ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 48, Number 6, 2018

THE EXPECTED NUMBER OF ELEMENTS TO GENERATE A FINITE GROUP WITH d-GENERATED SYLOW SUBGROUPS

ANDREA LUCCHINI AND MARIAPIA MOSCATIELLO

ABSTRACT. Given a finite group G, let $e(G)$ be the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. If all of the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d+\kappa$, where κ is an absolute constant that is explicitly described in terms of the Riemann zeta function and is the best possible in this context. Approximately, κ equals 2.752394. If G is a permutation group of degree n, then either $G = \mathrm{Sym}(3)$ and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \kappa^*$ with $\kappa^* \sim 1.606695$. These results improve weaker bounds recently obtained by Lucchini.

1. Introduction. In 1989, Guralnick [**5**] and the first author [**10**] independently proved that, if all of the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements. A probabilistic version of this result was obtained in [**12**]. 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 by

$$\tau_G = \min\{n \geq 1 \mid \langle x_1, \ldots, x_n\rangle = G\}.$$

We denote by $e(G)$ the expectation $\mathrm{E}(\tau_G)$ of this random variable: $e(G)$ is the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. In [**12**], it was proven that, if all of the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d+\eta$ with $\eta \sim 2.875065$. This bound is not too distant from being the best possible. Indeed, in [**15**], Pomerance proved that, if Ω_d is the set of all the d-generated finite abelian groups,

2010 AMS *Mathematics subject classification.* Primary 20P05.
Keywords and phrases. Groups generation, waiting time, Sylow subgroups, permutation groups.
Received by the editors on July 22, 2017, and in revised form on February 13, 2018.
DOI:10.1216/RMJ-2018-48-6-1963

then

$$\sup_{G\in\Omega_d} e(G) = d + \sigma, \quad \text{where } \sigma \sim 2.118457.$$

However, the bound $e(G) \leq d + \eta$ is approximative, and it may be interesting to find a best possible estimation for $e(G)$. We give an exhaustive answer to this question, proving the next result.

Theorem 1.1. *Let G be a finite group. If all of the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d + \kappa$, where κ is an absolute constant that is explicitly described in terms of the Riemann zeta function and is the best possible in this context. Approximately, κ equals* 2.752394.

This bound can further be improved under some additional assumptions on G. For example, we prove that, if all the Sylow subgroups of G can be generated by d elements and G is not soluble, then $e(G) \leq d + 2.750065$ (Proposition 3.1). A stronger result holds if $|G|$ is odd.

Theorem 1.2. *Let G be a finite group of odd order. If all the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d + \widetilde{\kappa}$, with $\widetilde{\kappa} \sim 2.148668$.*

In this case, the constant $\widetilde{\kappa}$ is probably not the best possible. In particular, as suggested by the proof of Theorem 1.2, a precise estimate would require a complete knowledge of the distribution of the Fermat primes.

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements (see **[7]**); thus, Theorem 1.1 has the following consequence: if G is a permutation group of degree n, then $e(G) \leq \lfloor n/2 \rfloor + \kappa$. However, this bound is not the best possible, and a better result can be obtained:

Corollary 1.3. *If G is a permutation group of degree n, then either $G = \mathrm{Sym}(3)$ and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \kappa^*$ with $\kappa^* \sim 1.606695$.*

The number κ^* is the best possible. Let $m = \lfloor n/2 \rfloor$, and set

$$G_n = \mathrm{Sym}(2)^m$$

if m is even,

$$G_n = \mathrm{Sym}(2)^{m-1} \times \mathrm{Sym}(3)$$

if m is odd. If $n \geq 8$, then $e(G_n) - m$ increases with n and $\lim_{n\to\infty} e(G) - m = \kappa^*$.

Our proofs implicitly depend on the classification of the finite simple groups. More precisely, the proof of Theorem 1.1 requires a result, proved by Pyber, which states that, for every finite group G and every $n \geq 2$, G has at most n^2 core-free maximal subgroups of index n (this is necessary in the proof of Lemma 2.3), while the proof of Corollary 1.3 uses a bound on the chief length of a permutation group of degree n (see Theorem 5.2).

2. Preliminary results. Let G be a finite group, and use the following notation:

- For a given prime p, $d_p(G)$ is the smallest cardinality of a generating set of a Sylow p-subgroup of G.
- For a given prime p and a positive integer t, $\alpha_{p,t}(G)$ is the number of complemented factors of order p^t in a chief series of G.
- For a given prime p, $\alpha_p(G) = \sum_t \alpha_{p,t}(G)$ is the number of complemented factors of p-power order in a chief series of G.
- $\beta(G)$ is the number of nonabelian factors in a chief series of G.

Lemma 2.1. *For every finite group G, we have*:

(i) $\alpha_p(G) \leq d_p(G)$.
(ii) $\alpha_2(G) + \beta(G) \leq d_2(G)$.
(iii) *If* $\beta(G) \neq 0$, *then* $\beta(G) \leq d_2(G) - 1$.
(iv) *If* $\alpha_{2,1}(G) = 0$, *then* $\alpha_2(G) + \beta(G) \leq d_2(G) - 1$.
(v) *If* $\alpha_{p,1}(G) = 0$, *then* $\alpha_p(G) \leq d_p(G) - 1$.

Proof. (i), (ii) and (iii) are proven in [**12,** Lemma 4]. Now, assume that no complemented chief factor of G has order 2, and let $r = \alpha_2(G) + \beta(G)$. There exists a sequence

$$X_r \leq Y_r \leq \cdots \leq X_1 \leq Y_1$$

of normal subgroups of G such that, for every $1 \leq i \leq r$, Y_i/X_i is a complemented chief factor of G of even order. Note that $\beta(G/Y_1) =$

$\alpha_2(G/Y_1) = 0$; hence, G/Y_1 is a finite soluble group, all of whose complemented chief factors have odd order, but, then, G/Y_1 has odd order, and consequently, $d_2(G) = d_2(Y_1)$. Moreover, as in the proof of **[12,** Lemma 4],

$$d_2(Y_1) \geq d_2(Y_1/X_1) + r - 1.$$

Since $|Y_1/X_1| \neq 2$ and the Sylow 2-subgroups of a finite nonabelian simple group cannot be cyclic **[16,** 10.1.9], we deduce $d_2(Y_1/X_1) \geq 2$, and consequently, $d_2(G) = d_2(Y_1) \geq r+1$. This proves (iv). The proof of (v) is similar. $\square$

