Università degli Studi di Padova

Padua Research Archive - Institutional Repository

The expected number of random elements to generate a finite group

Original Citation:

Availability:

This version is available at: 11577/3210788 since: 2016-11-18T17:57:15Z

Publisher:

Springer-Verlag Wien

Published version:

DOI: 10.1007/s00605-015-0789-5

Terms of use:

Open Access

This article is made available under terms and conditions applicable to Open Access Guidelines, as described at <http://www.unipd.it/download/file/fid/55401> (Italian only)

(Article begins on next page)

THE EXPECTED NUMBER OF RANDOM ELEMENTS TO GENERATE A FINITE GROUP

ANDREA LUCCHINI

ABSTRACT. We will see that the expected number of elements of a finite group G which have to be drawn at random, with replacement, before a set of generators is found, can be determined using the Möbius function defined on the subgroup lattice of G . We will discuss several applications of this result.

1. INTRODUCTION

Let G be a nontrivial finite group and let $x = (x_n)_{n \in \mathbb{N}}$ be a sequence of independent, uniformly distributed G -valued random variables. We may define a random variable τ_G (a waiting time) by

$$\tau_G = \min\{n \geq 1 \mid \langle x_1, \dots, x_n \rangle = G\} \in [1, +\infty].$$

Notice that $\tau_G > n$ if and only if $\langle x_1, \dots, x_n \rangle \neq G$, so we have

$$P(\tau_G > n) = 1 - P_G(n),$$

denoting by

$$P_G(n) = \frac{|\{(g_1, \dots, g_n) \in G^n \mid \langle g_1, \dots, g_n \rangle = G\}|}{|G|^n}$$

the probability that n randomly chosen elements of G generate G . We denote by $e_1(G)$ the expectation $E(\tau_G)$ of this random variable. In other word $e_1(G)$ is the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. Clearly we have:

$$\begin{aligned} (1.1) \quad e_1(G) &= \sum_{n \geq 1} n P(\tau_G = n) = \sum_{n \geq 1} \left(\sum_{m \geq n} P(\tau_G = m) \right) \\ &= \sum_{n \geq 1} P(\tau_G \geq n) = \sum_{n \geq 0} P(\tau_G > n) = \sum_{n \geq 0} (1 - P_G(n)). \end{aligned}$$

If $G = C_p$ is a cyclic group of prime order p , then τ_G is a geometric random variable with parameter $\frac{p-1}{p}$, so $e_1(C_p) = \frac{p}{p-1}$. But if we consider a group G with a richer subgroup structure, the computation of $e_1(G)$ appears to be more complicated. Consider for example the dihedral group $G = D_{2p}$ of order $2p$, with p an odd prime: then $\langle g_1, \dots, g_n \rangle = G$ if and only if there exist $1 \leq i < j \leq n$ such that $g_i \neq 1$ and $g_j \notin \langle g_i \rangle$. We may think that we are repeating independent trials (choices of an element from G in a uniform way). The number of trials

1991 *Mathematics Subject Classification.* 20P05.

Key words and phrases. groups generation; waiting time; permutations groups; profinite groups.

Partially supported by Università di Padova (Progetto di Ricerca di Ateneo: "Invariable generation of groups").

needed to obtain a nontrivial element x of G is a geometric random variable with parameter $\frac{2p-1}{2p}$: its expectation is equal to $E_0 = \frac{2p}{2p-1}$. With probability $p_1 = \frac{p}{2p-1}$, the nontrivial element x has order 2: in this case the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2p-2}{2p}$ and expectation $E_1 = \frac{2p}{2p-2}$; on the other hand, with probability $p_2 = \frac{p-1}{2p-1}$, the nontrivial element x has order p : in this second case the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2p-p}{2p}$ and expectation $E_2 = \frac{2p}{2p-p}$. This implies

$$(1.2) \quad e_1(D_{2p}) = E_0 + p_1 E_1 + p_2 E_2 = 2 + \frac{2p^2}{(2p-1)(2p-2)}.$$

Let $d(G)$ be the smallest cardinality of a generating set in G and call

$$ex(G) = e_1(G) - d(G)$$

the excess of G . From the results of Kantor and Lubotzky [8] the numbers $ex(G)$ are unbounded in general. Indeed they proved that for every positive real number ϵ and every positive integer k there exists a 2-generated finite group $G_{\epsilon,k}$ with $P_{G_{\epsilon,k}}(t) \leq \epsilon$ for every $t \leq k$: hence, by (1.1),

$$e_1(G_{\epsilon,k}) \geq \sum_{0 \leq t \leq k} (1 - P_{G_{\epsilon,k}}(t)) \geq (k+1)(1 - \epsilon) \text{ and } ex(G_{\epsilon,k}) \geq (k+1)(1 - \epsilon) - 2.$$

Pomerance [19] computed the excess $ex(G)$ for any finite abelian group G . Pak studied a closely related invariant: he defined $\nu(G) = \min\{k \in |P_G(k) \geq e^{-1}|\}$ and conjectured that $\nu(G) = O(d(G) \log \log |G|)$. Notice that an easy argument (see for example Lemma 19) implies that $e_1(G) \leq e\nu(G)$. Lubotzky [11] and, independently, Detomi and the author [2, Theorem 20] proved Pak's conjecture in a stronger form: $\nu(G) = d(G) + O(\log \log |G|)$.

We suggest in this note a different approach to the study of $e_1(G)$ and $ex(G)$. In particular we will see that these numbers can be directly determined using the Möbius function defined on the subgroup lattice of G by setting $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H < K} \mu_G(K)$ for any $H < G$. As was noticed by P. Hall [7], using the Möbius inversion formula it can be proved that

$$(1.3) \quad P_G(t) = \sum_{H \leq G} \frac{\mu_G(H)}{|G : H|^t}.$$

Combining (1.1) and (1.3) we will obtain:

Theorem 1. *If G is a nontrivial finite group, then*

$$e_1(G) = - \sum_{H < G} \frac{\mu_G(H)|G|}{|G| - |H|}.$$

Theorem 2. *If G is a nontrivial finite group, then*

$$ex(G) = e_1(G) - d(G) = - \sum_{H < G} \frac{\mu_G(H)}{|G : H|^{d(G)}} \frac{|G|}{|G| - |H|}.$$

Other numerical invariants may be derived from τ_G starting from the higher moments

$$E(\tau_G^k) = \sum_{n \geq 1} n^k P(\tau_G = n).$$

In particular it is probabilistically important, when the expectation of a random variable is known, to have control over its second moment. We will denote by $e_2(G)$ the second moment $E(\tau_G^2)$ and by $\text{var}(\tau_G) = e_2(G) - e_1(G)^2$ the variance of τ_G .

