The expected number of random elements to generate a finite group

Andrea Lucchini

Università di Padova, Italy

ISCHIA GROUP THEORY 2018
March, 19th - March, 23rd

There are 24 balls in a box, corresponding to the elements of Sym(4). One of the balls is randomly chosen, and then returned to the box. We repeat this procedure until the chosen elements generate Sym(4) and at the end we count how many balls have been chosen.

There are 24 balls in a box, corresponding to the elements of Sym(4). One of the balls is randomly chosen, and then returned to the box. We repeat this procedure until the chosen elements generate Sym(4) and at the end we count how many balls have been chosen.

Repeat the procedure many times, and compute the average of the numbers of chosen elements. Which value can we expect to obtain?

There are 24 balls in a box, corresponding to the elements of Sym(4). One of the balls is randomly chosen, and then returned to the box. We repeat this procedure until the chosen elements generate Sym(4) and at the end we count how many balls have been chosen.

Repeat the procedure many times, and compute the average of the numbers of chosen elements. Which value can we expect to obtain?

This average will be approximatively

$$\frac{164317}{53130} \sim 3.0927.$$

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

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

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

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

We denote by

$$e(G) = \mathrm{E}(\tau_G) = \sum_{n \in \mathbb{N}} n \cdot P(\tau_G = n)$$

the expectation 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.

Example

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

$$e(C_p) = \frac{p}{p-1}.$$

Example

Let $G = D_{2p}$ be the dihedral group of order $2p$, with p an odd prime.

$\langle g_1, \dots, g_n \rangle = G \Leftrightarrow$ there exist $1 \leq i < j \leq n$ s.t. $g_i \neq 1$ and $g_j \notin \langle g_i \rangle$.

- The number of trials 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 $p_1 = \frac{p}{2p-1}$, 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 $E_1 = \frac{2p}{2p-2}$.
- With probability $p_2 = \frac{p-1}{2p-1}$, x has order p: in this case the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2p-p}{2p}$ and expectation $E_2 = \frac{2p}{2p-p}$.

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

Example

Let $G = D_{2p}$ be the dihedral group of order $2p$, with p an odd prime.

$\langle g_1, \ldots, g_n \rangle = G \Leftrightarrow$ there exist $1 \leq i < j \leq n$ s.t. $g_i \neq 1$ and $g_j \notin \langle g_i \rangle$.

- The number of trials 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 $p_1 = \frac{p}{2p-1}$, 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 $E_1 = \frac{2p}{2p-2}$.
- With probability $p_2 = \frac{p-1}{2p-1}$, x has order p: in this case the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2p-p}{2p}$ and expectation $E_2 = \frac{2p}{2p-p}$.

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

In particular $e(\mathrm{Sym}(3)) = \frac{29}{10}$.

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.

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

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

denoting by

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

the probability that n randomly chosen elements of G generate G.

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

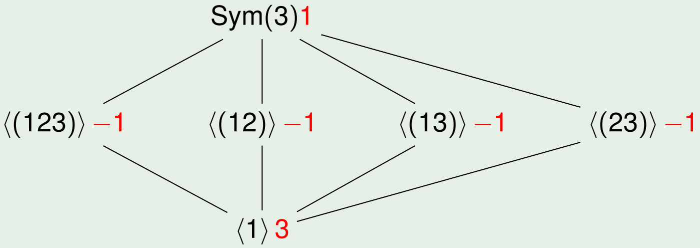
Consider the Möbius function defined on the subgroup lattice of G by setting $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{H<K} \mu_G(K)$ for any $H < G$.

