[Random thoughts] On the distribution of element orders in finite groups

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics
Budapest, Hungary

Ischia Group Theory 2022
June 23

Inspiration

Marcel Herzog, Patrizia Longobardi, Mercede Maj,
An exact upper bound for sums of element orders in non-cyclic finite groups,
Journal of Pure and Applied Algebra 222 (2018), 1628–1642.

and Marcel's talks at Ischia Group Theory:
Two criteria for solvability of finite groups (March 20, 2018)
New criteria for solvability, nilpotency and other properties of finite groups (March 26, 2021)

$$\boxed{\psi(G) = \sum_{g \in G} ord(g)}$$

Maximum for cyclic groups

H. Amiri, S. M. Jafarian Amiri, I. M. Isaacs,
Sums of element orders in finite groups,
Communications in Algebra 37 (2009), 2978–2980.

$\boxed{\psi(G) < \psi(C_n) \text{ for every non-cyclic group } G \text{ of order } n.}$

Asked by F. Schmidt in 1990 in The American Mathematical Monthly, and answered by
John H. Lindsey II, published in the 1991 December issue of the Monthly.

If $n = \prod_{i=1}^{r} p_i^{e_i}$, then

$$\psi(n) = \psi(C_n) = \prod_{i=1}^{r} \frac{p_i^{2e_i+1} + 1}{p_i + 1} = n^2 \prod_{i=1}^{r} \frac{p_i}{p_i + 1} \left(1 + \frac{1}{p_i^{2e_i+1}}\right)$$

Temptation

A well-known theorem of Frobenius states that the number of solutions of the equation $x^d = 1$ for any $d \mid |G|$ is divisible by d, hence it is at least d. Several people thought that this would yield a proof of the

> Conjecture: If G is a group of order n, then there exists a bijection $f : G \to C_n$ such that for all $g \in G$ the order of g divides the order of $f(g)$.

(see Problem 18.1 in The Kourovka Notebook). However, to achieve this one has to show (by Hall's marriage theorem) that for any set $\{d_1, \ldots, d_k\}$ of divisors of n, the number of elements in G satisfying at least one of the equations $x^{d_1} = 1$, . . . , $x^{d_k} = 1$ is at least as large as it is in the cyclic group of order n.

Average order

$\frac{\psi(G)}{|G|}$ is the average order. Let $|G| = n$, then

$$2 - \frac{1}{n} \leq \frac{\psi(G)}{n} \leq n - 1 + \frac{1}{n}$$

Mihai-Silviu Lazorec and Marius Tărnăuceanu,
A density result on the sum of element orders of a finite group,
Archiv der Mathematik 114 (2020), 601–607.

$$\frac{\psi(G)}{|G|^2} \text{ is dense in } [0,1].$$

The proof is easy, it is enough to consider cyclic groups of square-free order.
Then it is an exercise in calculus, using that $\sum \frac{1}{p}$ is divergent.

Comparison with $\psi(n)/n$ or $\phi(n)$

The meaningful comparison has to be made with $\psi(n) = \psi(C_n)$. If $n = \prod_{i=1}^{r} p_i^{e_i}$, then

$$\psi(n) = \psi(C_n) = \prod_{i=1}^{r} \frac{p_i^{2e_i+1}+1}{p_i+1} = n^2 \prod_{i=1}^{r} \frac{p_i}{p_i+1}\left(1+\frac{1}{p_i^{2e_i+1}}\right).$$

Euler's ϕ function

$$\phi(n) = n\prod_{i=1}^{r} \frac{p_i-1}{p_i}.$$

Obviously, $\psi(C_n) > \phi(n)n$ (assuming $n > 1$). Furthermore,

$$1 < \frac{\psi(C_n)}{n\phi(n)} < \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.943\ldots$$

Herzog–Longobardi–Maj:

If G is not cyclic, then $\psi(G) \leq \frac{7}{11}\psi(|G|)$. So $\boxed{\frac{\psi(G)}{\psi(n)} \notin (\frac{7}{11}, 1)}$.