Theorem 3. *If G is a finite group, then*

$$e_2(G) = - \sum_{H < G} \frac{\mu_G(H)|G|(|G| + |H|)}{(|G| - |H|)^2}.$$

We can use Theorem 1 to deduce in a different way the formula (1.2) giving $e_1(G)$ when $G = D_{2p}$ is the dihedral group of order $2p$ and p is an odd prime. The proper subgroups of G are the following:

- $H = 1$; in this case $\mu_G(H) = p$.
- H is the unique Sylow p -subgroup; in this case $\mu_G(H) = -1$.
- H is a Sylow 2-subgroup: in this case $\mu_G(H) = -1$.

Since D_{2p} contains exactly p subgroups of order 2 we conclude:

$$\begin{aligned} e_1(D_{2p}) &= -\frac{p \cdot 2p}{2p-1} + \frac{2p}{2p-p} + \frac{p \cdot 2p}{2p-2} = 2 + \frac{2p^2}{(2p-1)(2p-2)}, \\ e_2(D_{2p}) &= -\frac{p \cdot 2p \cdot (2p+1)}{(2p-1)^2} + \frac{2p \cdot (2p+p)}{(2p-p)^2} + \frac{p \cdot 2p \cdot (2p+2)}{(2p-2)^2} \\ &= 6 + \frac{2p^2 \cdot (12p^2 - 6p - 2)}{(2p-1)^2(2p-2)^2}. \end{aligned}$$

In particular, when $p = 3$, we deduce:

Example 4. $e_1(\text{Sym}(3)) = 29/10$, $e_2(\text{Sym}(3)) = \frac{249}{25}$, $\text{var}(\tau_{\text{Sym}(3)}) = \frac{31}{20}$.

It turns out that $e_1(D_{2p}), e_2(D_{2p}), \text{var}(D_{2p})$ decrease when p increase and

$$\lim_{p \rightarrow \infty} e_1(D_{2p}) = \frac{5}{2}, \quad \lim_{p \rightarrow \infty} e_2(D_{2p}) = \frac{15}{2}, \quad \text{var}(\tau_{D_6}) = \frac{5}{4}.$$

The Möbius function of the subgroup lattice of a finite group G can be easily computed when the table of marks of G is known [18]. We used the library of Table of Marks in GAP [6] to compute $e_1(G)$ and $e_2(G)$ for several groups of small order. For example we have:

Example 5. $e_1(\text{Alt}(4)) = \frac{163}{66} \sim 2.4697$, $e_2(\text{Alt}(4)) = \frac{7331}{1089} \sim 6.7319$.

Example 6. $e_1(\text{Sym}(4)) = \frac{164317}{53130} \sim 3.0927$, $e_2(\text{Sym}(4)) = \frac{7840917881}{705699225} \sim 11.1108$.

For the symmetric group $\text{Sym}(n)$ and the alternating group $\text{Alt}(n)$, the results of Dixon [4] yield that $e_1(\text{Sym}(n)) = 2.5 + o(1)$ and $e_1(\text{Alt}(n)) = 2 + o(1)$ as $n \rightarrow \infty$. More generally, if S is a nonabelian finite simple group, then $d(S) = 2$ and results of Dixon [4], Kantor-Lubotzky [8] and Liebeck-Shalev [9] establish that $P_S(2) \rightarrow 1$ as $|S| \rightarrow \infty$, so $e_1(S) = 2 + o(|S|)$ as $|S| \rightarrow \infty$. In Section 3 we analyze in more details the behavior of $e_1(S)$ and $e_2(S)$ when S is a nonabelian simple group; in particular it will turn out that the smallest values are assumed when $S = \text{Alt}(6)$.

Theorem 7. *Let S be a finite nonabelian simple group. Then*

$$e_1(S) \leq e_1(\text{Alt}(6)) = \frac{19 \cdot 1289 \cdot 39631 \cdot 5924159}{2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 29 \cdot 59 \cdot 89 \cdot 179 \cdot 359} \sim 2.494,$$

$$e_2(S) \leq e_2(\text{Alt}(6)) = \frac{13 \cdot 1362758815057749534622102868341}{2^3 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 17^2 \cdot 29^2 \cdot 59^2 \cdot 89^2 \cdot 179^2 \cdot 359^2} \sim 6.665.$$

Similarly we will analyse in Section 4 the behavior of $e_1(\text{Sym}(n))$ and $e_2(\text{Sym}(n))$ obtaining:

Theorem 8. *If $n \geq 5$, then $2.5 \leq e_1(\text{Sym}(n)) < e_1(\text{Sym}(6)) \sim 2.8816$ and $e_2(\text{Sym}(n)) < e_2(\text{Sym}(6)) \sim 9.5831$. Moreover*

$$\lim_{n \rightarrow \infty} e_1(\text{Sym}(n)) = 2.5 \text{ and } \lim_{n \rightarrow \infty} e_2(\text{Sym}(n)) = 7.5.$$

In Section 5 we approach a different but related problem: we compute the expected number $E(\tau_n)$ of elements of $\text{Sym}(n)$ which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of $\text{Sym}(n)$ is found. Denote by Π_n the set of partitions of n , i.e. nondecreasing sequences of natural numbers whose sum is n . Given $\omega = (n_1, \dots, n_k) \in \Pi_n$ with

$$n_1 = \dots = n_{k_1} > n_{k_1+1} = \dots = n_{k_1+k_2} > \dots > n_{k_1+\dots+k_{r-1}+1} = \dots = n_{k_1+\dots+k_r}$$

$$\text{define } \mu(\omega) = (-1)^{k-1} (k-1)!, \quad \iota(\omega) = \frac{n!}{n_1! n_2! \dots n_k!}, \quad \nu(\omega) = k_1! k_2! \dots k_r!.$$

Theorem 9. *For every $n \geq 2$ we have*

$$E(\tau_n) = - \sum_{\omega \in \Pi_n^*} \frac{\mu(\omega) \iota(\omega)^2}{\nu(\omega) (\iota(\omega) - 1)},$$

where Π_n^* is the set of partitions of n into at least two subsets.

Corollary 10. *For each $n \geq 2$, we have*

$$2 \leq E(\tau_n) \leq E(\tau_4) \sim 2.1033.$$

We may generalize the definition τ_G , considering, for any proper subgroup K of G , the random variable

$$\tau_{G,K} = \min\{n \geq 1 \mid \langle K, x_1, \dots, x_n \rangle = G\}$$

expressing the number of elements of G which have to be drawn before a set of elements generating G together with the elements of K is found. As noticed in [12], the formula (1.3) can be generalized to a similar formula for the probability $P_G(K, t)$ that t randomly chosen elements from G generate G together with K :

$$(1.4) \quad P_G(K, t) = \sum_{K \subseteq H \leq G} \frac{\mu(H, G)}{|G : H|^t}.$$

For $i \in \mathbb{N}$, denote by $e_i(G, K)$ the i -th moment $E(\tau_{G,K}^i)$ of the variable $\tau_{G,K}$. Using (1.4) we can generalize the arguments in the proof of Theorems 1 and 3 and obtain:

Theorem 11. *If G is a finite group and K is a proper subgroup of G , then*

$$e_1(G, K) = - \sum_{K \leq H < G} \frac{\mu_G(H) |G|}{|G| - |H|}$$

$$e_2(G, K) = - \sum_{K \leq H < G} \frac{\mu_G(H) |G| (|G| + |H|)}{(|G| - |H|)^2}.$$

Notice that $\gamma_K = \frac{|G|}{|G| - |K|}$ is the expected number of elements of G which have to be drawn before an elements outside K is found. Clearly $\gamma_K \leq e_1(G, K)$ and $\gamma_K = e_1(G, K)$ if and only if K is a maximal subgroup of G . So we have:

Corollary 12. *Let K be a proper subgroup of a finite group G . Then*

$$- \sum_{K \leq H < G} \frac{\mu_G(H)}{|G| - |H|} \geq \frac{1}{|G| - |K|}$$

and the equality holds if and only if K is a maximal subgroup of G .

