INEQUALITIES DETECTING CICLICITY AND NILPOTENCY OF FINITE GROUPS

Martino Garonzi
Joint work with Massimiliano Patassini

Brasilia
March 13th 2015

Let us start by clarifying what it means for a group invariant to "detect" a property. Let P be a property a group can have, i.e. a family of groups (we say that G has property P if $G \in P$). Let $\mathcal{F}$ be a family of finite groups containing P and let $f : \mathcal{F} \to X$ be some "invariant" function, i.e. such that $f(A) = f(B)$ if $A \cong B$. We say that f "detects property P in $\mathcal{F}$" (or just "detects property P" if $\mathcal{F}$ is the family of all finite groups) if and only if

$$f^{-1}(f(P)) = P.$$

For example,

- $f(G) := |G|$ detects the fact of being a p-group.
- $f(G) :=$ "the number of composition factors of G" detects the fact of being a simple group.
- $f(G) :=$ "the number of non-abelian composition factors of G" detects solvability.
- $f(G) := G'$ detects solvability.
- $f(G) := |Z(G)|$ detects abelianity for $\mathcal{F}$ the set of groups of a given order n.
- $f(G) :=$ "the set of Sylow subgroups of G" detects nilpotency.

We begin by the following question: for a finite group G of order n consider the monic polynomial of degree n

$$\mathrm{Pol}_G := \prod_{a \in G} (X - o(a)).$$

Clearly this equals $\prod_{m|n}(X - m)^{\ell_m}$ where ℓ_m is the number of elements of G of order m. Therefore knowing this polynomial is equivalent to knowing how many elements there are with any given order. It is known that $G \mapsto \mathrm{Pol}_G$ detects nilpotency.

QUESTION (THOMPSON)

Is it true that Pol_G detects solvability?

In other words, is it true that if A, B are two finite groups with A solvable and $Pol_A = Pol_B$ then B is solvable?

This is an open problem.

Another interesting worth mentioning conjecture (true in the solvable case) is the following.

CONJECTURE

Let G be a finite group of order n and let C_n denote the cyclic group of order n. There exists a bijection $f : G \to C_n$ such that $o(x)$ divides $o(f(x))$ for all $x \in G$.

Note that the existence of a bijection as in the conjecture is equivalent to the existence of a family $\{S_d \ : \ d|n\}$ of subsets of G with the following properties (here φ denotes Euler's totient function):

- The sets S_d are pairwise disjoint and $G = \bigcup_{d|n} S_d$.
- $x^d = 1$ for all $x \in S_d$, for all $d|n$.
- $|S_d| = \varphi(d)$ for all $d|n$.

Of course the existence of such a bijection would easily imply, for instance, that for G a group of order n the sum $\sum_{x \in G} o(x)^s$ is maximal for C_n if $s > 0$ and minimal for C_n if $s < 0$.

Let $S_G := \sum_{x \in G} o(x)$. The following result implies that $G \mapsto S_G$ detects ciclicity among groups of the same order.

Theorem (H. Amiri, S.M.J. Amiri, M. Isaacs)

If G is a noncyclic group of order n then $S_G < S_{C_n}$.

The idea is the following. Suppose by contradiction that $S_G \geq S_{C_n}$. Clearly

$$S_{C_n} \geq 1 + n\varphi(n) > n\varphi(n).$$

It follows that $S_G > n\varphi(n)$ hence $\frac{S_G}{|G|} > \varphi(n)$. This implies that there is $x \in G$ with $o(x) > \varphi(n)$ and this is at least n/p where p is the largest prime divisor of n. Therefore

$$|G : \langle x \rangle| = n/o(x) < n/(n/p) = p$$

hence p does not divide $|G : \langle x \rangle|$, implying that $\langle x \rangle$ contains a Sylow p-subgroup P of G which is normal in G (because $x \in N_G(P)$ and by Sylow theorem $p > |G : \langle x \rangle| \geq |G : N_G(P)| \equiv 1 \mod p$).

At this point one can apply induction on P and G/P.