Recall (see **[12,** (1.1)] for more details) that

$$e(G) = \sum_{n \geq 0} (1 - P_G(n)), \tag{2.1}$$

where

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

is the probability that n randomly chosen elements of G generate G. Denote by $m_n(G)$ the number of index n maximal subgroups of G. We have (see **[9,** 11.6]):

$$1 - P_G(k) \leq \sum_{n \geq 2} \frac{m_n(G)}{n^k}. \tag{2.2}$$

Using the notation introduced in **[8,** Section 2], we say that a maximal subgroup M of G is of type A if $\mathrm{soc}(G/\operatorname{Core}_G(M))$ is abelian, of type B otherwise, and we denote by $m_n^A(G)$ (respectively, $m_n^B(G)$) the number of maximal subgroups of G of type A (respectively, B) of index n. Denote the set of the prime divisors of $|G|$ by $\pi(G)$. Given $t \in \mathbb{N}$ and $p \in \pi(G)$, define

$$\mu^*(G,t) = \sum_{k \geq t} \left(\sum_{n \geq 5} \frac{m_n^B(G)}{n^k} \right),$$

$$\mu_p(G,t) = \sum_{k \geq t} \left(\sum_{n \geq 1} \frac{m_{p^n}^A(G)}{p^{nk}} \right).$$

Lemma 2.2. *Let $t \in \mathbb{N}$. Then,*

$$e(G) \leq t + \mu^*(G,t) + \sum_{p \in \pi(G)} \mu_p(G,t).$$

Proof. By (2.1) and (2.2),

$$e(G) \leq t + \sum_{n \geq t} (1 - P_G(n)) \leq t + \sum_{k \geq t} \left(\sum_{n \geq 2} \frac{m_n(G)}{n^k} \right). \qquad \square$$

Lemma 2.3. *Let $t \in \mathbb{N}$. If $\beta(G) = 0$, then $\mu^*(G,t) = 0$. If $t \geq \beta(G) + 3$, then*

$$\mu^*(G,t) \leq \frac{\beta(G)(\beta(G)+1)}{2 \cdot 5^{t-4}} \cdot \frac{1}{4}.$$

Proof. The result follows from [**12,** Lemma 8] and its proof. $\square$

Lemma 2.4. *Let $t \in \mathbb{N}$ and $p \in \pi(G)$. If $\alpha_p(G) = 0$, then $\mu_p(G,t) = 0$.*

(i) *If $\alpha_2(G) \leq t-1$ and $\alpha_{2,u}(G) \leq t-2$ for every $u > 1$, then*

$$\mu_2(G,t) \leq \frac{1}{2^{t-\alpha_2(G)-1}}.$$

(ii) *Let p be an odd prime. If $\alpha_p(G) \leq t-2$, then*

$$\mu_p(G,t) \leq \frac{1}{p^{t-\alpha_p(G)-2}} \frac{1}{(p-1)^2}.$$

Proof. The result follows from [**12,** Lemma 7] and its proof. $\square$

Let G be a finite soluble group, and let $\mathcal{A}$ be a set of representatives for the irreducible G-modules that are G-isomorphic to some complemented chief factor of G. For every $A \in \mathcal{A}$, let δ_A be the number of complemented factors G-isomorphic to A in a chief series of G,

$$q_A = |\operatorname{End}_G(A)|, \ r_A = \dim_{\operatorname{End}_G(A)}(A),$$

$\zeta_A = 0$, if A is a trivial G-module, $\zeta_A = 1$, otherwise. Moreover, for every $l \in \mathbb{N}$, let $Q_{A,l}(s)$ be the Dirichlet polynomial, defined by

$$Q_{A,l}(s) = 1 - \frac{q_A^{l + r_A \cdot \zeta_A}}{q_A^{r_A \cdot s}}.$$

By [**4,** Satz 1], for every positive integer k, we have

$$P_G(k) = \prod_{A\in\mathcal{A}} \Big(\prod_{0\le l\le \delta_A - 1} Q_{A,l}(k)\Big). \tag{2.3}$$

For every prime p dividing $|G|$, let $\mathcal{A}_p$ be the subset of $\mathcal{A}$ consisting of the irreducible G-modules having order a power of p, and let

$$P_{G,p}(k) = \prod_{A\in\mathcal{A}_p} \Big(\prod_{0\le l\le \delta_A - 1} Q_{A,l}(k)\Big). \tag{2.4}$$

Definition 2.5. For every prime p and every positive integer α, let

$$C_{p,\alpha}(s) = \prod_{0\le i\le \alpha-1} \left(1 - \frac{p^i}{p^s}\right),$$
$$D_{p,\alpha}(s) = \prod_{1\le i\le \alpha} \left(1 - \frac{p^i}{p^s}\right).$$

Lemma 2.6. *Let G be a finite soluble group and let k be a positive integer.*

(i) *If $d_p(G) \le d$, then $P_{G,p}(k) \ge D_{p,d}(k)$.*
(ii) *If p divides $|G/G'|$, then $P_{G,p}(k) \ge C_{p,d}(k)$.*
(iii) *If $\alpha_{p,1}(G) = 0$, then $P_{G,p}(k) \ge C_{p,d}(k)$.*
(iv) *If $d_2(G) \le d$, then $P_{G,2}(k) \ge C_{2,d}(k)$.*

Proof. Suppose that $\mathcal{A}_p = \{A_1, \dots, A_t\}$, and let $q_i = q_{A_i}$, $r_i = r_{A_i}$, $\zeta_i = \zeta_{A_i}$ and $\delta_i = \delta_{A_i}$. Recall that

$$P_{G,p}(k) = \prod_{\substack{1\le i\le t\\ 0\le l\le \delta_i - 1}} Q_{A_i,l}(k). \tag{2.5}$$

By Lemma 2.1,

$$\delta_1 + \delta_2 + \dots + \delta_t = \alpha_p(G) \le d_p(G);$$

hence, the number of factors $Q_{A_i,l}(k)$ in (2.5) is at most $d_p(G)$. We order these factors in such a way that $Q_{A_i,u}(k)$ precedes $Q_{A_j,v}(k)$ if either $i < j$ or $i = j$ and $u < v$. Moreover, we order the elements of $\mathcal{A}_p$ in such a way that A_1 is the trivial G-module if p divides $|G/G'|$.