In the last section of this note, we will extend the definition and the study of $e_1(G)$ to the case of a (topologically) finitely generated profinite group G . A profinite group G , being a compact topological group, can be seen as a probability space. If we denote with μ the normalized Haar measure on G , so that $\mu(G) = 1$, the probability that k random elements generate (topologically) G is defined as

$$P_G(k) = \mu(\{(x_1, \dots, x_k) \in G^k \mid \langle x_1, \dots, x_k \rangle = G\}),$$

where μ denotes also the product measure on G^k . A profinite group G is said to be positively finitely generated, PFG for short, if $P_G(k)$ is positive for some natural number k , and the least such natural number is denoted by $d_P(G)$. Not all finitely generated profinite groups are PFG (for example if $\hat{F}_d$ is the free profinite group of rank $d \geq 2$ then $P_{\hat{F}_d}(t) = 0$ for every $t \geq d$, see for example [8]): if G is not PFG we set $d_P(G) = \infty$. The relation

$$e_1(G) = \sum_{n \geq 0} 1 - P_G(n)$$

remains true when G is a profinite group. Since $P_G(n) = 0$ whenever $n \leq d_P(G)$ we immediately deduce that $e_1(G) > d_P(G)$. Moreover (see Lemma 31) $e_1(G) < \infty$ if and only if G is PFG. Denote by $m_n(G)$ the number of index n maximal subgroups of G . A group G is said to have polynomial maximal subgroup growth (PMSG) if $m_n(G) \leq \alpha n^\sigma$ for all n (for some constant α and σ). A one-line argument shows that PMSG groups are positively finitely generated. By a very surprising result of Mann and Shalev [14] the converse also holds: a profinite group is PFG if and only if it has polynomial maximal subgroup growth. In particular we have:

Theorem 13. *Let G be a PFG group and assume that $m_n(G) \leq \alpha n^\sigma$ for each $n \in \mathbb{N}$. Let $\beta = \lceil \sigma + \log_2 \alpha \rceil$. Then*

$$e_1(G) \leq \beta + 3 \quad \text{and} \quad e_1(G) + e_2(G) \leq \beta^2 + \frac{(15 + \pi^2)\beta}{3} + 6 + \pi^2.$$

We will discuss some applications of the previous theorem. For example we have:

Corollary 14. *Denote by G_d the free prosolvable group of rank d . There exists a constant α^* such that, for each $d \geq 2$, we have*

$$\lceil \gamma d - \gamma \rceil + 1 \leq e_1(G_d) \leq \lceil \gamma d \rceil + \alpha^*,$$

where $\gamma \simeq 3.243$ is the Pálffy-Wolf constant.

Corollary 15. *Denote by M_d the free prometabelian group of rank $d \geq 2$. We have*

$$2d + 1 < e_1(M_d) < 2d + 2.$$

Finally we notice that Theorem 13 allows us to obtain a small improvement to a bound given by Lubotzky for the excess $ex(G)$ of a finite group: he proved that $e_1(G) \leq ed(G) + 2e \log \log |G| + 11$ [11, Corollary p. 453]; an intermediate step in his proof is to show that for any finite group G and any $n \in \mathbb{N}$, one has $m_n(G) \leq r^2 n^{d(G)+2}$ where r is the number of complemented factors in a chief series

of G [11, Corollary 2.6]. This inequality, together with Theorem 13, immediately implies the following result:

Theorem 16. *If G is a finite group, then $e_1(G) \leq d(G) + \lceil 2 \log_2 r \rceil + 5$, where r is the number of complemented factors in a chief series of G . In particular $ex(G) = e_1(G) - d(G) \leq \lceil 2 \log_2 \log_2 |G| \rceil + 5$.*

2. PROOFS OF THEOREMS 1, 2 AND 3

We will deduce Theorems 1 and 2 as particular cases of the following more general result.

Proposition 17. *If G is a finite group and $d \in \mathbb{N}$, then*

$$e_1(G) \leq d - \sum_{H < G} \frac{\mu_G(H)|G|}{(|G : H|^d)(|G| - |H|)},$$

with equality if $d \leq d(G)$.

Proof. Since $1 - P_G(n) \leq 1$ for any $n \in \mathbb{N}$, from (1.1) and (1.3) it follows that

$$\begin{aligned} e_1(G) &= \sum_{n \geq 0} 1 - P_G(n) \leq d + \sum_{n \geq d} 1 - P_G(n) \\ &= d + \sum_{n \geq d} \left(1 - \sum_{H \leq G} \frac{\mu_G(H)}{|G : H|^n} \right) \\ &= d - \sum_{n \geq d} \left(\sum_{H < G} \frac{\mu_G(H)}{|G : H|^n} \right) \\ &= d - \sum_{H < G} \left(\sum_{n \geq d} \frac{\mu_G(H)}{|G : H|^n} \right) \\ &= d - \sum_{H < G} \frac{\mu_G(H)|G|}{(|G : H|^d)(|G| - |H|)}. \end{aligned}$$

Since $P_G(n) = 0$ when $n < d(G)$, the previous inequality is indeed an equality if $d \leq d(G)$. $\square$

Proofs of Theorems 1 and 2. Theorems 1 and 2 follow from Proposition 17 by setting, respectively, $d = 0$ or $d = d(G)$. $\square$

The proof of Theorem 3 requires a preliminary Lemma.

Lemma 18. $e_1(G) + e_2(G) = 2 \sum_{n \geq 1} nP(\tau_G \geq n)$.