To discuss other sums we introduce some notation.
For G a finite group of order n and m a divisor of n set

$$\ell_m := |\{x \in G \ : \ o(x) = m\}|,$$

$$B(m) := |\{x \in G \ : \ x^m = 1\}|.$$

Clearly $B(m) = \sum_{d|m} \ell_d$. By Moebius inversion formula we obtain $\ell_m = \sum_{d|m} \mu(m/d)B(d)$ where μ is the Moebius function, defined as follows: $\mu(k)$ equals zero if k is divisible by a square different from 1 and $\mu(k) = (-1)^t$ if k is a product of t pairwise distinct prime numbers.

Theorem (Frobenius)

Let m be a divisor of n. Then m divides $B(m)$.

In particular $B(m) \geq m$ for all $m|n$.

Let $I_G := \sum_{x\in G}\frac{1}{o(x)}$. The following result implies that $G \mapsto I_G$ detects ciclicity among groups of the same order.

THEOREM (G, PATASSINI)

If G is a non-cyclic group of order n then $I_G > I_{C_n}$.

Here the idea is very different.

$$\sum_{x\in G}\frac{1}{o(x)} = \sum_{m|n}\frac{\ell_m}{m} = \sum_{m|n}\sum_{d|m}\frac{B(d)\mu(m/d)}{m}$$

$$= \sum_{d|n}\sum_{i|n/d}\frac{B(d)\mu(i)}{id} = \sum_{d|n}\left(\sum_{i|n/d}\frac{\mu(i)}{i}\right)\frac{B(d)}{d}.$$

So we have to understand the sum $\sum_{i|j} \frac{\mu(i)}{i}$. Write $j = p_1^{c_1} \cdots p_t^{c_t}$. Then i takes the form $p_1^{\beta_1} \cdots p_t^{\beta_t}$ where we may assume $\beta_v \in \{0,1\}$ for all v because otherwise $\mu(i) = 0$. Hence

$$\sum_{i|j} \frac{\mu(i)}{i} = \sum_{\beta_v \in \{0,1\}} \frac{(-1)^{\beta_1} \cdots (-1)^{\beta_t}}{p_1^{\beta_1} \cdots p_t^{\beta_t}}$$

$$= \sum_{\beta_v \in \{0,1\}} \left(-\frac{1}{p_1}\right)^{\beta_1} \cdots \left(-\frac{1}{p_t}\right)^{\beta_t} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right).$$

In particular this is a positive number. It follows by Frobenius Theorem that

$$I_G = \sum_{d|n} \left(\sum_{i|n/d} \frac{\mu(i)}{i} \right) \frac{B(d)}{d} \geq \sum_{d|n} \left(\sum_{i|n/d} \frac{\mu(i)}{i} \right) = I_{C_n}.$$

Equality only occurs if $B(d) = d$ for all $d|n$, i.e. $\ell_d = \varphi(d)$ for all $d|n$, i.e. G is cyclic.

Let $P_G := \prod_{x \in G} o(x)$. The following result implies that $G \mapsto P_G$ detects ciclicity among groups of the same order.

THEOREM

If G is a non-cyclic group of order n then $P_G < P_{C_n}$.

The idea is similar to the previous one. We have

$$\log P_G = \sum_{m|n} \ell_m \log m = \sum_{d|m|n} \mu(m/d) B(d) \log m$$
$$= \sum_{d|n} \left(\sum_{i|n/d} \mu(i) \log(id) \right) B(d).$$

Computing the sum similarly as before we find the following formula for P_G:

$$P_G = \frac{n^n}{p_1^{B_1} \cdots p_t^{B_t}}$$

where $n = p_1^{c_1} \cdots p_t^{c_t}$ and $B_i = \sum_{j=1}^{c_i} B(n/p_i^j)$. Again, the fact that $P_G \leq P_{C_n}$ follows by Frobenius Theorem and equality occurs if and only if G is cyclic.

Now we ask a question that will turn out to be related to the previous computations: can we estimate the **number of cyclic subgroups** of G? The cyclic group C_n has exactly $d(n)$ cyclic subgroups, where $d(n)$ denotes the number of divisors of n. The following result implies that $G \mapsto$ "the number of cyclic subgroups of G" detects ciclicity among groups of the same order.

THEOREM (G, PATASSINI)

Let G be a non-cyclic group of order n. Then G has strictly more than $d(n)$ cyclic subgroups.