(i) Since $D_{p,d}(k) = 0$, if $k \leq d$, we may take $k > d$. To show that $P_{G,p}(k) \geq D_{p,d}(k)$, it is sufficient to show that the jth factor $Q_j(k) = Q_{A_i,l}(k)$ of $P_{G,p}(k)$ is greater than the jth factor $D_j(k) = 1 - p^j/p^k$ of $D_{p,d}(k)$. If $j \leq \delta_1$, then $Q_j(k) = Q_{A_1,l}(k)$ with $l = j - 1$. If $j > \delta_1$, then $Q_j(k) = Q_{A_i,l}(k)$ for some $i \in \{2, \ldots, t\}$ and $l \in \{0, \ldots, \delta_i - 1\}$; thus,

$$j = \delta_1 + \delta_2 + \cdots + \delta_{i-1} + l + 1 \geq l + 2.$$

In any case,

$$q_i^{r_i\zeta_i} q_i^l \leq q_i^{r_i(l+1)} \leq q_i^{r_i j}.$$

We have $q_i = p^{n_i}$ for some $n_i \in \mathbb{N}$. Since $j \leq d < k$, we deduce that

$$\frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \leq \frac{q_i^{r_i j}}{q_i^{r_i k}} = \left(\frac{p^j}{p^k}\right)^{r_i n_i} \leq \frac{p^j}{p^k}.$$

Then,

$$Q_j(k) = 1 - \frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \geq 1 - \frac{p^j}{p^k} = D_j(k).$$

(ii) Since $C_{p,d}(k) = 0$ if $k < d$, we may take $k \geq d$. To show that $P_{G,p}(k) \geq C_{p,d}(k)$, it is sufficient to show that the jth factor $Q_j(k) = Q_{A_i,l}(k)$ of $P_{G,p}(k)$ is greater than the jth factor $C_j(k) = 1 - p^{j-1}/p^k$ of $C_{p,d}(k)$. If $i = 1$, then, by the way in which we ordered the elements of $\mathcal{A}_p$, we have $Q_j(k) = C_j(k)$. Otherwise, as we see in the proof of (i), $l + 2 \leq j$; thus, $r_i\zeta_i + l \leq r_i + j - 2 \leq r_i(j-1)$. Since $j \leq d \leq k$, we deduce that

$$\frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \leq \frac{q_i^{r_i(j-1)}}{q_i^{r_i k}} \leq \frac{p^{j-1}}{p^k}$$

and

$$Q_j(k) = 1 - \frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \geq 1 - \frac{p^{j-1}}{p^k} = C_j(k).$$

(iii) Assume that no complemented chief factor of G has order p. By Lemma 2.1 (v), $\alpha_p(G) \leq d_p(G) - 1 \leq d - 1$. But, then, in the factorization of $P_{G,p}(k)$ described in (2.5), the number of factors is at most $d - 1$, and, arguing as in the proof of (i), we conclude that

$$P_{G,p}(k) \geq D_{p,d-1}(k) \geq C_{p,d}(k).$$

(iv) We may assume that $\alpha_2(G) \neq 0$ (otherwise, $P_{G,2}(k) = 1$). Since $\alpha_{2,1}(G) \neq 0$ if and only if 2 divides $|G/G'|$, the conclusion follows from (ii) and (iii). $\square$

3. The main result.

Proposition 3.1. *Let G be a finite group. If all of the Sylow subgroups of G can be generated by d elements and G is not soluble, then*

$$e(G) \leq d + \kappa^* \quad \textit{with } \kappa^* \leq 2.750065.$$

Proof. Let $\beta = \beta(G)$. Since G is not soluble, $\beta > 0$; hence, by Lemma 2.1 (ii), (iii), we have

$$1 \leq \beta \leq d_2(G) - 1 \leq d - 1$$

and

$$\alpha_2(G) \leq d_2(G) - \beta \leq d - 1.$$

We distinguish two cases:

Case (a) $\beta < d - 1$. From Lemmas 2.2, 2.3 and 2.4 and, using a rather precise approximation of $\sum_p (p-1)^{-2}$ given in [**1**], we conclude:

$$\begin{aligned} e(G) &\leq d + 2 + \mu^*(G, d+2) + \mu_2(G, d+2) + \sum_{p>2} \mu_p(G, d+2) \\ &\leq d + 2 + \frac{1}{20} + \frac{1}{4} + \sum_{p>2} \frac{1}{(p-1)^2} \leq d + 2.675065. \end{aligned}$$

Case (b) $\beta = d - 1$. By Lemma 2.1 (ii), (iv), either $\alpha_2(G) = 0$ or $\alpha_2(G) = \alpha_{2,1}(G) = 1$. In the first case, $\mu_2(G, d+2) = 0$; in the second case, $m_2^A(G) = 1$, and consequently,

$$\mu_2(G, d+2) = \sum_{k \geq d+2} \frac{m_2^A(G)}{2^k} \leq \sum_{k \geq d+2} \frac{1}{2^k} \leq \sum_{k \geq 4} \frac{1}{2^k} \leq \frac{1}{8}.$$

From Lemmas 2.2, 2.3 and 2.4, we conclude:

$$\begin{aligned} e(G) &\leq d+2+\mu^*(G,d+2)+\mu_2(G,d+2)+\sum_{p>2}\mu_p(G,d+2) \\ &\leq d+2+\frac{1}{4}+\frac{1}{8}+\sum_{p>2}\frac{1}{(p-1)^2} \leq d+2.750065. \qquad \square \end{aligned}$$

The previous proposition reduces the proof of Theorem 1.1 to the particular case when G is soluble. In order to deal with this case, we shall introduce, for every positive integer d and every set of primes π, a supersoluble group $H_{\pi,d}$, all of whose Sylow subgroups are d-generated and with the property that $e(G) \leq e(H_{\pi,d})$, whenever G is soluble, $\pi(G) \subseteq \pi$ and the Sylow subgroups of G are d-generated.

