# Desigualdades detectando ciclicidade e nilpotência de grupos finitos.

Martino Garonzi
Trabalho conjunto com Massimiliano Patassini

Brasília
13 de março 2015

Antes de começar vamos clarificar o que significa para um invariante de grupos “detectar” uma propriedade. Seja $P$ uma propriedade que um grupo pode ter, isto é, uma família de grupos (dizemos que $G$ tem a propriedade $P$ se $G \in P$). Seja $\mathcal{F}$ uma família de grupos finitos contendo $P$ e seja $f : \mathcal{F} \to X$ uma função “invariante”, isto é, tal que $f(A) = f(B)$ se $A \cong B$. Vamos dizer que $f$ “detecta a propriedade $P$ em $\mathcal{F}$” (ou apenas “detecta a propriedade $P$” se $\mathcal{F}$ é a família de todos os grupos finitos) se e somente se

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

Por exemplo,

- $f(G) := |G|$ detecta o fato de ser um $p$-grupo.
- $f(G) :=$ “o número de fatores de composição de $G$” detecta o fato de ser um grupo simples.
- $f(G) :=$ “o número de fatores de composição não abelianos de $G$” detecta a solvabilidade.

Vamos começar com a pergunta seguinte: dado um grupo finito $G$ de ordem $n$ consideramos o polinômio mônico de grau $n$

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

Este é obviamente igual a $\prod_{m|n}(X-m)^{\ell_m}$ onde $\ell_m$ é o numero de elementos de $G$ de ordem $m$. Portanto, conhecer este polinômio é equivalente a conhecer quantos elementos tem de qualquer ordem. É conhecido que $G \mapsto \mathrm{Pol}_G$ detecta a nilpotência.

**Pergunta (Thompson)**

*É verdade que $\mathrm{Pol}_G$ detecta a solvabilidade?*

*Em outras palavras, é verdade que se $A$, $B$ são dois grupos finitos com $A$ solúvel e $\mathrm{Pol}_A = \mathrm{Pol}_B$ então $B$ é solúvel também?*

Este é um problema aberto.

Uma outra interessante conjectura que vale a pena mencionar (verdadeira no caso solúvel) é a seguinte:

**CONJECTURA**

*Seja $G$ um grupo finito de ordem $n$ e seja $C_n$ o grupo cíclico de ordem $n$. Existe uma bijeção $f : G \to C_n$ tal que $o(x)$ divide $o(f(x))$ para cada $x \in G$.*

Observamos que a existência de uma bijeção como na conjectura é equivalente à existência de uma família $\{S_d \ : \ d|n\}$ de subconjuntos de $G$ com a seguinte propriedade (aqui $\varphi$ indica a função totiente de Euler):

- Os conjuntos $S_d$ são disjuntos dois a dois e $G = \bigcup_{d|n} S_d$.
- $x^d = 1$ para cada $x \in S_d$, para cada $d|n$.
- $|S_d| = \varphi(d)$ para cada $d|n$.

É claro que a existência de uma tal bijeção implicaria facilmente, por exemplo, que se $G$ é um grupo de ordem $n$ a soma $\sum_{x \in G} o(x)^s$ é máxima para $C_n$ se $s > 0$ e mínima para $C_n$ se $s < 0$.

Seja $S_G := \sum_{x \in G} o(x)$. O seguinte resultado implica que $G \mapsto S_G$ detecta a ciclicidade para grupos de ordem fixada.

**TEOREMA (H. AMIRI, S.M.J. AMIRI, M. ISAACS)**

*Se $G$ é um grupo não cíclico de ordem $n$ então $S_G < S_{C_n}$.*

A idéia é a seguinte. Supomos por contradição que $S_G \geq S_{C_n}$. É claro que

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

Devido a isso, $S_G > n\varphi(n)$ portanto $\frac{S_G}{|G|} > \varphi(n)$. Isso implica que existe $x \in G$ tal que $o(x) > \varphi(n)$ e esse é maior ou igual a $n/p$ onde $p$ é o maior divisor primo de $n$. Portanto,

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

e disso obtemos que $p$ não divide $|G : \langle x \rangle|$, o que implica que $\langle x \rangle$ contém um $p$-subgrupo de Sylow $P$ de $G$ que é normal em $G$ (porque $x \in N_G(P)$ e pelo teorema de Sylow $p > |G : \langle x \rangle| \geq |G : N_G(P)| \equiv 1 \mod p$).