Theorem (AL 2015)

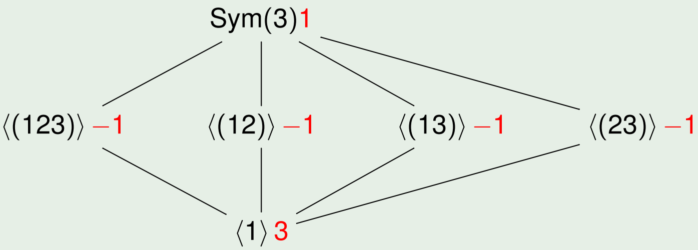
If G is a nontrivial finite group, then

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

Example: $G = \mathrm{Sym}(3)$



Example: $G = \mathrm{Sym}(3)$



$$e(\mathrm{Sym}(3)) = -\sum_{H<\mathrm{Sym}(3)} \frac{\mu_{\mathrm{Sym}(3)}(H)|\mathrm{Sym}(3)|}{|\mathrm{Sym}(3)|-|H|}$$

$$= \frac{6}{6-3} + 3\left(\frac{6}{6-2}\right) - \frac{3\cdot 6}{6-1} = \frac{29}{10}$$

PROOF.

As it was noticed by P. Hall:

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

Proof.

As it was noticed by P. Hall:

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

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

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

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

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 $\mathrm{E}(\tau_G^2)$ and by $\mathrm{var}(\tau_G) = e_2(G) - e(G)^2$ the variance of τ_G.

The Chebyshev's inequality:

$$P(|\tau_G - e(G)| \geq k) \leq \frac{\mathrm{var}(\tau_G)}{k^2}.$$

THEOREM (AL 2015)

If G is a nontrivial finite group, then

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

Theorem (AL 2015)

If G is a nontrivial finite group, then

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

Example

$e(\mathrm{Alt}(4)) = \frac{163}{66} \sim 2.4697, \quad e_2(\mathrm{Alt}(4)) = \frac{7331}{1089} \sim 6.7319.$

Example

$e(\mathrm{Sym}(4)) = \frac{164317}{53130} \sim 3.0927, \quad e_2(\mathrm{Sym}(4)) = \frac{7840917881}{705699225} \sim 11.1108.$

Example

$$e(D_{2p}) = 2 + \frac{2p^2}{(2p-1)(2p-2)}, \; e_2(D_{2p}) = 6 + \frac{2p^2(12p^2-6p-2)}{(2p-1)^2(2p-2)^2}.$$

Let S be a finite nonabelian simple group. Since $d(S) = 2$ we have $2 \leq (1-P_S(0))+(1-P_S(1))+(1-P_S(2)) = 3-P_S(2) \leq e(S) \leq \frac{2}{P_S(2)}$.

Results of Dixon, Kantor-Lubotzky and Liebeck-Shalev establish that that $P_S(2) \to 1$ as $|S| \to \infty$, so

$$\lim_{|S|\to\infty} e(S) = 2.$$

Moreover

$$\lim_{|S|\to\infty} e_2(S) = 4, \qquad \lim_{|S|\to\infty} \mathrm{var}(\tau_S) = 0.$$

Except for very few cases, $P_S(2) > 9/10$ (and so $e(S) \leq 20/9$); the exceptional cases are listed in the following table:

TABLE:

S	$P_S(2)$	$e(S)$	$e_2(S)$	$\mathrm{var}(S)$
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

Theorem (AL 2015)

Let S be a finite nonabelian simple group. Then

$$e(S) \leq e(\mathrm{Alt}(6)) = \frac{5750005437452539}{2305683264972780} \sim 2.494,$$

$$e_2(S) \leq e_2(\mathrm{Alt}(6)) = \frac{177158645957507439500873372884 33}{26580876591877694140270704642 00} \sim 6.665.$$

Theorem (AL 2015)

Let S be a finite nonabelian simple group. Then

$$e(S) \leq e(\mathrm{Alt}(6)) = \frac{575000543745253 9}{230568326497278 0} \sim 2.494,$$

$$e_2(S) \leq e_2(\mathrm{Alt}(6)) = \frac{177158645957507439500873372884 33}{265808765918776941402707046420 0} \sim 6.665.$$

Theorem (AL 2015)

If $n \geq 5$, then

$$e(\mathrm{Sym}(n)) \leq e(\mathrm{Sym}(6)) \sim 2.8816,$$
$$e_2(\mathrm{Sym}(n)) \leq e_2(\mathrm{Sym}(6)) \sim 9.5831.$$

Moreover $\lim_{n\to\infty} e(\mathrm{Sym}(n)) = 2.5$ *and* $\lim_{n\to\infty} e_2(\mathrm{Sym}(n)) = 7.5$.