Definition 3.2. Let π be a finite set of prime numbers with $2 \in \pi$, and let d be a positive integer. We define $H_{\pi,d}$ as the semidirect product of A with $\langle y, z_1, \ldots, z_{d-1}\rangle$, where A is isomorphic to

$$\prod_{p\in\pi\setminus\{2\}} C_p^d$$

and $\langle y, z_1, \ldots, z_{d-1}\rangle$ is isomorphic to C_2^d and acts on A via $x^y = x^{-1}$, $x^{z_i} = x$ for all $x \in A$ and $1 \leq i \leq d-1$. Thus,

$$H_{\pi,d} \cong \left(\left(\prod_{p\in\pi\setminus\{2\}} C_p^d\right) \rtimes C_2\right) \times C_2^{d-1}.$$

Theorem 3.3. *Let G be a finite soluble group. If all of the Sylow subgroups of G can be generated by d elements, then $e(G) \leq e(H_{\pi,d})$, where $\pi = \pi(G) \cup \{2\}$.*

Proof. Let $H = H_{\pi,d}$, $p \in \pi$, $k \in \mathbb{N}$. Let $\mathcal{A}$ be a set of representatives for the irreducible H-modules that are H-isomorphic to some complemented chief factor of H, and let $\mathcal{A}_p$ be the subset of $\mathcal{A}$ consisting of the irreducible H-modules having as order a power of p. For every $p \in \pi$, $\mathcal{A}_p$ contains a unique element A_p. Moreover, $|A_p| = p$, $\delta_{A_p} = d$ and $\zeta_{A_p} = 1$ if $p \neq 2$, while $\zeta_{A_2} = 0$. Hence, by (2.4), $P_{H,p}(k) = D_{p,d}(k)$ if $p \neq 2$, while $P_{H,2}(k) = C_{2,d}(k)$. From Lemma 2.6, $P_{G,p}(k) \geq P_{H,p}(k)$

for every $p \in \pi(G)$. This implies

$$P_G(k) = \prod_{p\in\pi(G)} P_{G,p}(k) \geq \prod_{p\in\pi} P_{H,p}(k) = P_H(G),$$

and consequently,

$$e(G) = \sum_{k\geq 0}(1 - P_G(k)) \leq \sum_{k\geq 0}(1 - P_H(k)) = e(H). \qquad \square$$

Definition 3.4. Let π be a finite set of prime numbers with $2 \in \pi$, and let d be a positive integer. We set $e_d = \sup_\pi e(H_{\pi,d})$ and $\kappa = \sup_d(e_d - d)$.

Let $\pi^* = \pi \setminus \{2\}$. Since $P_{H_{\pi,d}}(k) = 0$, for all $k \leq d$, we have

$$\begin{aligned} e(H_{\pi,d}) &= \sum_{k\geq 0}(1 - P_{H_{\pi,d}}(k)) = d + 1 + \sum_{k\geq d+1}\left(1 - C_{2,d}(k)\prod_{p\in\pi^*} D_{p,d}(k)\right) \\ &= d+1+\sum_{k\geq d+1}\left(1-\prod_{1\leq i\leq d}\left(1-\frac{2^{i-1}}{2^k}\right)\prod_{p\in\pi^*}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^k}\right)\right) \\ &= d+1+\sum_{t\geq 0}\left(1-\prod_{1\leq i\leq d}\left(1-\frac{2^{i-1}}{2^{t+(d+1)}}\right)\prod_{p\in\pi^*}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^{t+(d+1)}}\right)\right). \end{aligned}$$

We immediately deduce that $e(H_{\pi,d}) - d$ increases as d increases. Moreover, we have

$$\begin{aligned} e_d - d &= \sup_\pi(e(H_{\pi,d}) - d) \\ &= 1 + \sum_{k\geq d+1}\left(1 - \frac{(1-1/2^k)}{(1-2^d/2^k)}\prod_p\prod_{1\leq i\leq d}\left(1 - \frac{p^i}{p^k}\right)\right). \end{aligned}$$

For $k = d+1$, the double product tends to 0, while, for $k \geq d+2$, it tends to $\prod_{1\leq i\leq d}\zeta(k-i)^{-1}$, where ζ denotes the Riemann zeta function. Hence, we obtain

$$\begin{aligned} e_d - d &= 2 + \sum_{k\geq d+2}\left(1 - \frac{(1-1/2^k)}{(1-2^d/2^k)}\prod_{1\leq i\leq d}\zeta(k-i)^{-1}\right) \\ &= 2 + \sum_{j\geq 1}\left(1 - \frac{(1-1/2^{j+(d+1)})}{(1-1/2^{j+1})}\prod_{1\leq l\leq d}\zeta(j+l)^{-1}\right) \\ &= 2 + \sum_{j\geq 1}\left(1 - \left(\frac{2^{j+1}-2^{-d}}{2^{j+1}-1}\right)\prod_{1+j\leq n\leq d+j}\zeta(n)^{-1}\right). \end{aligned}$$

Let $c = \prod_{2\leq n\leq \infty} \zeta(n)^{-1}$. Since $e_d - d$ increases as d grows, we get

$$\begin{aligned}\kappa &= \lim_{d\to\infty} e_d - d \\ &= 2 + \left(1 - \left(\frac{2^2}{2^2-1}\right)c\right) + \sum_{j\geq 2}\left(1 - \left(\frac{2^{j+1}}{2^{j+1}-1}\right)c \prod_{2\leq n\leq j}\zeta(n)\right) \\ &= 2 + \left(1 - \frac{4}{3}\cdot c\right) + \sum_{j\geq 2}\left(1 - \left(1 + \frac{1}{2^{j+1}-1}\right)c \prod_{2\leq n\leq j}\zeta(n)\right).\end{aligned}$$

Using the computer algebra system `PARI/GP` [**14**], we obtain

$$\kappa = 2 + \left(1 - \frac{4}{3}\cdot c\right) + \sum_{j\geq 2}\left(1 - \left(1 + \frac{1}{2^{j+1}-1}\right)c \prod_{2\leq n\leq j}\zeta(n)\right) \sim 2.752395.$$

Combining this result with Proposition 3.1 and Theorem 3.3, we obtain the proof of Theorem 1.1.