Neste ponto pode-se aplicar indução sobre $P$ e $G/P$.

Para discutir outras somas introduzimos algumas notações.
Para $G$ um grupo finito de ordem $n$ e $m$ um divisor de $n$ sejam

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

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

Evidentemente $B(m) = \sum_{d|m} \ell_d$. Pela fórmula de inverção de Moebius obtemos $\ell_m = \sum_{d|m} \mu(m/d)B(d)$ onde $\mu$ é a função de Moebius, definida como se segue: $\mu(k)$ vale zero se $k$ é divisível por um quadrado diferente de 1 e $\mu(k) = (-1)^t$ se $k$ é um produto de $t$ números primos diferentes dois a dois.

**Teorema (Frobenius)**

*Seja $m$ um divisor de $n$. Então $m$ divide $B(m)$.*

Em particular $B(m) \geq m$ para cada $m|n$.

Seja $I_G := \sum_{x \in G} \frac{1}{o(x)}$. O seguinte resultado implica que $G \mapsto I_G$ detecta a ciclicidade para grupos de ordem fixada.

**Teorema (G, Patassini)**

*Se $G$ é um grupo não cíclico de ordem $n$ então $I_G > I_{C_n}$.*

Aqui a idéia é muito diferente.

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

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

Assim temos que comprender a soma $\sum_{i|j} \frac{\mu(i)}{i}$. Escrevemos $j = p_1^{c_1} \cdots p_t^{c_t}$. Então $i$ assume a forma $p_1^{\beta_1} \cdots p_t^{\beta_t}$ onde podemos assumir $\beta_v \in \{0,1\}$ para cada $v$ porque senão $\mu(i) = 0$. Portanto,

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

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

Em particular este é um número positivo. Segue do teorema de Frobenius que

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

Igualdade só ocorre se $B(d) = d$ para cada $d|n$, isto é, $\ell_d = \varphi(d)$ para cada $d|n$, isto é, $G$ é cíclico.

Seja $P_G := \prod_{x \in G} o(x)$. O seguinte resultado implica que $G \mapsto P_G$ detecta a ciclicidade para grupos de ordem fixada.

**Teorema**

*Se $G$ é um grupo não cíclico de ordem $n$, $P_G < P_{C_n}$.*

A idéia é semelhante à anterior. Temos

$$\log P_G = \sum_{m|n} \ell_m \log m = \sum_{d|m|n} \mu(m/d) B(d) \log m$$

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

Computando a soma como anteriormente encontramos a fórmula seguinte para $P_G$:

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

onde $n = p_1^{c_1} \cdots p_t^{c_t}$ e $B_i = \sum_{j=1}^{c_i} B(n/p_i^j)$. De novo, o fato que $P_G \leq P_{C_n}$ segue do teorema de Frobenius e igualdade ocorre se e somente se $G$ é cíclico.

Agora fazemos uma pergunta que vai se revelar relacionada aos cálculos anteriores: podemos estimar o **número de subgrupos cíclicos** de $G$? O grupo cíclico $C_n$ tem exactamente $d(n)$ subgrupos cíclicos, onde $d(n)$ indica o número dos divisores de $n$. O seguinte resultado implica que $G \mapsto$ "o número de subgrupos cíclicos de $G$" detecta a ciclicidade para grupos de ordem fixada.