Proof. We have

$$\begin{aligned} \sum_{n \geq 1} nP(\tau_G \geq n) &= \sum_{n \geq 1} \frac{n(n+1)}{2} P(\tau_G = n) \\ &= \sum_{n \geq 1} \frac{n^2}{2} P(\tau_G = n) + \sum_{n \geq 1} \frac{n}{2} P(\tau_G = n) \\ &= \frac{e_2(G)}{2} + \frac{e_1(G)}{2}. \end{aligned} \quad \square$$

Proof of Theorem 3. Using Lemma 18 we get

$$\begin{aligned}
e_2(G) &= 2 \sum_{n \geq 1} nP(\tau_G \geq n) - e_1(G) \\
&= 2 \sum_{n \geq 0} (n+1)P(\tau_G > n) - e_1(G) \\
&= 2 \sum_{n \geq 0} (n+1)(1 - P_G(n)) - e_1(G) \\
&= -2 \sum_{n \geq 0} (n+1) \left(\sum_{H < G} \frac{\mu_G(H)}{|G:H|^n} \right) - e_1(G) \\
&= -2 \sum_{H < G} \mu_G(H) \left(\sum_{n \geq 0} \frac{(n+1)}{|G:H|^n} \right) - e_1(G) \\
&= -2 \sum_{H < G} \mu_G(H) \left(\sum_{n \geq 0} \frac{1}{|G:H|^n} \right)^2 - e_1(G) \\
&= -2 \sum_{H < G} \mu_G(H) \left(\frac{1}{1 - |G:H|^{-1}} \right)^2 - e_1(G) \\
&= -2 \sum_{H < G} \mu_G(H) \left(\frac{1}{1 - |G:H|^{-1}} \right)^2 + \sum_{H < G} \frac{\mu_G(H)}{1 - |G:H|^{-1}} \\
&= \sum_{H < G} \mu_G(H) \left(\frac{1}{1 - |G:H|^{-1}} \right) \left(1 - \frac{2}{1 - |G:H|^{-1}} \right) \\
&= - \sum_{H < G} \frac{\mu_G(H)|G|(|G| + |H|)}{(|G| - |H|)^2}. \quad \square
\end{aligned}$$

We conclude this section with other two lemmas which will be useful in our further discussions.

Lemma 19. *If $P_G(k) \geq \epsilon$, then $e_1(G) \leq k/\epsilon$.*

Proof. Assume that $P_G(k) \geq \epsilon$, let $n \in \mathbb{N}$ and write n in the form $n = kq + r$ with $q \in \mathbb{N}$ and $r \in \{0, \dots, k-1\}$. If $\langle x_1, \dots, x_n \rangle \neq G$, then in particular $\langle x_1, \dots, x_k \rangle \neq G$, $\langle x_{k+1}, \dots, x_{2k} \rangle \neq G, \dots, \langle x_{(q-1)k+1}, \dots, x_{qk} \rangle \neq G$ and therefore

$$\begin{aligned}
P(\tau_G > n) &= P(\langle x_1, \dots, x_n \rangle \neq G) \leq \prod_{0 \leq i \leq q-1} P(\langle x_{ik+1}, \dots, x_{(i+1)k} \rangle \neq G) \\
&= \prod_{0 \leq i \leq q-1} (1 - P_G(k)) \leq (1 - \epsilon)^q.
\end{aligned}$$

It follows that

$$\begin{aligned}
e_1(G) &= \sum_{n \geq 0} P(\tau_G > n) = \sum_{q \geq 0} \left(\sum_{0 \leq r \leq k-1} P(\tau_G > qk + r) \right) \\
&\leq \sum_{q \geq 0} \left(\sum_{0 \leq r \leq k-1} (1 - \epsilon)^q \right) = \sum_{q \geq 0} k(1 - \epsilon)^q = \frac{k}{\epsilon}. \quad \square
\end{aligned}$$

Lemma 20. *If $P_G(k) \geq \epsilon$, then $e_1(G) + e_2(G) \leq \frac{2k^2}{\epsilon^2} - \frac{k^2}{\epsilon} + \frac{k}{\epsilon}$.*

Proof. Using Lemma 18 and arguing as in the proof of Lemma 19, we get

$$\begin{aligned}
e_1(G) + e_2(G) &= 2 \sum_{n \geq 0} (n+1)P(\tau_G > n) \\
&= 2 \sum_{q \geq 0} \left(\sum_{0 \leq r \leq k-1} (qk + r + 1)P(\tau_G > qk + r) \right) \\
&\leq 2 \sum_{q \geq 0} \left(\sum_{0 \leq r \leq k-1} (qk + r + 1)(1 - \epsilon)^q \right) \\
&= 2 \sum_{q \geq 0} \left(k^2(q+1) - \frac{k^2 - k}{2} \right) (1 - \epsilon)^q \\
&= 2k^2 \sum_{q \geq 0} (q+1)(1 - \epsilon)^q - (k^2 - k) \sum_{q \geq 0} (1 - \epsilon)^q \\
&= 2k^2 \left(\sum_{q \geq 0} (1 - \epsilon)^q \right)^2 - (k^2 - k) \sum_{q \geq 0} (1 - \epsilon)^q \\
&= \frac{2k^2}{\epsilon^2} - \frac{k^2}{\epsilon} + \frac{k}{\epsilon}. \quad \square
\end{aligned}$$

3. FINITE SIMPLE GROUPS

Let S be a finite simple group and let $p_S = P_S(2)$. Since $d(S) = 2$, we have

$$e_1(S) \geq \sum_{n \geq 0} (1 - P_S(n)) \geq (1 - P_S(0)) + (1 - P_S(1)) + (1 - P_S(2)) = 3 - p_S \geq 2$$

and, by Lemma 18,

$$e_1(S) + e_2(S) \geq 2((1 - P_S(0)) + 2(1 - P_S(1)) + 3(1 - P_S(2))) = 12 - 6p_S.$$

By applying Lemma 19 and Lemma 20 with $k = 2$ we obtain

$$3 - p_S \leq e_1(S) \leq \frac{2}{p_S} \quad \text{and} \quad 12 - 6p_S \leq e_1(S) + e_2(S) \leq \frac{8}{p_S^2} - \frac{2}{p_S}.$$

Since, by [4], [8] and [9], $\lim_{|S| \rightarrow \infty} p_S = 1$, we deduce that

$$\lim_{|S| \rightarrow \infty} e_1(S) = 2, \quad \lim_{|S| \rightarrow \infty} e_2(S) = 4, \quad \lim_{|S| \rightarrow \infty} \text{var}(\tau_S) = \lim_{|S| \rightarrow \infty} e_2(S) - e_1(S)^2 = 0.$$

By [16, Table 1], there are only few simple groups S with $p_S \leq 9/10$; the corresponding values of $e_1(S)$ and $e_2(S)$ are listed in Table 1.

On the other hand, if $p_S \geq \epsilon = 9/10$, then

$$e_1(S) \leq 2/\epsilon = 20/9 \sim 2.222 \text{ and } e_2(S) \leq \frac{8}{\epsilon^2} - \frac{2}{\epsilon} - 3 + \epsilon = \frac{4499}{810} \sim 5.554.$$

The conclusion of all these considerations is the statement of Theorem 7.