4. Finite groups of odd order.

Theorem 4.1. *Let G be a finite soluble group. There exists a finite supersoluble group H, such that*

(i) $\pi(H) = \pi(G)$,
(ii) $P_G(k) \geq P_H(k)$ *for all* $k \in \mathbb{N}$,
(iii) $d_p(G) \geq d_p(H)$ *for all* $p \in \pi(G)$,
(iv) $\pi(G/G') \subseteq \pi(H/H')$.

Proof. Let $\pi(G) = \{p_1, \ldots, p_n\}$ with $p_1 \leq \cdots \leq p_n$. For $i \in \{1, \ldots, n\}$, set $\pi_i = \{p_1, \ldots, p_i\}$. We will prove, by induction on i, that, for every $i \in \{1, \ldots, n\}$, there exists a supersoluble group H_i such that $\pi(H_i) = \pi_i$ and, for every $j \leq i$,

(i) $P_{H_i,p_j}(k) \leq P_{G,p_j}(k)$ for all $k \in \mathbb{N}$;
(ii) $d_{p_j}(H_i) \leq d_{p_j}(G)$;
(iii) if C_{p_j} is an epimorphic image of G, then C_{p_j} is an epimorphic image of H_i;
(iv) $\pi_i \cap \pi(G/G') \subseteq \pi(H_i/H_i')$.

Assume that H_i has been constructed, and set $p = p_{i+1}$ and $d_p = d_p(G)$. We distinguish two different cases:

Case (i). Either p divides $|G/G'|$ or G contains no complemented chief factor of order p. We consider the direct product $H_{i+1} = H_i \times C_p^{d_p}$. Clearly,

$$P_{H_{i+1},p_j}(k) = P_{H_i,p_j}(k) \le P_{G,p_j}(k) \quad \text{if } j \le i.$$

Moreover, by Lemma 2.6 (ii), (iii),

$$P_{H_{i+1},p}(k) = C_{p,d_p}(k) \le P_{G,p}(k).$$

Case (ii). p does not divide $|G/G'|$, but G contains a complemented chief factor which is isomorphic to a nontrivial G-module, say A, of order p. In this case, $G/C_G(A)$ is a nontrivial cyclic group whose order divides $p-1$. Let q be a prime divisor of $|G/C_G(A)|$ (it must be $q = p_j$ for some $j \le i$). Since q divides $|G/G'|$, we have that q divides also $|H_i/H_i'|$; hence, there exists a normal subgroup N of H_i with $H_i/N \cong C_q$ and a nontrivial action of H_i on C_p with kernel N. We use this action to construct the supersoluble group $H_{i+1} = C_p^{d_p} \rtimes H_i$. Clearly, $P_{H_{i+1},p_j}(k) = P_{H_i,p_j}(k) \le P_{G,p_j}(k)$ if $j \le i$. Moreover, by Lemma 2.6 (i), $P_{H_{i+1},p}(k) = D_{p,d_p}(k) \le P_{G,p}(k)$.

The proof is complete, noting that $H = H_n$ satisfies the requests in the statement. □

Proof of Theorem 1.2. Let $\pi = \pi(G)$. From Theorem 4.1, there exists a supersoluble group H such that $\pi(H) = \pi$, $d_p(H) \le d$ for every $p \in \pi$ and $P_G(k) \ge P_H(k)$ for every $k \in \mathbb{N}$. In particular,

$$e(G) = \sum_{k\ge 0}(1 - P_G(k)) \le \sum_{k\ge 0}(1 - P_H(k)) = e(H).$$

Since H is supersoluble, if A is H-isomorphic to a chief factor of H, then $|A| = p$ for some $p \in \pi$ and $H/C_H(A)$ is a cyclic group of order dividing $p-1$. If p is a Fermat prime, then $H/C_H(A)$ is a 2-group and, since $|H|$ is odd, we must have $H = C_H(A)$. This implies that, if $p \in \pi$ is a Fermat prime, then $P_{H,p}(k) = C_{p,d_p(H)}(k) \ge C_{p,d}(k)$. For all of the other primes in π, by Lemma 2.6 (i), we have $P_{H,p}(k) \ge D_{p,d}(k)$. Therefore, denoting the set of Fermat primes by Λ and the set of the remaining odd primes by Δ, we obtain

$$P_H(k) = \prod_{p\in\pi} P_{H,p}(k) \ge \prod_{p\in\Lambda} C_{p,d}(k) \prod_{p\in\Delta} D_{p,d}(k).$$

It follows that

$$\begin{aligned}
e(H) &= \sum_{k\geq 0}(1-P_H(k)) \\
&\leq \sum_{k\geq 0}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^k}\right)\prod_{\substack{p\in\Delta\\ p\neq 2}}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^k}\right)\right) \\
&= d+1+\sum_{k\geq d+1}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^k}\right)\prod_{p\in\Delta}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^k}\right)\right) \\
&= d+1+\sum_{t\geq 0}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^{t+(d+1)}}\right)\prod_{p\in\Delta}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^{t+(d+1)}}\right)\right).
\end{aligned}$$

Let

$$\widetilde{\kappa}_d=\sum_{t\geq 0}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^{t+(d+1)}}\right)\prod_{p\in\Delta}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^{t+(d+1)}}\right)\right)+1.$$

It can easily be verified that $\widetilde{\kappa}_d$ increases as d increases. Let

$$b=\prod_{1\leq n\leq\infty}\left(1-\frac{1}{2^n}\right)^{-1}, \qquad c=\prod_{2\leq n\leq\infty}\zeta(n)^{-1},$$

and let $\Lambda^*=\{3,\ 5,\ 17,\ 257,\ 65537\}$ be the set of the known Fermat primes. Similar computations to those in the final part of Section 3 lead to the conclusion:

$$\begin{aligned}
\widetilde{\kappa}_d &\leq 3-\frac{b\cdot c}{2}\prod_{p\in\Lambda}\frac{p^2}{p^2-1} \\
&\quad +\sum_{j\geq 2}\left(1-b\prod_{1\leq n\leq j}\left(1-\frac{1}{2^n}\right)\prod_{p\in\Lambda}\left(1+\frac{1}{p^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right) \\
&\leq 3-\frac{b\cdot c}{2}\prod_{p\in\Lambda^*}\frac{p^2}{p^2-1} \\
&\quad +\sum_{j\geq 2}\left(1-b\prod_{1\leq n\leq j}\left(1-\frac{1}{2^n}\right)\prod_{p\in\Lambda^*}\left(1+\frac{1}{p^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right).
\end{aligned}$$