**Teorema (G, Patassini)**

*Seja $G$ um grupo não cíclico de ordem $n$. Então $G$ tem mais que $d(n)$ subgrupos cíclicos.*

Sejam $\langle x_1 \rangle, \ldots, \langle x_k \rangle$ os diferentes subgrupos cíclicos de $G$. Então $\langle x_i \rangle$ contém $\varphi(o(x_i))$ elementos de ordem $o(x_i)$. Para $x, y \in G$ escrevemos $x \sim y$ se $x, y$ geram o mesmo subgrupo cíclico de $G$. Então $\sim$ é uma relação de equivalência em $G$, portanto

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

Assim a pergunta torna-se a seguinte: podemos estimar a soma $\sum_{x \in G} \frac{1}{\varphi(o(x))}$ ?

Prosseguindo como antes encontramos

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

Trabalhando com o coeficiente e usando o fato que $\varphi$ é uma função multiplicativa obtemos que o coeficiente de $B(d)$ é igual a

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

onde $p_1,\ldots,p_\ell$ são os primos que dividem tanto $d$ e $n/d$, e $p_{\ell+1},\ldots,p_t$ são os primos que dividem $n/d$ e não $d$. Este é um numero não negativo. Portanto,

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

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

De novo, igualdade ocorre se e somente se $G$ é cíclico.

Usando isso, é óbvio que vale o seguinte.

**Proposição**

*Seja $G$ um grupo finito não cíclico de ordem $n$, e seja $\mathcal{P}$ uma das propriedades seguintes: cíclico, nilpotente, solúvel, grupo qualquer. Então $G$ tem mais que $d(n)$ subgrupos com a propriedade $\mathcal{P}$.*

De fato, para cada tal $\mathcal{P}$, os grupos cíclicos tem a propriedade $\mathcal{P}$.

Isso implica que o número de subgrupos cíclicos, o número de subgrupos solúvel, o número de subgrupos nilpotentes, e o número de subgrupos detectam a ciclicidade para grupos de ordem fixada.

Dados um número real $r \neq 0$ e um grupo finito $G$ de ordem $n$, só de brincadeira vamos olhar para a soma

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

$SC_1(G)$ é igual à soma das ordens dos subgrupos cíclicos de $G$.

**PROPOSIÇÃO**

*Se $G$ é nilpotente, $SC_r(G) = SC_r(C_n)$.*

**DEMONSTRAÇÃO.**

Observamos que $SC_r(A \times B) = SC_r(A)SC_r(B)$ se $A$ e $B$ tem ordens coprimas (porque $m \mapsto \frac{m}{\varphi(m)}$ é multiplicativa). Portanto podemos supor que $G$ é um $p$-grupo. É claro que se $x$ é diferente de 1 então $\frac{o(x)}{\varphi(o(x))}$ é igual a $\frac{p}{p-1}$. Daqui $SC_r(G)$ não depende de $G$ assim é igual a $SC_r(C_n)$. □

Portanto, não há esperança de detectar a ciclicidade neste caso. O que acontece com a nilpotência?

Se $r < 0$ então $G \mapsto SC_r(G)$ detecta nilpotência para grupos de ordem fixada:

## Teorema (G, Patassini)

*Seja $G$ um grupo de ordem $n$ e seja $r$ um número real negativo.*
*Se $G$ é nilpotente então $SC_r(G) = SC_r(C_n)$.*
*Se $G$ não é nilpotente então $SC_r(G) > SC_r(C_n)$.*

## Demonstração.

Trabalhando com a soma como antes obtemos

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

O coeficiente de $B(d)$ é positivo porque $r < 0$. Assim, pelo teorema de Frobenius, $SC_r(G) \geq SC_r(C_n)$. A igualdade ocorre se e somente se $B(d) = d$ para cada $d|n$ tal que $(d, n/d) = 1$. Isso é equivalente a dizer que $G$ é nilpotente (pelo teorema de Sylow aplicado ao caso em que $d$ é uma potência de primo). □

Algumas perguntas.

1. $SC_1(G)$ detecta nilpotência para grupos de ordem fixada? (De Medts, Tarnauceanu).
2. $SC_r(G)$ com $r > 0$ detecta nilpotência para grupos de ordem fixada?
3. Como pode Keila ser tão linda?