Let $K < G$. We may generalize the definition τ_G, considering the random variable $\tau_{G,K}$ 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. Let $e(G,K)$ be the expectation of $\tau_{G,K}$.

Theorem (AL 2016)

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

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

Corollary

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

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

Recalling the talk of Ramón Esteban-Romero

$$\mathcal{M}(G) = \max_{n \geq 2} \log_n m_n(G), \quad \mathcal{V}(G) = \min \left\{ k \in \mathbb{N} \mid P_G(k) \geq \frac{1}{e} \right\}.$$

Elementary arguments in probability theory imply

$$\frac{1}{e} \cdot e(G) \leq \mathcal{V}(G) \leq \frac{e}{e-1} \cdot e(G).$$

Recalling the talk of Ramón Esteban-Romero

$$\mathcal{M}(G) = \max_{n \geq 2} \log_n m_n(G), \quad \mathcal{V}(G) = \min \left\{ k \in \mathbb{N} \mid P_G(k) \geq \frac{1}{e} \right\}.$$

Elementary arguments in probability theory imply

$$\frac{1}{e} \cdot e(G) \leq \mathcal{V}(G) \leq \frac{e}{e-1} \cdot e(G).$$

Theorem (Lubotzky 2002)

$$\mathcal{M}(G) - 3.5 \leq \mathcal{V}(G) \leq \mathcal{M}(G) + 2.02.$$

Thus we may use the results described in the talk by Ramón Esteban-Romero to bound $e(G)$.

$$\mathcal{M}(G) = \max_{n\geq 2} \log_n m_n(G), \quad \mathcal{V}(G) = \min\left\{k \in \mathbb{N} \mid P_G(k) \geq \frac{1}{e}\right\}.$$

Elementary arguments in probability theory imply

$$\frac{1}{e} \cdot e(G) \leq \mathcal{V}(G) \leq \frac{e}{e-1} \cdot e(G).$$

THEOREM (LUBOTZKY 2002)

$$\mathcal{M}(G) - 3.5 \leq \mathcal{V}(G) \leq \mathcal{M}(G) + 2.02.$$

Thus we may use the results described in the talk by Ramón Esteban-Romero to bound $e(G)$.

A better upper bound for $e(G)$ can be deduced combining the results described by Ramón Esteban-Romero with the following result:

Theorem (AL 2015)

$$e(G) \leq \mathcal{M}(G).$$

A better upper bound for $e(G)$ can be deduced combining the results described by Ramón Esteban-Romero with the following result:

THEOREM (AL 2015)

$$e(G) \leq \mathcal{M}(G).$$

Lubotzky proved that $\mathcal{M}(G) - 3.5 \leq \mathcal{V}(G)$. Does there exist a similar lower bound for $e(G)$? Can $e(G)$ be much smaller then $\mathcal{M}(G)$?

A DIFFERENT RELATED QUESTION

Let $E(\tau_n)$ be the expected number of elements of $\mathrm{Sym}(n)$ which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of $\mathrm{Sym}(n)$ is found.

A DIFFERENT RELATED QUESTION

Let $E(\tau_n)$ be the expected number of elements of $\mathrm{Sym}(n)$ which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of $\mathrm{Sym}(n)$ is found.