Let

$$\widetilde{\kappa} = 3 - \frac{b \cdot c}{2} \prod_{p \in \Lambda^*} \frac{p^2}{p^2 - 1}$$
$$+ \sum_{j \geq 2} \left(1 - b \prod_{1 \leq n \leq j} \left(1 - \frac{1}{2^n}\right) \prod_{p \in \Lambda^*} \left(1 + \frac{1}{p^{j+1} - 1}\right) c \prod_{2 \leq n \leq j} \zeta(n)\right).$$

With the aid of `PARI/GP`, we get that $\widetilde{\kappa} \sim 2.148668$. □

5. Permutation groups.

Theorem 5.1 ([**7**]). *If G is a p-subgroup of* $\mathrm{Sym}(n)$, *then G can be generated by $\lfloor n/p \rfloor$ elements.*

Theorem 5.2 ([**13,** Theorem 10.0.5]). *The chief length of a permutation group of degree n is at most $n - 1$.*

Lemma 5.3. *If $G \leq \mathrm{Sym}(n)$ and $n \geq 8$, then $\beta(G) \leq \lfloor n/2 \rfloor - 3$.*

Proof. Let $R(G)$ be the soluble radical of G. From [**6,** Theorem 2], $G/R(G)$ has a faithful permutation representation of degree at most n, so we may assume that $R(G) = 1$. In particular,

$$\mathrm{soc}(G) = S_1 \times \cdots \times S_r,$$

where $S_1, \ldots, S_r$ are nonabelian simple groups and, by [**2,** Theorem 3.1], $n \geq 5r$. Let

$$K = N_G(S_1) \cap \cdots \cap N_G(S_r).$$

We have that $K/\mathrm{soc}(G)$ is soluble and that $G/K \leq \mathrm{Sym}(r)$; thus, by Theorem 5.2, $\beta(G/K) \leq r - 1$ (and, indeed, $\beta(G/K) = 0$ if $r \leq 4$). However, then, $\beta(G) \leq 2r - 1 \leq 2\lfloor n/5 \rfloor - 1$ if $r \geq 5$, $\beta(G) \leq r \leq \lfloor n/5 \rfloor$ otherwise. □

Lemma 5.4. *Suppose that $G \leq \mathrm{Sym}(n)$ with $n \geq 8$. If G is not soluble, then*

$$e(G) \leq \lfloor n/2 \rfloor + 1.533823.$$

Proof. Let $m = \lfloor n/2 \rfloor$. From Theorem 5.1, $d_2(G) \leq m$. Since G is not soluble, we must have $\beta(G) \geq 1$. By Lemma 5.3, $\beta(G) \leq m - 3$;

hence, by Lemma 2.3, $\mu^*(G,m) \leq 1/4$. From Lemma 2.1 (ii), (iv), $\alpha_2(G) \leq m-1$ and $\alpha_{2,u}(G) \leq m-2$ for every $u > 1$; hence, by Lemma 2.4, $\mu_2(G,m) \leq 1$. If $p \geq 5$, then, by Theorem 5.1,

$$m - \alpha_p(G) \geq m - d_p(G) \geq m - \lfloor n/5 \rfloor \geq 3;$$

thus, by Lemma 2.4, $\mu_p(G,m) \leq (p(p-1)^2)^{-1}$. Since $n \geq 8$, we have $m - \alpha_3(G) \geq m - \lfloor n/3 \rfloor \geq 2$ if $n \neq 9$. On the other hand, it can be easily verified that $\alpha_3(G) \leq 2$ for every non-soluble subgroup G of $\mathrm{Sym}(9)$; hence, $m - \alpha_3(G) \geq 2$ also when $n = 9$. But, then, again by Lemma 2.4, $\mu_3(G,m) \leq 1/4$. It follows that

$$\begin{aligned} e(G) &\leq m + \mu^*(G,m) + \mu_2(G,m) + \mu_3(G,m) + \sum_{p>3} \mu_p(G,m) \\ &\leq m + \frac{1}{4} + 1 + \frac{1}{4} + \sum_{p\geq 5} \frac{1}{p(p-1)^2} \leq m + \frac{3}{2} + \sum_{n \geq 5} \frac{1}{n(n-1)^2} \\ &\leq m + 1.533823. \end{aligned}$$

□

Lemma 5.5. *Suppose that $G \leq \mathrm{Sym}(n)$ with $n \geq 8$. If G is soluble and $\alpha_{2,1}(G) < \lfloor n/2 \rfloor$, then*

$$e(G) \leq \lfloor n/2 \rfloor + 1.533823.$$

Proof. Let $\alpha = \alpha_{2,1}(G)$, $\alpha^* = \sum_{i>1} \alpha_{2,i}(G)$ and $m = \lfloor n/2 \rfloor$. Note that $\alpha^* \leq m-1$ by Lemma 2.1 (iv). Set

$$\mu_{2,1}(G,t) = \sum_{k \geq t} \frac{m_2^A(G)}{2^k}, \qquad \mu_{2,2}(G,t) = \sum_{k\geq t} \left(\sum_{n \geq 2} \frac{m_{2^n}^A(G)}{2^{nk}} \right).$$

We distinguish two cases:

Case (1). $\alpha_{2,u}(G) < m-1$ for every $u \geq 2$. Since $m_2^A(G) = 2^\alpha - 1$, we have

$$\mu_{2,1}(G,m) \leq \sum_{k \geq m} \frac{2^\alpha}{2^k} = \frac{1}{2^{m-\alpha-1}} \leq 1.$$

Moreover, arguing as in the proof of [**12,** Lemma 7], we deduce that

$$\mu_{2,2}(G,m) \leq \frac{1}{2^{m-\alpha^*-1}} \leq 1.$$

Note that, if $\alpha = m-1$, then $\alpha^* \leq 1$, and consequently, $\mu_{2,2}(G,m) \leq 2^{2-m} \leq 1/4$. Similarly, if $\alpha^* = m-1$, then $\alpha \leq 1$ and $\mu_{2,1}(G,m) \leq$