Groups with large average order

Herzog–Longobardi–Maj:
If $\dfrac{\psi(G)}{\psi(|G|)} > \dfrac{7}{11} = \dfrac{\psi(C_2 \times C_2)}{\psi(4)}$, then G is cyclic.

Groups with large average order

Herzog–Longobardi–Maj:
If $\frac{\psi(G)}{\psi(|G|)} > \frac{7}{11} = \frac{\psi(C_2 \times C_2)}{\psi(4)}$, then G is cyclic.

Morteza Baniasad Azad and Behrooz Khosravi,
A criterion for solvability of a finite group by the sum of element orders,
Journal of Algebra 516 (2018), 115–124.

If $\frac{\psi(G)}{\psi(|G|)} > \frac{211}{1617} = \frac{\psi(A_5)}{\psi(60)}$, then G is solvable.

Nearly cyclic groups

Fix k, and consider the class of groups $\mathcal{G}_k$ that contain a cyclic subgroup of index $\leq k$.
I.e., the maximum element order is at least n/k, where $n = |G|$.

Andrea Lucchini,
On the order of transitive permutation groups with cyclic point-stabilizer,
Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Serie IX. Rendiconti Lincei. Matematica e Applicazioni 9 (1998), 241–243.
If $G \in \mathcal{G}_k$, then G contains a cyclic normal subgroup of index $\leq k(k-1)$.

If $G \in \mathcal{G}_k$, then $|G''|$ is bounded by a function of k.

Average order in nearly cyclic groups

If $G \in \mathcal{G}_k$, then

$$\psi(G) \geq \frac{1}{k^2}\psi(|G|).$$

Average order in nearly cyclic groups

If $G \in \mathcal{G}_k$, then

$$\psi(G) \geq \frac{1}{k^2}\psi(|G|).$$

For every $\epsilon > 0$, there exist groups $G \in \mathcal{G}_k$ such that

$$\psi(G) \leq \frac{1+\epsilon}{\psi(k)}\psi(|G|).$$

Note that $\psi(k) > k\phi(k) > k^2/(e^\gamma \log\log k + \epsilon)$.

Multiplicative versus additive

$ord(g)$ has more multiplicative features than additive ones, e.g.,

- $ord(g)$ divides $|G|$,
- if $a, b \in G$ commute and have coprime orders, then

$ord(ab) = ord(a)ord(b)$.

Multiplicative versus additive

$ord(g)$ has more multiplicative features than additive ones, e.g.,
- $ord(g)$ divides $|G|$,
- if $a, b \in G$ commute and have coprime orders, then $ord(ab) = ord(a)ord(b)$.

Therefore, the random variable we have to study is

$$\boxed{\log ord(g)}$$

and instead of the the arithmetic mean we should take the geometric mean

$$\boxed{\left(\prod_{g\in G} ord(g)\right)^{1/|G|}}$$

or its logarithm $\frac{1}{|G|}\sum_{g\in G} \log ord(g)$.

Symmetric groups

Paul Erdős and Pál Turán,
On some problems of a statistical group-theory, III,
Acta Math. Academiae Scientiarum Hungaricae 18 (1967), 309–320.

For the symmetric groups the distribution of $\log ord(g)$ is asymptotically Gaussian, namely,

$$\boxed{\begin{gathered}\lim_{n\to\infty}\operatorname*{Prob}_{g\in S_n}\left(\log ord(g) < \tfrac{1}{2}\log^2 n + x\left(\tfrac{1}{3}\log^3 n\right)^{1/2}\right)\\ = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt.\end{gathered}}$$

Edmund Landau,
Über die Maximalordnung der Permutationen gegebenen Grades,
Archiv der Mathematik und Physik, 3. Reihe 5 (1903), 92–103.

$$\boxed{\lim_{n\to\infty}\frac{\max(\log ord(g) : g\in S_n)}{\sqrt{n\log n}} = 1.}$$

Symmetric p-groups

Let P_k denote the Sylow p-subgroup of the symmetric group of degree p^k.