Given $\omega = (n_1, \dots, n_k) \in \Pi_n$, the set of partitions of n, with $n_1 = \cdots = n_{k_1} > n_{k_1+1} = \cdots = n_{k_1+k_2} > \cdots > n_{k_1+\cdots+k_{r-1}+1} = \cdots = n_{k_1+\cdots+k_r}$ define $\mu(\omega) = (-1)^{k-1}(k-1)!$, $\iota(\omega) = \frac{n!}{n_1!n_2!\dots n_k!}$, $\nu(\omega) = k_1!k_2!\dots k_r!$

THEOREM (AL 2015)

For each $n \geq 2$, 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.

A DIFFERENT RELATED QUESTION

Let $E(\tau_n)$ be the expected number of elements of Sym(n) which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of Sym(n) is found.

Given $\omega = (n_1, \dots, n_k) \in \Pi_n$, the set of partitions of n, with $n_1 = \dots = n_{k_1} > n_{k_1+1} = \dots = n_{k_1+k_2} > \dots > n_{k_1+\dots+k_{r-1}+1} = \dots = n_{k_1+\dots+k_r}$ define $\mu(\omega) = (-1)^{k-1}(k-1)!$, $\iota(\omega) = \frac{n!}{n_1!n_2!\dots n_k!}$, $\nu(\omega) = k_1!k_2!\dots k_r!$

THEOREM (AL 2015)

For each $n \geq 2$, 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.

$$\lim_{n\to\infty} E(\tau_n) = 2 \text{ and } 2 \leq E(\tau_n) \leq E(\tau_4) = \frac{7982}{3795} \sim 2.1033 \text{ for } n \geq 2.$$

Let $n \in \mathbb{N}$. There are two boxes: the balls in the blue box correspond to the elements of Sym(n), the balls in the red box correspond to the elements of Alt(n). We choose one of the boxes, and then we extract balls from the chosen box, with replacement, until a transitive permutation group of degree n is generated. Is it better to choose the red box or the blue one?

Let $n \in \mathbb{N}$. There are two boxes: the balls in the blue box correspond to the elements of $\mathrm{Sym}(n)$, the balls in the red box correspond to the elements of $\mathrm{Alt}(n)$. We choose one of the boxes, and then we extract balls from the chosen box, with replacement, until a transitive permutation group of degree n is generated. Is it better to choose the red box or the blue one? It depends on the parity of n.

Let $n \in \mathbb{N}$. There are two boxes: the balls in the blue box correspond to the elements of $\mathrm{Sym}(n)$, the balls in the red box correspond to the elements of $\mathrm{Alt}(n)$. We choose one of the boxes, and then we extract balls from the chosen box, with replacement, until a transitive permutation group of degree n is generated. Is it better to choose the red box or the blue one? It depends on the parity of n.

Let $\mathrm{E}(\tau_n)$ the expected number of elements of $\mathrm{Sym}(n)$ needed to generate a transitive subgroup and let $\mathrm{E}(\tilde{\tau}_n)$ the expected number of elements of $\mathrm{Alt}(n)$ needed to generate a transitive subgroup.

If $n \geq 3$, then

$$\mathrm{E}(\tau_n) - \mathrm{E}(\tilde{\tau}_n) = \frac{(-1)^{n-1} n!(n-1)!}{(n!-1)(n!-2)}.$$

A probabilistic version of an old theorem

Theorem (R. Guralnick, AL 1989)

If all 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 an old theorem

Theorem (R. Guralnick, AL 1989)

If all 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.

Theorem (M. Moscatiello, AL 2017)

If all the Sylow subgroups of a finite group 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 best possible in this context. Approximately, κ equals 2.752394.

Some steps of the proof

Proposition

Let G be a finite non-soluble group. If all the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d + 2.7501$.

Proof.