$2^{2-m} \leq 1/4$. If follows that

$$\mu_2(G,m) = \mu_{2,1}(G,m) + \mu_{2,2}(G,m) \leq 5/4.$$

Except for the case when $n = 9$ and $\alpha_3(G) = 3$, arguing as near the end of the proof of Lemma 5.4, we conclude that

$$\begin{aligned} e(G) &\leq m + \mu_2(G,m) + \mu_3(G,m) + \sum_{p>3} \mu_p(G,m) \\ &\leq m + \frac{5}{4} + \frac{1}{4} + \sum_{p\geq 5} \frac{1}{p(p-1)^2} \leq m + 1.533823. \end{aligned}$$

It remains to deal with the case when G is a soluble subgroup of $\mathrm{Sym}(9)$ with $\alpha_3(G) = 3$. This occurs only if G is contained in the wreath product $\mathrm{Sym}(3) \wr \mathrm{Sym}(3)$. In particular, $\alpha_2(G) \leq 3$. If $\alpha_2(G) \leq 2$, then, by Lemma 2.4,

$$e(G) \leq 5 + \mu_2(G,5) + \mu_3(G,5) \leq 5 + 1/4 + 1/4 = 5.5.$$

We have $\alpha_2(G) = \alpha_3(G) = 3$ only in two cases: $\mathrm{Sym}(3) \times \mathrm{Sym}(3) \times \mathrm{Sym}\,3$ and $\langle (1,2,3),(4,5,6),(1,4)(2,5)(3,6),(1,2)(4,5)\rangle \times \mathrm{Sym}(3)$. In these two cases, G contains exactly 16 maximal subgroups, 7 of index 2 and 9 of index 3. But, then,

$$\begin{aligned} e(G) &\leq 4 + \sum_{k\geq 4} \frac{m_2(G)}{2^k} + \sum_{k\geq 4} \frac{m_3(G)}{3^k} \\ &= 4 + \sum_{k\geq 4} \frac{7}{2^k} + \sum_{k\geq 4} \frac{9}{3^k} \\ &= 4 + \frac{7}{8} + \frac{1}{6} \sim 5.041667. \end{aligned}$$

Case (2). $\alpha_{2,u}(G) = m-1$ for some $u \geq 2$. In this case, $m_2^A(G) \leq 1$; so,

$$\mu_{2,1}(G,m+1) \leq \sum_{k\geq m+1} \frac{1}{2^k} = \frac{1}{2^m} \leq \frac{1}{16}.$$

Moreover, by [**12,** Lemma 5], $m_{2^u}^A(G) \leq 2^{u\alpha_{2,t}(G)+u}$, which yields:

$$\mu_{2,2}(G,m+1) = \sum_{k\geq m+1} \left(\sum_{n\geq 2} \frac{m_{2^n}^A(G)}{2^{nk}} \right)$$

$$= \sum_{k \geq m+1} \frac{m^A_{2^u}(G)}{2^{uk}} \leq \sum_{k \geq m+1} \frac{2^{u\alpha_{2,t}(G)+u}}{2^{uk}}$$
$$\leq \sum_{k \geq m+1} \frac{2^{um}}{2^{uk}} = \frac{1}{2^u - 1} \leq \frac{1}{3}.$$

If $p \geq 5$, then $m - \alpha_p(G) \geq 3$; thus, by Lemma 2.4, $\mu_p(G, m+1) \leq (p(p-1))^{-2}$. Moreover, $m - \alpha_3(G) \geq 2$ (note that there is no subgroup of $\mathrm{Sym}(9)$ with $\alpha_3(G) = 3$ and $\alpha_{2,u}(G) = 3$ for some $u \geq 2$). Therefore, again by Lemma 2.4, $\mu_3(G, m+1) \leq 1/12$. It follows that

$$\begin{aligned} e(G) &\leq m + 1 + \mu_{2,1}(G, m+1) + \mu_{2,2}(G, m+1) \\ &\quad + \mu_3(G, m+1) + \sum_{p>3} \mu_p(G, m+1) \\ &\leq m + 1 + \frac{1}{16} + \frac{1}{3} + \frac{1}{12} + \sum_{p \geq 5} \frac{1}{p^2(p-1)^2} \\ &\leq m + 71/48 + \sum_{n \geq 5} \frac{1}{n^2(n-1)^2} \leq m + 1.484316. \end{aligned}$$ □

When $G \leq \mathrm{Sym}(n)$ and $n \leq 7$, the precise value of $e(G)$ can be computed by `GAP` **[3]** using the formula

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

where μ_G is the Möbius function defined on the subgroup lattice of G (see **[11,** Theorem 1]). The crucial information is contained in the next lemma.

Lemma 5.6. *Suppose that* $G \leq \mathrm{Sym}(n)$ *with* $n \leq 7$. *Either* $e(G) \leq \lfloor n/2 \rfloor + 1$, *or one of the following cases occurs*:

(1) $G \cong \mathrm{Sym}(3)$, $n = 3$, $e(G) = 29/10$;
(2) $G \cong C_2 \times C_2$, $n = 4$, $e(G) = 10/3$;
(3) $G \cong D_8$, $n = 4$, $e(G) = 10/3$;
(4) $G \cong C_2 \times \mathrm{Sym}(3)$, $n = 5$, $e(G) = 1181/330$;
(5) $G \cong C_2 \times C_2 \times C_2$, $n = 6$, $e(G) = 94/21$;
(6) $G \cong C_2 \times D_8$, $n = 6$, $e(G) = 94/21$;
(7) $G \cong C_2 \times C_2 \times \mathrm{Sym}(3)$, $n = 7$, $e(G) = 241789/53130$;
(8) $G \cong D_8 \times \mathrm{Sym}(3)$, $n = 7$, $e(G) = 241789/53130$.