TABLE 1

S	$P_S(2)$	$e_1(S)$	$e_2(S)$	$\text{var}(S)$
Alt(6)	0.588	2.494	6.665	0.446
Alt(5)	0.633	2.457	6.502	0.468
$L_2(7)$	0.678	2.383	6.059	0.380
Alt(7)	0.726	2.308	5.622	0.294
Alt(8)	0.738	2.290	5.515	0.271
$L_2(11)$	0.769	2.256	5.334	0.246
M_{12}	0.813	2.202	5.043	0.195
M_{11}	0.817	2.199	5.039	0.197
$L_2(8)$	0.845	2.171	4.888	0.177
Alt(9)	0.848	2.166	4.863	0.172
$L_3(3)$	0.863	2.149	4.773	0.154
$L_3(4)$	0.864	2.142	4.720	0.134
Alt(10)	0.875	2.137	4.709	0.144
$S_4(3)$	0.887	2.116	4.589	0.111
Alt(11)	0.893	2.116	4.599	0.123

4. SYMMETRIC GROUPS

In order to compute $e_1(\text{Sym}(n))$ it is useful to introduce another random variable τ_n^* . Given a sequence of independent, uniformly distributed $\text{Sym}(n)$ -valued random variables $(x_n)_{n \in \mathbb{N}}$, we define

$$\tau_n^* = \min\{n \geq 1 \mid \text{Alt}(n) \leq \langle x_1, \dots, x_n \rangle\}.$$

$E(\tau_n^*)$ is the expected number of elements of $\text{Sym}(n)$ which have to be drawn at random, with replacement, before the subgroup H generated by these elements contains $\text{Alt}(n)$.

Lemma 21. *If $n \geq 3$, then $e_1(\text{Sym}(n)) \geq 2.5$ and $e_1(\text{Sym}(n)) + e_2(\text{Sym}(n)) \geq 10$.*

Proof. We have $P_{\text{Sym}(n)}(t) = 0$ if $t < 2$. Moreover, since $\text{Sym}(n)/\text{Alt}(n) \cong C_2$, we have $P_{\text{Sym}(n)}(t) \leq P_{C_2}(t) = 1 - 1/2^t$, hence

$$e_1(\text{Sym}(n)) = \sum_{t \geq 0} (1 - P_{\text{Sym}(n)}(t)) \geq 2 + \sum_{t \geq 2} \frac{1}{2^t} = 2.5.$$

By Lemma 18, we have

$$\begin{aligned} \frac{e_1(\text{Sym}(n)) + e_2(\text{Sym}(n))}{2} &= \sum_{t \geq 0} (t+1) (1 - P_{\text{Sym}(n)}(t)) \geq 3 + \sum_{t \geq 2} \frac{t+1}{2^t} \\ &= 1 + \sum_{t \geq 0} \frac{t+1}{2^t} = 1 + \left(\sum_{t \geq 0} \frac{1}{2^t} \right)^2 = 5. \quad \square \end{aligned}$$

Lemma 22. *If $n \geq 4$, then*

$$e_1(\text{Sym}(n)) \leq E(\tau_n^*) + 0.5 \quad \text{and} \quad e_2(\text{Sym}(n)) \leq E(\tau_n^*) + E(\tau_n^{*2}) + 1.5.$$

Proof. Let $p_n^*(t)$ be the probability that t randomly chosen elements of $\text{Sym}(n)$ generate a subgroup containing $\text{Alt}(n)$. Notice that for any $t \in \mathbb{N}$, we have

$$(4.1) \quad p_n^*(t) = \frac{P_{\text{Alt}(n)}(t)}{2^t} + P_{\text{Sym}(n)}(t).$$

Hence

$$\begin{aligned} e_1(\text{Sym}(n)) &= \sum_{t \geq 0} (1 - P_{\text{Sym}(n)}(t)) = \sum_{t \geq 0} \left(1 - p_n^*(t) + \frac{P_{\text{Alt}(n)}(t)}{2^t} \right) \\ &= E(\tau_n^*) + \sum_{t \geq 0} \frac{P_{\text{Alt}(n)}(t)}{2^t} \leq E(\tau_n^*) + \sum_{t \geq 2} \frac{1}{2^t} = E(\tau_n^*) + \frac{1}{2}. \end{aligned}$$

(notice that we need to assume $n \geq 4$ to ensure that $P_{\text{Alt}(n)}(t) = 0$ for $t < 2$). Moreover

$$\begin{aligned} e_1(\text{Sym}(n)) + e_2(\text{Sym}(n)) &= 2 \left(\sum_{t \geq 0} (t+1) (1 - P_{\text{Sym}(n)}(t)) \right) \\ &= 2 \left(\sum_{t \geq 0} (t+1) \left(1 - p_n^*(t) + \frac{P_{\text{Alt}(n)}(t)}{2^t} \right) \right) \\ &= E(\tau_n^*) + E(\tau_n^{*2}) + 2 \sum_{t \geq 0} \frac{(t+1)P_{\text{Alt}(n)}(t)}{2^t} \\ &\leq E(\tau_n^*) + E(\tau_n^{*2}) + 2 \sum_{t \geq 2} \frac{t+1}{2^t} = E(\tau_n^*) + E(\tau_n^{*2}) + 4. \end{aligned}$$

The conclusion follows from the fact that $e_1(\text{Sym}(n)) \geq 2.5$. $\square$

Lemma 23. *If $n \geq 5$ then*

$$\begin{aligned} e_1(\text{Sym}(n)) &\leq 2 \left(1 - \frac{1}{n} - \frac{13}{n^2} \right)^{-1} + 0.5, \\ e_2(\text{Sym}(n)) &\leq 8 \left(1 - \frac{1}{n} - \frac{13}{n^2} \right)^{-2} - 2 \left(1 - \frac{1}{n} - \frac{13}{n^2} \right)^{-1} + 1.5. \end{aligned}$$

Proof. By [15, Theorem 1.1], if $n \geq 5$, then $p_n^*(2) \geq 1 - \frac{1}{n} - \frac{13}{n^2}$. But then we deduce from Lemmas 19 and 20 that

$$E(\tau_n^*) \leq 2 \left(1 - \frac{1}{n} - \frac{13}{n^2} \right)^{-1}, \quad E(\tau_n^*) + E(\tau_n^{*2}) \leq 8 \left(1 - \frac{1}{n} - \frac{13}{n^2} \right)^{-2} \left(1 - \frac{1}{n} - \frac{13}{n^2} \right)^{-1}$$

and the conclusion follows from Lemma 22. $\square$

From Lemmas 21 and 23 we conclude:

$$\lim_{n \rightarrow \infty} e_1(\text{Sym}(n)) = 2.5, \quad \lim_{n \rightarrow \infty} e_2(\text{Sym}(n)) = 7.5.$$