$\log_p ord(g)$ $(g \in P_k)$ has values $0, 1, \ldots, k$.

Miklós Abért and Bálint Virág,
Dimension and randomness in groups acting on rooted trees,
Journal of the American Mathematical Society 18 (2005), 157–192.

The expected value of $\log_p ord(g)$ $(g \in P_k)$ is asymptotically ck, where $0 < c = c(p) < 1$ satisfies the equation

$$\frac{c \log c + (1-c)\log(1-c)}{c} = \log\left(1 - \frac{1}{p}\right).$$

Péter P. Pálfy and Mihály Szalay,
On a problem of P. Turán concerning Sylow subgroups,
Studies in Pure Mathematics, Birkhäuser, 1983, 531–542.

The variance of the distribution of $\log_p ord(g)$ $(g \in P_k)$ is bounded by

$$\frac{1}{4} + 48\frac{\log p}{p}.$$

Groups with large geometric mean of element orders

Morteza Baniasad Azad and Behrooz Khosravi,
Properties of finite groups determined by the product of their element orders,
Bulletin of the Australian Mathematical Society 103 (2021), 88–95.

If $\frac{1}{|G|}\sum_{g\in G}\log ord(g)$ is larger than this average for

- $C_2 \times C_2$, then G is cyclic,
- Q_8, then G is abelian,
- S_3, then G is nilpotent,
- A_4, then G is supersolvable,
- A_5, then G is solvable.

Largest product of element orders

Martino Garonzi and Massimiliano Patassini,
Inequalities detecting structural properties of a finite group,
Communications in Algebra 45 (2017), 677–687.

If G is a non-cyclic group of order n, then

$$\boxed{\prod_{g \in G} ord(g) < \prod_{g \in C_n} ord(g).}$$

Notation and preliminaries

$|G| = n = \prod_{i=1}^{r} p_i^{e_i}$

$E(k) =$ the number of elements of order k in G

$D(k) =$ the number of solutions of $x^k = 1$ in G, $= \sum_{m|k} E(m)$

Frobenius: $k \mid D(k)$, thus $D(k) \geq k$ (for $k \mid n$)

Möbius: $E(k) = \sum_{m|k} D(m)\mu(\frac{k}{m})$

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{otherwise} \end{cases}$$

$$\sum_{d|n} \mu(d) \log d = \begin{cases} -\log p, & \text{if } n = p^e > 1 \\ 0, & \text{otherwise} \end{cases}$$

Proof après Garonzi–Patassini

$$\log \prod_{g \in G} ord(g) = \sum_{k|n} E(k) \log k$$

$$= \sum_{k|n} \sum_{m|k} D(m)\, \mu\left(\frac{k}{m}\right) \left(\log \frac{k}{m} + \log m\right)$$

$$= \sum_{m|n} D(m) \log m \cdot \sum_{d|\frac{n}{m}} \mu(d) + \sum_{m|n} D(m) \sum_{d|\frac{n}{m}} \mu(d) \log d$$

$$= D(n) \log n - \sum_{i=1}^{r} \left(D\left(\frac{n}{p_i}\right) + D\left(\frac{n}{p_i^2}\right) + \cdots + D\left(\frac{n}{p_i^{e_i}}\right) \right) \log p_i$$

$$\leq n \log n - \sum_{i=1}^{r} \left(\frac{n}{p_i} + \frac{n}{p_i^2} + \cdots + \frac{n}{p_i^{e_i}} \right) \log p_i$$

$$= \log \prod_{g \in C_n} ord(g)$$

The End

GRAZIE PER LA VOSTRA ATTENZIONE

The End

GRAZIE PER LA VOSTRA ATTENZIONE

E PER AVER ORGANIZZATO QUESTA MERAVIGLIOSA SERIE DI CONFERENZE