We use the inequality

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

where $m_n(G)$ is the number of maximal subgroups of G of index n and the following result, proved by Pyber using the CFSG: for every finite group G and every $n \geq 2$, G has at most n^2 core-free maximal subgroups of index n. □

Some steps of the proof

Definition

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

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

Some steps of the proof

$$e(H_{\pi,d}) = d+1+\sum_{t\geq 0}\left(1-\prod_{1\leq i\leq d}\left(1-\frac{2^{i-1}}{2^{t+d+1}}\right)\prod_{\substack{p\in\pi\\ p\neq 2}}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^{t+d+1}}\right)\right)$$

Set $e_d = \sup_\pi e(H_{\pi,d})$, $\kappa = \sup_d(e_d - d)$, $c = \prod_{2\leq n\leq\infty}\zeta(n)^{-1}$.

$$\kappa = 2+\left(1-\frac{4c}{3}\right)+\sum_{j\geq 2}\left(1-\left(1+\frac{1}{2^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right)\sim 2.75239495.$$

Theorem (M. Moscatiello, AL 2017)

Let G be a finite group of odd order. If all the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d + \tilde{\kappa}$ with $\tilde{\kappa} \sim 2.1487$.

This bound is probably not best possible. A precise estimation 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, so if $G \leq \mathrm{Sym}(n)$, then $e(G) \leq \lfloor n/2 \rfloor + \kappa$.

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements, so if $G \leq \mathrm{Sym}(n)$, then $e(G) \leq \lfloor n/2 \rfloor + \kappa$.

However this bound is not best possible and a better result can be obtained:

THEOREM (M. MOSCATIELLO, AL 2017)

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 $\kappa^* \sim 1.606695$.

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements, so if $G \leq \mathrm{Sym}(n)$, then $e(G) \leq \lfloor n/2 \rfloor + \kappa$.

However this bound is not best possible and a better result can be obtained:

THEOREM (M. MOSCATIELLO, AL 2017)

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 best possible. Let $m = \lfloor n/2 \rfloor$ and set

$$G_n = \begin{cases} \mathrm{Sym}(2)^m & \text{if } m \text{ is even,} \\ \mathrm{Sym}(2)^{m-1} \times \mathrm{Sym}(3) & \text{if } m \text{ is odd.} \end{cases}$$

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

An open question

If G is a finite p-group, then $e(G) \leq d(G) + \frac{p}{p-1} \leq d(G) + 2$.

An open question

If G is a finite p-group, then $e(G) \leq d(G) + \frac{p}{p-1} \leq d(G) + 2$.

So we could conjecture that our previous results can be generalized as follows: there exists a constant ρ such that, if a finite group G has the property that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $e(G_p) \leq d$, then $e(G) \leq d + \rho$.

An open question

If G is a finite p-group, then $e(G) \leq d(G) + \frac{p}{p-1} \leq d(G) + 2$.

So we could conjecture that our previous results can be generalized as follows: there exists a constant ρ such that, if a finite group G has the property that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $e(G_p) \leq d$, then $e(G) \leq d + \rho$.

This would be a probabilistic version of the following result:

Theorem (AL 2000)

If a finite group G has a family of d-generator subgroups whose indices have no common divisor, then G can be generated by $d + 2$ elements.

A partial result in this direction

$$\mathcal{V}(G) = \min \left\{ k \in \mathbb{N} \mid P_G(k) \geq \frac{1}{e} \right\}.$$

Theorem (Moscatiello, AL 2018)

Let G be a finite soluble group. Assume that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $\mathcal{V}(G_p) \leq d$. Then $\mathcal{V}(G) \leq d + 7$.

Another related open question

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

Another related open question

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

A profinite group G is PFG if and only if $e(G) < \infty$.

Another related open question

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

A profinite group G is PFG if and only if $e(G) < \infty$.

Theorem

Let G be a finitely generated profinite group. If a 2-Sylow subgroup of G is finitely generated, then G is PFG.

Another related open question

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

A profinite group G is PFG if and only if $e(G) < \infty$.

Theorem

Let G be a finitely generated profinite group. If a 2-Sylow subgroup of G is finitely generated, then G is PFG.

Question

Let G be a finitely generated profinite group. Is it true that if G contains a PFG closed subgroup of odd index, then G is PFG?