Theorem 5.7. *Let G be a permutation group of degree $n \neq 3$. If $\alpha_{2,1}(G) = \lfloor n/2 \rfloor$, then $e(G) \leq \lfloor n/2 \rfloor + \nu$, with $\nu \sim 1.606695$.*

Proof. Let $m = \lfloor n/2 \rfloor$. We have that $\alpha_{2,1}(G) = m$ if and only if C_2^m is an epimorphic image of G. If C_2^m is an epimorphic image of G, then, by [**7,** main theorem], the group G is the direct product of its transitive constituents, and each constituent is one of the following: Sym(2) of degree 2, Sym(3) of degree 3, $C_2 \times C_2$ and D_8 of degree 4, and the central product $D_8 \circ D_8$ of degree 8. Consequently:

$$G/\operatorname{Frat}(G) \simeq \begin{cases} C_2^m & \text{if } n = 2m, \\ C_2^{m-1} \times \operatorname{Sym}(3) & \text{if } n = 2m+1. \end{cases}$$

Therefore, by (2.3),

$$P_G(k) = P_{G/\operatorname{Frat}(G)}(k) = \prod_{0 \leq i \leq m-1} \left(1 - \frac{2^i}{2^k}\right)\left(1 - \frac{3}{3^k}\right)^{n-2m}.$$

Setting $\eta = 0$ if n is even, and $\eta = 1$ otherwise, we have

$$\begin{aligned} e(G) &= \sum_{k\geq 0}(1 - P_G(k)) \leq \sum_{k \geq 0}\left(1 - \prod_{0 \leq i \leq m-1}\left(1 - \frac{2^i}{2^k}\right)\left(1 - \frac{3}{3^k}\right)^{\eta}\right) \\ &= m + \sum_{k \geq m}\left(1 - \prod_{0 \leq i \leq m-1}\left(1 - \frac{2^i}{2^k}\right)\left(1 - \frac{3}{3^k}\right)^{\eta}\right) \\ &= m + \sum_{j \geq 0}\left(1 - \prod_{1 \leq l \leq m}\left(1 - \frac{1}{2^{j+l}}\right)\left(1 - \frac{3}{3^{j+m}}\right)^{\eta}\right). \end{aligned}$$

Set

$$\omega_{m,\eta} = \sum_{j \geq 0}\left(1 - \prod_{1 \leq l \leq m}\left(1 - \frac{1}{2^{j+l}}\right)\left(1 - \frac{3}{3^{j+m}}\right)^{\eta}\right).$$

Clearly, $\omega_{m,0}$ increase with m. On the other hand, if $m \geq 4$ and $j \geq 0$, then

$$\left(1 - \frac{1}{2^{j+m+1}}\right)\left(1 - \frac{3}{3^{j+m+1}}\right) \leq \left(1 - \frac{3}{3^{j+m}}\right),$$

and thus, $\omega_{m,1} \leq \omega_{m+1,1}$ if $m \geq 4$. Moreover,

$$\lim_{m\to\infty} \omega_{m,1} = \lim_{m \to \infty} \omega_{m,0} \sim 1.606695.$$

Then, $e(G) \leq m + 1.606695$ whenever $m \geq 4$. The values of $e(G)$ when n is small are given in the following table (which also indicates how fast $e(G) - m$ tends to 1.606695).

TABLE 1.

n	$e(G)$	n	$e(G)$
2	2	9	$\frac{4633553}{832370} \sim 5.566699$
3	$\frac{29}{10} = 2.900000$	10	$\frac{7134}{1085} \sim 6.575115$
4	$\frac{10}{3} \sim 3.333334$	11	$\frac{3227369181}{490265930} \sim 6.582895$
5	$\frac{1181}{330} \sim 3.578788$	12	$\frac{74126}{9765} \sim 7.590988$
6	$\frac{94}{21} \sim 4.476191$	13	$\frac{6399598043131}{842767133670} \sim 7.593554$
7	$\frac{241789}{53130} \sim 4.550894$	14	$\frac{10663922}{1240155} \sim 8.598862$
8	$\frac{194}{35} \sim 5.542857$	15	$\frac{70505670417749503}{8198607229768494} \sim 8.599713$

From the information contained in Table 1, we deduce that $e(G) \leq m + 1.606695$, except when $G = \mathrm{Sym}(3)$. $\square$

REFERENCES

1. H. Cohen, *High precision computation of Hardy-Littlewood constants*, preprint, `https://www.math.u-bordeaux.fr/~hecohen/`.

2. D. Easdown and C. Praeger, *On minimal faithful permutation representations of finite groups*, Bull. Australian Math. Soc. **38** (1988), 207–220.

3. The GAP Group, GAP–*Groups, algorithms, and programming*, version `4.7.7`, `http://www.gap-system.org` (2015).

4. W. Gaschütz, *Die Eulersche Funktion endlicher auflösbarer Gruppen*, Illinois J. Math. **3** (1959), 469–476.

5. R. Guralnick, *On the number of generators of a finite group*, Arch. Math. **53** (1989), 521–523.

6. D. Holt, *Representing quotients of permutation groups*, Quart. J. Math. Oxford **48** (1997), 347–350.

7. L.G. Kovács and C.E. Praeger, *Finite permutation groups with large abelian quotients*, Pacific J. Math. **136** (1989), 283-292.

8. A. Lubotzky, *The expected number of random elements to generate a finite group*, J. Algebra **257** (2002), 452–495.

9. A. Lubotzky and D. Segal, *Subgroup growth*, Progr. Math. **212** (2003).

10. A. Lucchini, *A bound on the number of generators of a finite group*, Arch. Math. **53** (1989), 313–317.

11. ———, *The expected number of random elements to generate a finite group*, Monatsh. Math. **181** (2016), 123-142.

12. ———, *A bound on the expected number of random elements to generate a finite group all of whose Sylow subgroups are d-generated*, Arch. Math. **107** (2016), 1-8.

13. N.E. Menezes, *Random generation and chief length of finite groups*, Ph.D. dissertation, `http://hdl.handle.net/10023/3578`.

14. The PARI Group, *PARI/GP* version `2.9.0`, University of Bordeaux, 2016, `http://pari.math.u-bordeaux.fr/`.

15. C. Pomerance, *The expected number of random elements to generate a finite abelian group*, Period. Math. Hungar. **43** (2001), 191–198.

16. D. Robinson, *A course in the theory of groups*, Grad. Texts Math. **80** (1993).

Università degli Studi di Padova, Dipartimento di Matematica, "Tullio Levi-Civita," Italy
Email address: lucchini@math.unipd.it

Università degli Studi di Padova, Dipartimento di Matematica, "Tullio Levi-Civita," Italy
Email address: moscatie@math.unipd.it, mariapia.moscatiello@gmail.com