We have already given (Examples 4 and 6) the values of $e_1(\text{Sym}(n))$ and $e_2(\text{Sym}(n))$ when $n \in \{3, 4\}$. Applying Theorems 1 and 3 we can compute that:

$$\begin{aligned} e_1(\text{Sym}(5)) &= \frac{284263035913}{99577017540} \sim 2.8547, \\ e_1(\text{Sym}(6)) &= \frac{1540174028733778237709351}{534488528295916921285020} \sim 2.8816, \\ e_2(\text{Sym}(5)) &= \frac{46956613736860583432939}{4957791211080733825800} \sim 9.4713, \\ e_2(\text{Sym}(6)) &= \frac{1368837541136020534875191952448889920769855832073}{142838993439967591711705620401962361364038200200} \sim 9.5831. \end{aligned}$$

Proof of Theorem 8. By Lemma 23, $e_1(\text{Sym}(n)) \leq 2.82$ and $e_2(\text{Sym}(n)) \leq 9.5703$ if $n \geq 14$. The other values can be computed with GAP [6] and the formulas given in Theorem 1 and Theorem 3 : for n from 6 to 13, $e_1(\text{Sym}(n))$ and $e_2(\text{Sym}(n))$ are strictly decreasing functions (and $e_1(\text{Sym}(13)) \sim 2.570$, $e_2(\text{Sym}(13)) \sim 7.8659$). $\square$

5. GENERATING A TRANSITIVE SUBGROUP OF $\text{Sym}(n)$

Let $G = \text{Sym}(n)$ and let $x = (x_m)_{m \in \mathbb{N}}$ be a sequence of independent, uniformly distributed G -valued random variables. We may define a random variable τ_n by

$$\tau_n = \min\{t \geq 1 \mid \langle x_1, \dots, x_t \rangle \text{ is a transitive subgroup of } \text{Sym}(n)\}.$$

Denote by $P_n(t)$ the probability that t randomly chosen elements in $\text{Sym}(n)$ generate a transitive subgroup of $\text{Sym}(m)$. We have

$$(5.1) \quad \mathbb{E}(\tau_n) = \sum_{t \geq 0} 1 - P_n(t).$$

We may compute the expectation $\mathbb{E}(\tau_n)$ using a formula for the probability $P_n(t)$ proved in [3]. Denote by Π_n the set of partitions of n , i.e. nondecreasing sequences of natural numbers whose sum is n . Given $\omega = (n_1, \dots, n_k) \in \Pi_n$ with

$$n_1 = \dots = n_{k_1} > n_{k_1+1} = \dots = n_{k_1+k_2} > \dots > n_{k_1+\dots+k_{r-1}+1} = \dots = n_{k_1+\dots+k_r},$$

$$\text{define } \mu(\omega) = (-1)^{k-1}(k-1)!, \quad \iota(\omega) = \frac{n!}{n_1!n_2!\dots n_k!}, \quad \nu(\omega) = k_1!k_2!\dots k_r!.$$

Proposition 24. [3, Proposition 2.1]

$$P_n(t) = \sum_{\omega \in \Pi_n} \frac{\mu(\omega)\iota(\omega)}{\nu(\omega)\iota(\omega)^t}.$$

Proof of Theorem 9. By (5.1) and Proposition 24 we have:

$$\begin{aligned} \mathbb{E}(\tau_n) &= \sum_{t \geq 0} 1 - P_n(t) = \sum_{t \geq 0} \left(1 - \sum_{\omega \in \Pi_n} \frac{\mu(\omega)\iota(\omega)}{\nu(\omega)\iota(\omega)^t} \right) \\ &= - \sum_{\omega \in \Pi_n^*} \left(\frac{\mu(\omega)\iota(\omega)}{\nu(\omega)} \sum_{t \geq 0} \frac{1}{\iota(\omega)^t} \right) = - \sum_{\omega \in \Pi_n^*} \frac{\mu(\omega)\iota(\omega)^2}{\nu(\omega)(\iota(\omega) - 1)}. \quad \square \end{aligned}$$

Example 25. If $n = 2$, then τ_2 is a geometric random variable with parameter $\frac{1}{2}$, so $\mathbb{E}(\tau_2) = 2$.

Example 26. If $n = 3$, then the information needed to apply Theorem 9 is collected in Table 2. We obtain

$$E(\tau_3) = \frac{-12}{5} + \frac{9}{2} = \frac{21}{10}.$$

TABLE 2

ω	$\mu(\omega)$	$\nu(\omega)$	$\iota(\omega)$
(1,1,1)	2	6	6
(2,1)	-1	1	3

Example 27. If $n = 4$, then the information needed to apply Theorem 9 is collected in Table 3. We obtain

$$E(\tau_4) = \frac{6 \cdot 24^2}{24 \cdot 23} - \frac{2 \cdot 12^2}{2 \cdot 11} + \frac{4^2}{3} + \frac{6^2}{2 \cdot 5} = \frac{7982}{3795} \sim 2.1033.$$

TABLE 3

ω	$\mu(\omega)$	$\nu(\omega)$	$\iota(\omega)$
(1,1,1,1)	-6	24	24
(2,1,1)	2	2	12
(3,1)	-1	1	4
(2,2)	-1	2	6

Proposition 28. If $n \geq 5$, then

$$2 \leq E(\tau_n) \leq 2 \left(1 - \frac{1}{n} - \frac{3}{2n(n-1)} - \frac{3}{(n-1)(n-2)} \right)^{-1}.$$

Proof. By (5.1), $E(\tau_n) \geq (1 - P_n(0)) + (1 - P_n(1)) + (1 - P_n(2)) + (1 - P_n(3))$. Clearly $P_n(0) = 0$ while $P_n(1) = \frac{1}{n}$ since an element of $\text{Sym}(n)$ generates a transitive subgroup if and only if it is a cycle of length n . Moreover, by [15, Lemma 2.1] and its proof,

$$P_n(t) \leq 1 - \frac{1}{n^{t-1}} + \frac{1}{2(n(n-1))^{t-1}}.$$

Hence

$$E(\tau_n) \geq 1 + \left(1 - \frac{1}{n} \right) + \left(\frac{1}{n} - \frac{1}{2n(n-1)} \right) + \left(\frac{1}{n^2} - \frac{1}{2(n(n-1))^2} \right) \geq 2.$$

The same argument used in the proof of Lemma 19 implies that $E(\tau_n) \leq 2/\epsilon$ if $P_2(n) \geq \epsilon$. On the other hand (see [15, Lemma 2.2] and its proof)

$$P_n(2) \geq 1 - \frac{1}{n} - \frac{3}{2n(n-1)} - \frac{3}{(n-1)(n-2)}$$

so the conclusion follows. $\square$

Corollary 29. If $n \geq 5$, then

$$E(\tau_n) < E(\tau_5) \leq \frac{290968955}{139268556} \sim 2.0893.$$

Proof. We computed the value of $E(\tau_n)$ using Theorem 9 for $5 \leq n \leq 27$: we noticed that $E(\tau_5) \sim 2.0893$ and $E(\tau_n) < E(\tau_{n-1})$; in particular $E(\tau_{27}) < 2.004$. For $n \geq 28$ the conclusion follows from Proposition 28. $\square$

Repeating the same arguments used in the proof of Theorem 3, we can compute the second moment of the variable τ_n .

