements of the n-row in Tartaglia-triangle and it is well known that

$$\sum_{0 \leq i \leq n} (-1)^i \frac{n!}{i!(n-i)!} = 0. \qquad \square$$

We say that H is a good subgroup of S if

(1) for any maximal subgroup M of G containing H, we have that $M \cap S$ is a maximal subgroup of S;

(2) when $M_1, \ldots, M_r$ are maximal subgroups of G and $H = \cap_{1 \leq i \leq r} M_i$ then one of the M_i coincides with S.

Suppose that H is a good subgroup of S. If H is an intersection of maximal subgroups of G, then it is also an intersection of maximal subgroups of S. In that case if $S, M_1, \ldots, M_r$ are the maximal subgroups of G containing H then $S \cap M_1, \ldots, S \cap M_r$ are the maximal subgroups of S containing H. Moreover if $(S, M_{j_1}, \ldots, M_{j_i}) \in A_{i+1,G}(H)$ then $(S \cap M_{j_1}, \ldots, S \cap M_{j_i}) \in A_{i,S}(H)$, hence $\lambda_{i,S}(H) = \lambda_{i+1,G}(H)$. So, from Lemma 9, we deduce that if H is a good subgroup of S then $\mu_S(H) + \mu_G(H) = 0$.

When $S = \mathrm{PSL}(2, p)$ and either $p = 5$ or $p \equiv \pm 2 \bmod 5$ and $p \equiv \pm 3 \bmod 8$ (case a), then any $1 < H < S$ is good. Moreover $\mu_S(S) = 1 = -\mu_G(S)$. Since

$$\phi_S(1) = \sum_{H \leq S} \mu_S(H)|H| = 0 \quad \text{and} \quad \frac{\phi_G(1)}{\phi_{G/S}(1)} = \sum_{H \leq S} \mu_G(H)|H| = 0,$$

we have also $\mu_S(1) + \mu_G(1) = 0$. This explains how $f_a = 0$ in Theorem 7. In case b, there is a maximal subgroup M isomorphic to Sym(4) which is not good while the subgroups of S not contained in a conjugate of M are good. So the computation of $f_b(n)$ depends only on the values of $(\mu_S(H) + \mu_G(H))|H|^n$ for H contained in a maximal subgroup isomorphic to Sym(4). Similarly, in case c, S has a maximal subgroup M isomorphic to Alt(5) which is not good and $f_c(n)$ depends only on the values of $(\mu_S(H) + \mu_G(H))|H|^n$ for H contained in a conjugate of this maximal subgroup M. In case d, S has a maximal subgroup isomorphic to Sym(4) and a maximal subgroup isomorphic to Alt(5), both these maximal subgroups are not good and $f_d = f_b + f_c$.

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

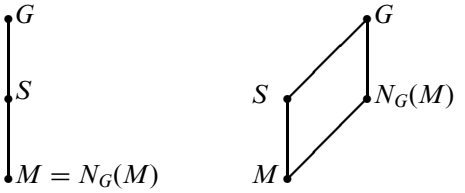
The example of $\mathrm{PSL}(2,p)$ could suggest that in order to study the difference $\psi_G(n) - \psi_S(n)$ it suffices to know which maximal subgroups of G are not good. However this is not true. We try now to say something about that.

One can think to approximate $P_S(u) - P_{G,S}(u)$ substituting the exact value given by (4.1), with

$$\mathcal{P}(u) = \sum_{M \max S} \frac{(\mu_S(M) + \mu_G(M))|M|^u}{|S|^u},$$

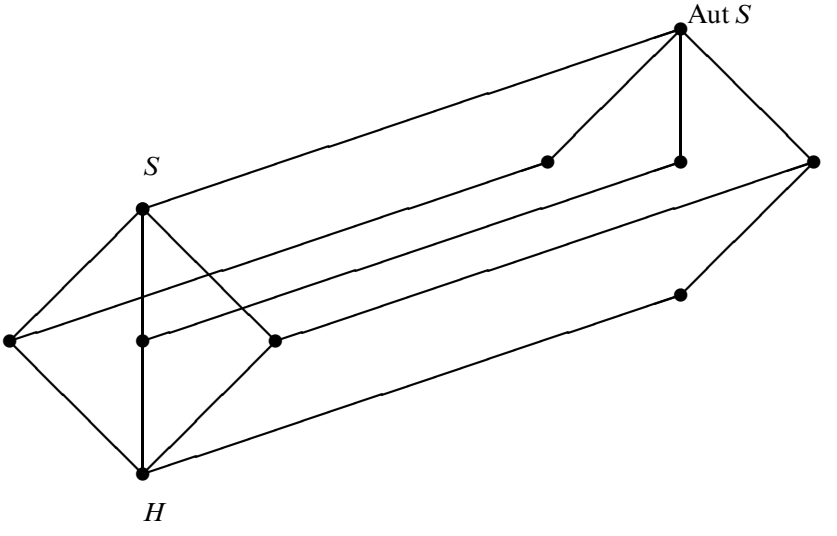
when only the contribution due to the maximal subgroups is considered.

If M is a maximal subgroup of S, the lattice of the subgroups of G containing M is one of the following:



If $M \neq N_G(M)$ then $\mu_S(M) = -1$, $\mu_G(M) = 1$ and $(\mu_S(M) + \mu_G(M)) = 0$; if $M = N_G(M)$ then $\mu_S(M) = -1$, $\mu_G(M) = 0$ and $(\mu_S(M) + \mu_G(M)) = -1$. Therefore $\mathcal{P}(u) \leq 0$. Moreover $\mathcal{P}(u) < 0$ if and only if there exists a maximal subgroup M of S with $M = N_G(M)$. This suggests that if there is a maximal subgroup M of S with $M = N_G(M)$ then $P_S(u) < P_{G,S}(u)$.

However if $G = SN_G(M)$ for any maximal subgroup M of S, (i.e. if all maximal subgroups of G are good) then $\mathcal{P}(u) = 0$ and the contribution of the "smaller subgroups" in the sum is important. For example if $S = \mathrm{PSU}(3,3)$ and $G = \mathrm{Aut}\, S$, then all the maximal subgroups of G are good. However there exists a 2-maximal subgroup H of S ($H \cong \mathrm{Sym}(4)$) such that the lattice of subgroups of G containing H is



Therefore $\mathcal{P}(u) = 0$ but H is not a good subgroup (H coincides with the intersection of the three maximal subgroups of G containing H but not S) and $\mu_S(H) - \mu_G(H) = 2 - 0 > 0$. This explains why $\psi_{\mathrm{PSU}(3,3)}(2) > \psi_{\mathrm{Aut}\,\mathrm{PSU}(3,3)}(2)$.

https://doi.org/10.1017/S0017089503001241 Published online by Cambridge University Press

REFERENCES

1. F. Dalla Volta and A. Lucchini, Generation of almost simple groups, *J. Algebra* **178** (1995), 194–223.

2. F. Dalla Volta, A. Lucchini and F. Morini, On the probability of generating a minimal d-generated group, *J. Austral. Math. Soc.* **71** (2001), 177–185.

3. The GAP group, GAP – Groups, Algorithms and Programming, Version 4.2 (Aachen, St. Andrews, 1999).

4. W. Gaschütz, Zu einem von B.H. und H. Neumann gestellten Problem, *Math. Nachr.* **14** (1955), 249–252.

5. P. Hall, The Eulerian function of a group, *Quart. J. Math. Oxford* **7** (1936), 134–151.