The Number of Cyclic Subgroups of a Finite Group

Martino Garonzi
with Massimiliano Patassini, Igor Lima

Ischia Group Theory 2018
March 23rd 2018

CONTEXT

Let $f : \mathbb{N} \to \mathbb{R}$ be a function and let G be a finite group. Consider

$$s_f(G) = \sum_{x \in G} f(o(x))$$

where $o(x)$ denotes the order of x.

The general problem we want to consider is how (and in what sense) $s_f(G)$ encodes properties of G (typically we compare different values of $s_f(G)$ when G varies in the family of groups of fixed order n).

Interesting functions that were considered are $f(t) = t$ (Amiri, Isaacs), $f(t) = 1/t$ (Salmasian) and $f(t) = t/\varphi(t)$ (De Medts, Tarnauceanu). Typically the question is the following: given a property P such that $s_f(G)$ is the same for all $G \in P$ of the same order, is the membership $G \in P$ detected by the fact that $s_f(G)$ equals this common value?

Interesting related open problem: given a number n and a finite group G of order n is there a bijection $h : G \to C_n$ with the property that $o(x)$ divides $o(f(x))$ for all $x \in G$?

Let G be a finite group. We are interested in studying the number of cyclic subgroups of G, let it be denoted by $c(G)$. We start by an easy but very powerful information ("main formula"):

$$c(G) = \sum_{x \in G} \frac{1}{\varphi(o(x))}.$$

This is because $\langle x \rangle$ contains $\varphi(o(x))$ elements generating $\langle x \rangle$.

$$c(S_3) = \frac{1}{\varphi(1)} + \frac{1}{\varphi(2)} + \frac{1}{\varphi(2)} + \frac{1}{\varphi(2)} + \frac{1}{\varphi(3)} + \frac{1}{\varphi(3)} = 5.$$

For any given m let $B(m)$ denote the size of the set $\{x \in G \ : \ x^m = 1\}$. Then

$$c(G) = \sum_{x \in G} \frac{1}{\varphi(o(x))} = \sum_{d|n} \left(\sum_{i|n/d} \frac{\mu(i)}{\varphi(id)} \right) B(d).$$

Here μ is the Möbius function, defined as follows: $\mu(1) = 1$, $\mu(m)$ is 0 if m is divisible by a square, otherwise $\mu(m) = (-1)^k$ where k is the number of primes dividing m.

Theorem (G, Patassini 2016)

If $|G| = n$ then $c(G) \geq c(C_n)$ with equality if and only if $G \cong C_n$.

Proof.

(Sketch). For any given m let $B(m)$ denote the size of the set $\{x \in G \ : \ x^m = 1\}$. Let μ be the Moebius function ($\mu(1) = 1$, $\mu(m)$ is 0 if m is divisible by a square, otherwise $\mu(m) = (-1)^k$ where k is the number of primes dividing m). Then

$$c(G) = \sum_{x \in G} \frac{1}{\varphi(o(x))} = \sum_{d|n} \left(\sum_{i|n/d} \frac{\mu(i)}{\varphi(id)} \right) B(d).$$

By a deep theorem of Frobenius if d divides $|G|$ then d divides $B(d)$, in particular $B(d) \geq d$. Incidentally d equals $B(d)$ when $G = C_n$ and d is any divisor of n. Since the coefficient of $B(d)$ is non-negative the inequality follows. □

In a recent work with Igor Lima we got interested in comparing the number of cyclic subgroups of G with the order of G. Let

$$\alpha(G) = c(G)/|G|.$$

This number is between 0 and 1. It is never 0, and it is 1 if and only if G is an elementary abelian 2-group.

We always have $\alpha(G) \leq \alpha(G/N)$. One main point of study is to ask when we have equality. If equality holds then N is an elementary abelian 2-group.

For example (direct product case) $\alpha(H \times C_2^n) = \alpha(H)$. However $\alpha(A_4) = \alpha(C_3) = 2/3$ and C_3 is a quotient of A_4 so equality does not only occur for direct products.

Theorem (G, Lima - Extension argument)

If $\alpha(G) = \alpha(G/N)$ and G/N is a symmetric group then $G \cong N \times G/N$.

Interesting problem: for what other groups (other than symmetric) does this hold?

Given a group G, we denote by $cp(G)$ the "commuting probability" in G, that is the probability that a pair $(x, y) \in G \times G$ verifies $xy = yx$. It turns out that

$$cp(G) = k(G)/|G|$$

where $k(G)$ is the number of conjugacy classes of G.

Using the Frobenius-Schur indicator and the Cauchy-Schwarz inequality it is possible to show that setting

$$I(G) = |\{x \in G \ : \ x^2 = 1\}|$$

we have the well-known inequality

$$I(G)^2 \leq k(G)|G|.$$

Using the above ingredients it is easy to show that

$$2\alpha(G) - 1 \leq I(G)/|G| \leq \sqrt{k(G)/|G|} = \sqrt{cp(G)}.$$

THEOREM (G, LIMA)

If $\alpha(G) > \alpha(S_5)$ then G is solvable.

PROOF.

Suppose $\alpha(G) \geq \alpha(S_5)$. Let $\mathrm{sol}(G)$ the solvable radical of G (the largest normal solvable subgroup).

The idea is to show that $G/\mathrm{sol}(G) \cong S_5$ because then $\alpha(S_5) \leq \alpha(G) \leq \alpha(G/\mathrm{sol}(G)) = \alpha(S_5)$ hence by the extension argument $G \cong C_2^n \times S_5$.

Let $cp(G)$ be the probability that two random elements of G commute, as it turns out $cp(G) = k(G)/|G|$ where $k(G)$ is the number of conjugacy classes of G.

If $\alpha(G) \geq 1/2$ then using a result by G. R. Robinson and R. Guralnick, $|G : \mathrm{sol}(G)|^{-1/2} \geq cp(G) \geq (2\alpha(G) - 1)^2$.

We deduce $|G/\mathrm{sol}(G)| \leq 5397$, also $\alpha(S_5) \leq \alpha(G) \leq \alpha(G/\mathrm{sol}(G))$. We may assume $\mathrm{sol}(G) = \{1\}$ and we solve the problem. □

Theorem (G, Lima)

If $\alpha(G) > \alpha(S_4)$ then G is supersolvable.

Proof.

Suppose $\alpha(G) \geq \alpha(S_4)$ and G not supersolvable. We prove that $G \cong S_4 \times C_2^n$. Here the main idea is to use the solution to the $k(GV)$ problem ("if V is a faithful $\mathbb{F}_p G$-module of order prime to $|G|$ then $k(GV) \leq |V|$") in the case of Fitting height 2. Let F be the Fitting subgroup of G. If G/F is nilpotent then $k(G) \leq |F|$ so

$$(2\alpha(G) - 1)^2 \leq cp(G) = \frac{k(G)}{|G|} \leq \frac{1}{|G : F|}.$$

The idea is to use this, the inequality involving $\alpha(G)$ and $cp(G)$, and the Fitting length to deduce that G/F is one of C_2, C_4, $C_2 \times C_2$ and S_3. Since G is not supersolvable there is a maximal subgroup M whose index is not a prime, let $X := G/M_G$. This is a solvable primitive group. We next show that $X \cong S_4$ and conclude by the extension argument. □