Proposition 30. *For every $n \geq 2$ we have*

$$E(\tau_n^2) = - \sum_{\omega \in \Pi_n^*} \frac{\mu(\omega) \iota(\omega)^2 (\iota(\omega) + 1)}{\nu(\omega) (1 - \iota(\omega))^2},$$

where Π_n^* is the set of partitions of n in at least two subsets.

6. FROM FINITE TO PROFINITE

In this section we will assume that G is a (topologically) finitely generated profinite group G . Let $\mathcal{N}$ be the set of the open normal subgroups of G . Since (see [10, (11.5)])

$$P_G(n) = \inf_{N \in \mathcal{N}} P_{G/N}(n)$$

we have

$$\begin{aligned} e_1(G) &= \sum_{n \geq 0} (1 - P_G(n)) = \sum_{n \geq 0} \left(1 - \inf_{N \in \mathcal{N}} P_{G/N}(n) \right) = \sum_{n \geq 0} \left(\sup_{N \in \mathcal{N}} (1 - P_{G/N}(n)) \right) \\ &= \sup_{N \in \mathcal{N}} \left(\sum_{n \geq 0} (1 - P_{G/N}(n)) \right) = \sup_{N \in \mathcal{N}} e_1(G/N). \end{aligned}$$

Lemma 31. *$e_1(G) < \infty$ if and only if G is PFG.*

Proof. If $e_1(G) < \infty$, then $d_P(G) \leq e_1(G) < \infty$ hence G is PFG. Conversely, assume that $P_G(k) \geq \epsilon \neq 0$ for some $k \in \mathbb{N}$: then $e_1(G) \leq k/\epsilon$ by Lemma 19. $\square$

Proof of Theorem 13. Let $\beta = \lceil \sigma + \log_2 \alpha \rceil$ and let $k = \beta + t$ with $t \in \mathbb{N}$. As in the proof of [10, Proposition 11.2.2] we have

$$1 - P_G(k) \leq \sum_{n \geq 2} \frac{m_n(G)}{n^k} \leq \sum_{n \geq 2} \frac{\alpha n^\sigma}{n^k} \leq \sum_{n \geq 2} \frac{n^{\sigma + \log_2 \alpha}}{n^k} \leq \sum_{n \geq 2} \frac{1}{n^t}.$$

It follows that

$$\begin{aligned} e_1(G) &= \sum_{k \geq 0} (1 - P_G(k)) \leq \beta + 2 + \sum_{k \geq \beta+2} (1 - P_G(k)) \\ &\leq \beta + 2 + \sum_{u \geq 2} \left(\sum_{n \geq 2} n^{-u} \right) = \beta + 2 + \left(\sum_{n \geq 2} \left(\sum_{u \geq 2} n^{-u} \right) \right) \\ &= \beta + 2 + \sum_{n \geq 2} \frac{1}{n^2} \frac{n}{n-1} = \beta + 2 + \left(\sum_{n \geq 1} \frac{1}{n(n+1)} \right) = \beta + 3. \end{aligned}$$

Moreover we have

$$\begin{aligned}
e_1(G) + e_2(G) &= 2 \sum_{k \geq 0} (k+1)(1 - P_G(k)) \\
&\leq 2 \sum_{0 \leq k \leq \beta+1} (k+1) + 2 \sum_{k \geq \beta+2} \left(\sum_{n \geq 2} \frac{(k+1)n^\beta}{n^k} \right) \\
&\leq (\beta+2)(\beta+3) + 2 \sum_{k \geq \beta+2} \left(\sum_{n \geq 2} \frac{(k+1)n^\beta}{n^k} \right) \\
&\leq (\beta+2)(\beta+3) + 2 \sum_{n \geq 2} \left(\sum_{u \geq 2} \frac{u + \beta + 1}{n^u} \right) \\
&\leq (\beta+2)(\beta+3) + 2 \sum_{n \geq 2} \frac{1}{n^2} \left(\sum_{t \geq 0} \frac{t + \beta + 3}{n^t} \right) \\
&\leq (\beta+2)(\beta+3) + 2 \sum_{n \geq 2} \frac{\beta+3}{n^2} \left(\sum_{t \geq 0} \frac{t+1}{n^t} \right) \\
&= (\beta+2)(\beta+3) + 2 \sum_{n \geq 2} \frac{\beta+3}{(n-1)^2} \\
&= (\beta+2)(\beta+3) + \frac{\pi^2(\beta+3)}{3}. \quad \square
\end{aligned}$$

If G is a d -generated pronilpotent group, then all the maximal subgroups have prime index and $m_p(G) \leq \frac{p^d-1}{p-1}$ for every prime p . So, repeating the argument of the previous proof and using $\sum_p (p-1)^{-2} \sim 1.3751$ (see for example [5, p. 95]), we obtain

$$e_1(G) \leq d+1 + \sum_{u \geq 1} \left(\sum_p \frac{1}{(p-1)p^u} \right) \leq d+1 + \sum_p \frac{1}{(p-1)^2} \leq d+2.3751.$$

A more accurate estimation is given in [19]: by [19, Corollary 2] if N_d is the free pronilpotent group of rank d , then $e_1(N_d) \leq d+2.1185$.

Lemma 32. *Let G be a finite d -generated metabelian group. If $m_n(G) \neq 0$, then q is a prime power. Moreover*

$$m_2(G) \leq 2^d \text{ and } m_q(G) \leq \frac{q^{2d}}{q-1} \text{ if } q \neq 2.$$

Proof. Without loss of generality we can assume that $\text{Frat}(G) = 1$. In this case the Fitting subgroup $\text{Fit}(G)$ of G is a direct product of minimal normal subgroups of G , it is abelian and complemented. Let K be a complement of $\text{Fit}(G)$ in G ; since G is metabelian, K is abelian. Let F be a complement of $Z(G)$ in $\text{Fit}(G)$ and let $H = Z(G) \times K$. We have $G = F \rtimes H$ and we can write F in the form

$$F = V_1^{n_1} \times \cdots \times V_r^{n_r}$$

where $V_1, \dots, V_r$ are irreducible H -modules, pairwise not H -isomorphic. All the maximal subgroups of G have prime-power index. Let q be a prime power and