Let $\langle x_1 \rangle, \dots, \langle x_k \rangle$ be the distinct cyclic subgroups of G. Then $\langle x_i \rangle$ contains $\varphi(o(x_i))$ elements of order $o(x_i)$. For $x, y \in G$ write $x \sim y$ if x, y generate the same cyclic subgroup of G. Then $\sim$ is an equivalence relation in G hence

$$\sum_{x \in G} \frac{1}{\varphi(o(x))} = \sum_{i=1}^{k} \sum_{x \sim x_i} \frac{1}{\varphi(o(x))} = \sum_{i=1}^{k} \frac{\varphi(o(x_i))}{\varphi(o(x_i))} = k.$$

So the question becomes the following: can we estimate the sum $\sum_{x \in G} \frac{1}{\varphi(o(x))}$?

Proceeding as before we find

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

Working out the coefficient and using the fact that φ is a multiplicative function we obtain that the coefficient of $B(d)$ equals

$$\frac{1}{\varphi(d)} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right) \left(1 - \frac{1}{p_{\ell+1} - 1}\right) \cdots \left(1 - \frac{1}{p_t - 1}\right)$$

where $p_1, \dots, p_\ell$ are the primes that divide both d and n/d, and $p_{\ell+1}, \dots, p_t$ are the primes that divide n/d and not d. This is a non-negative number hence

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

Again, equality only occurs if G is cyclic.

Using this, it is obvious that the following also holds.

Proposition

Let G be a finite non-cyclic group of order n and let $\mathcal{P}$ be any of the following properties: cyclic, nilpotent, solvable, any group. Then G has strictly more than $d(n)$ subgroups with property $\mathcal{P}$.

Indeed, for any of those $\mathcal{P}$, cyclic groups have property $\mathcal{P}$.

This implies that the number of cyclic subgroups, the number of solvable subgroups, the number of nilpotent subgroups, and the number of subgroups, all detect ciclicity among the groups of the same order.

Given a nonzero real number r, and a finite group G of order n, just for fun let us look at the sum

$$SC_r(G) := \sum_{x \in G} \left(\frac{o(x)}{\varphi(o(x))} \right)^r .$$

$SC_1(G)$ equals the sum of the cyclic subgroup sizes.

PROPOSITION

If G is nilpotent then $SC_r(G) = SC_r(C_n)$.

PROOF.

Note that $SC_r(A \times B) = SC_r(A)SC_r(B)$ if A and B have coprime orders (this is because $m \mapsto \frac{m}{\varphi(m)}$ is multiplicative). Hence we may assume G is a p-group. But then clearly if x is not 1 then $\frac{o(x)}{\varphi(o(x))}$ equals $\frac{p}{p-1}$. Hence $SC_r(G)$ does not depend on G thus it equals $SC_r(C_n)$. □

So there is no hope to detect ciclicity in this case. What about nilpotency?

If $r < 0$ then $G \mapsto SC_r(G)$ detects nilpotency among the groups of the same order:

THEOREM (G, PATASSINI)

Let G be a group of order n and let r be a negative real number.
If G is nilpotent then $SC_r(G) = SC_r(C_n)$.
If G is not nilpotent then $SC_r(G) > SC_r(C_n)$.

PROOF.

Working out the sum as before we find

$$SC_r(G) = \sum_{d|n,(d,n/d)=1} B(d) \prod_{p|n/d} \left(1 - \left(\frac{p}{p-1}\right)^r\right).$$

The coefficient of $B(d)$ is positive because $r < 0$. Hence by Frobenius Theorem $SC_r(G) \geq SC_r(C_n)$ and equality occurs if and only if $B(d) = d$ for all $d|n$ such that $(d, n/d) = 1$. This is equivalent to say that G is nilpotent (by Sylow Theorem applied to the case in which d is a prime power). $\square$

Some open questions.

1. (Thompson's question) Does $G \mapsto \mathrm{Pol}_G$ detect solvability?
2. (Pointwise argument) For a group G of order n is there a bijection $f : G \to C_n$ such that $o(x)$ divides $o(f(x))$ for all $x \in G$?
3. Note that $SC_1(G)$ is the sum of the cyclic subgroup sizes. Does $G \mapsto SC_1(G)$ detect nilpotency among groups of given order? (De Medts, Tarnauceanu).
4. If $r > 0$ does $SC_r(G)$ detect nilpotency among groups of given order?