let $\mathcal{M}_q$ be the set of maximal subgroups of G of index q . Let $M \in \mathcal{M}_q$. If $F \leq M$ then q is a prime and there are at most $(q^d - 1)/q - 1$ possible choices for M . If M is a maximal subgroup supplementing F , then M contains the subgroup $X_i = \left(\prod_{j \neq i} V_j^{n_j}\right) C_H(V_i)$ for some index $i \in \Omega_q := \{j \mid |V_j| = q\}$. In this case $\mathbb{F}_i = \text{End}_H(V_i)$ is a field and V_i is an absolutely irreducible $\mathbb{F}_i H_i$ -module. Since H is abelian, $\dim_{\mathbb{F}_i} V_i = 1$ and $H_i = H/C_H(V_i)$ is isomorphic to a subgroup of $\mathbb{F}_i^*$. Given $i \in \Omega_q$, the number of maximal subgroups M containing X_i and supplementing F coincides with the number $q \cdot (q^{n_i} - 1)/(q - 1)$ of maximal subgroups of $V_i^{n_i} \rtimes H_i$ not containing $V_i^{n_i}$. On the other hand, being an epimorphic image of G , the group $V_i^{n_i} \rtimes H_i$ is d -generated, and this implies $n_i \leq d - 1$. Finally notice that to any $i \in \Omega_q$, there corresponds a different nontrivial homomorphism from H to $\mathbb{F}_i^* \cong C_{q-1}$. Since $d(H) \leq d$, it follows $|\Omega_q| \leq (q - 1)^d - 1$. But then

$$m_q(G) \leq \frac{q^d - 1}{q - 1} + ((q - 1)^d - 1) \frac{q^d - q}{q - 1} \leq \frac{q^{2d}}{q - 1}. \quad \square$$

Proof of Corollary 15. It follows from [20, Theorem D] that $d_P(M_d) = 2d + 1$ hence $e_1(M_d) > 2d + 1$. On the other hand, by Lemma 32,

$$\begin{aligned} e_1(M_d) &= \sum_{k \geq 0} (1 - P_{M_d}(k)) \leq 2d + 1 + \sum_{k \geq 2d+1} 1 - P_{M_d}(k) \\ &\leq 2d + 1 + \sum_{k \geq 2d+1} \left(\sum_q \frac{m_q(M_d)}{n^k} \right) \\ &\leq 2d + 1 + \sum_{k \geq 2d+1} \left(\frac{2^d}{2^k} + \sum_{q \neq 2} \frac{q^{2d}}{q^k(q-1)} \right) \\ &\leq 2d + 1 + \sum_{u \geq d+1} \frac{1}{2^u} + \sum_{q \neq 2} \left(\sum_{u \geq 1} \frac{1}{(q-1)q^u} \right) \\ &= 2d + 1 + \frac{1}{2^d} + \sum_{q \neq 2} \frac{1}{(q-1)^2} < 2d + 2. \quad \square \end{aligned}$$

A similar approach can be applied to the free prosupersolvable group H_d of rank $d \geq 2$. By [1], $d_p(H_d) = 2d + 1$. The maximal subgroups of H_p have prime index and, since $H_d/\text{Frat}(H_t)$ is metabelian, we may estimate $m_p(H_d)$ using Lemma 32. Repeating the argument of the previous proof, we conclude

$$2d + 1 \leq e_1(H_d) \leq 2d + 1 + \frac{1}{2^d} + \sum_{p \neq 2} \frac{1}{(p-1)^2} \leq 2d + 1.3751 + \frac{1}{2^d}.$$

Consider now the case of the free prosolvable group G_d of rank $d \geq 2$. By [17, Theorem A] $d_P(G) = \lceil \gamma d - \gamma \rceil + 1$, with

$$\gamma = \log_9 48 + \frac{1}{3} \log_9 24 + 1 \simeq 3.243,$$

the Pálffy-Wolf constant. From Lemma 31 and Theorem 13 we deduce:

Proof of Corollary 14. There exists a constant δ such that $f^{20(\log_2 f)^3 + 5} \leq \delta p^f$ for any prime p and any positive integer f . By [13, Theorem 10] and its proof,

$m_n(G_d) \leq \delta n^{\gamma d+2}$ for all $n \in \mathbb{N}$. Hence by Theorem 13, $e_1(G_d) \leq \lceil \gamma d + \log_2 \delta \rceil + 5$. $\square$

REFERENCES

1. Crestani, E., De Franceschi, G., Lucchini, A.: Probability and bias in generating supersoluble groups. *Proc. Edinb. Math. Soc.*, to appear
2. Detomi, E., Lucchini, A.: Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* 265, 651–668 (2003)
3. Detomi, E., Lucchini, A.: Some generalizations of the probabilistic zeta function. In: *Ischia group theory 2006*, pp. 56–72, World Sci. Publ., Hackensack, NJ (2007)
4. Dixon, J.D.: The probability of generating the symmetric group. *Math. Z.* 110, 199–205 (1969)
5. Finch, S.: *Mathematical constants. Encyclopedia of Mathematics and its Applications.* 94, Cambridge University Press, Cambridge (2003)
6. The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.7 (2015). <http://www.gap-system.org>
7. Hall, P.: The Eulerian functions of a group. *Quart. J. Math.* 7, 134–151 (1936)
8. Kantor, W.M., Lubotzky, A.: The probability of generating a finite classical group. *Geom. Ded.* 36, 67–87 (1990)
9. Liebeck, M.W., Shalev, A.: The probability of generating a finite simple group. *Geom. Ded.* 56, 103–113 (1995)
10. Lubotzky, A., Segal, D.: *Subgroup growth. Progress in Mathematics*, 212. Birkhäuser Verlag, Basel (2003)
11. Lubotzky, A.: The expected number of random elements to generate a finite group.
12. Lucchini, A.: The X -Dirichlet polynomial of a finite group. *J. Group Theory* 8, 171–188 (2005)
13. Mann, A.: Positively finitely generated groups. *Forum Math.* 8, 429–459 (1996)
14. Mann, A., Shalev, A.: Simple groups, maximal subgroups, and probabilistic aspects of profinite groups. *Israel J. Math.* 96, 449–468 (1996)
15. Maróti, A., Tamburini M.C.: Bounds for the probability of generating the symmetric and alternating groups. *Arch. Math.* 96, 115–121 (2011)
16. Menezes, N.E., Quick M., Roney-Dougal, C.M.: The probability of generating a finite simple group. *Israel J. Math.* 198:1, 371–392 (2013)
17. Morigi, M.: On the probability of generating free prosoluble groups of small rank. *Israel J. Math.* 155, 117–123 (2006)
18. Pfeiffer, G.: The subgroups of M_{24} , or how to compute the table of marks of a finite group. *Experiment. Math.* 6, 247–270 (1997)
19. Pomerance, C.: The expected number of random elements to generate a finite abelian group. *Period. Math. Hungar.* 43, 191–19 (2001)
20. Weigel, T.: On the probabilistic ζ -function of pro(finite-soluble) groups. *Forum Math.* 17, 669–698 (2005)

ANDREA LUCCHINI, UNIVERSITÀ DEGLI STUDI DI PADOVA, DIPARTIMENTO DI MATEMATICA, VIA TRIESTE 63, 35121 PADOVA, ITALY, EMAIL: LUCCHINI@MATH.UNIPD.IT