The Chobatarev invariant of a finite group

Andrea Lucchini

Università di Padova, Italy

ISCHIA GROUP THEORY 2016
March, 29th - April, 2nd

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.

$e(G)$ can be determined using the Möbius function defined on the subgroup lattice 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

$e(\mathrm{Sym}(4)) = \frac{164317}{53130} \sim 3.0927.$

Theorem (Lubotzky 2002, AL 2015)

If G is a finite group, then $e(G) \leq d(G) + \lceil 2 \log_2 r \rceil + 5$, where r is the number of non-Frattini factors in a chief series of G.

Definition

Let G be a finite group, and $\mathcal{C} = \{C_1, \ldots, C_m\}$ be a set of conjugacy classes in G. We say that $\mathcal{C}$ generates G if, for any choice of representatives $g_i \in C_i$, the elements of the tuple $(g_1, \ldots, g_m)$ generates G. Equivalently, $\mathcal{C}$ generates G if and only if there is no maximal subgroup H of G that has non-empty intersection with each of the C_i.

Let $\mathrm{Con}(G)$ be the set of the conjugacy classes of G and let $C = (C_n)_{n \in \mathbb{N}}$ be a sequence of independent, uniformly distributed $\mathrm{Con}(G)$-valued random variables.

We may define a random variable $\tilde{\tau}_G$ by

$$\tilde{\tau}_G = \min\{n \geq 1 \mid \{C_1, \ldots, C_n\} \text{ generates } G\}.$$

The Chebotarev invariant $c(G)$ of G is the expectation of this random variable.

A subset $\{g_1, \ldots, g_d\}$ of a finite group G invariably generates G if $\{g_1^{x_1}, \ldots, g_d^{x_d}\}$ generates G for every choice of $x_i \in G$.

The Chebotarev invariant $c(G)$ of G is the expected number of elements of G which have to be drawn at random, with replacement, before a set of invariably generating elements is found.

Motivation

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G. For each prime p that is unramified in K, we have a well-defined Frobenius conjugacy class C_p in G. For simplicity, we set $C_p = 1$ when p is ramified in K. The Chebotarev density theorem says that

$$\lim_{y\to\infty} \frac{|\{p \leq y \mid C_p = C\}|}{\pi(y)} = \frac{|C|}{|G|}$$

where C is a fixed conjugacy class and $\pi(y)$ is the number of $p \leq y$.

Now fix a real number y large enough and for each $i \in \mathbb{N}$ select a random prime $p_i \leq y$. We thus have a sequence of independent and identically distributed random variables $(C_{p_i})_{i\in\mathbb{N}}$. We define the waiting time $\tau_{\mathcal{C}_y} = \min\{n \geq 1 \mid C_{p_1}, \ldots, C_{p_n} \text{ generate } G\}$. Using the Chebotarev density theorem, one can show that

$$\lim_{y\to\infty} \mathrm{E}(\tau_{\mathcal{C}_y}) = c(G).$$

Therefore, $c(G)$ can be thought of as the expected number of "random" primes p needed for C_p to generate $G = \mathrm{Gal}(K/\mathbb{Q})$.

Conjecture (Kowalski and Zywina (2010))

There exists β such that $c(G) \leq \beta\sqrt{|G|}$ for all finite groups G.

Theorem (Pomerance 2001)

Let G be a finite abelian group and for any prime divisor p of $|G|$ let $\delta_p(G) = \dim_{\mathbb{F}_p}(G/pG)$. Let $d(G) = \max_p \delta_p(G)$ be the minimal cardinality of a generating set of G. Then

$$c(G) = e(G) = d(G) + \sum_{j \geq 1} \left(1 - \prod_{p||G|} \prod_{1 \leq i \leq \delta_p(G)} \left(1 - p^{-(d(G)-\delta_p(G)+j-i)} \right) \right).$$

Corollary

If G is a finite nilpotent group, then $c(G) = e(G) \leq d(G) + \sigma$, where $\sigma \sim 2.118456565...$ (the exact value of σ can be explicitly described in terms of the Riemann zeta–function).

Kowalski and Zywina

Let $G_q = \mathrm{AGL}(1,q) = \mathbb{F}_q \rtimes \mathbb{F}_q^*$. We have

$$c(G_q) = q + \frac{1}{q} \sum_{1 \neq d \mid q-1} \frac{\mu(d)}{\left(1 - \frac{1}{d}\right)\left(1 - \frac{1}{d} + \frac{1}{q}\right)}.$$

In particular, $c(G_q) \sim q$ as $q \to \infty$.

Theorem (Kantor, Lubotzky, Shalev 2011)

There exists an absolute constant β such that

$$c(G) \leq \beta \sqrt{|G| \log |G|}$$

for all finite groups G.

THEOREM (AL 2015)

There exists an absolute constant β such that $c(G) \leq \beta\sqrt{|G|}$ for all finite groups G.

For $k \geq 1$, let $P_l(G, k)$ be the probability that k randomly chosen elements of G generate G invariably. An easy argument in probability theory shows that if $P_l(G, k) \geq \epsilon$, then $c(G) \leq k/\epsilon$. Indeed we obtain the previous theorem as a corollary of the following result.

THEOREM (2015)

For any $\epsilon > 0$ there exists τ_ϵ such that $P_l(G, k) \geq 1 - \epsilon$ for any finite group G and any $k \geq \tau_\epsilon\sqrt{|G|}$.

Let $G = C_2 \times C_2$. Then $\langle g_1, \ldots, g_n \rangle = G$ if and only if there exist $1 \leq i < j \leq n$ such that $g_i \neq 1$ and $g_j \notin \langle g_i \rangle$. We may think that we are repeating independent trials (choices of an element from G in a uniform way).

- The number of trials needed to obtain a nontrivial element x is a geometric random variable with parameter $\frac{3}{4}$ and expectation $\frac{4}{3}$.
- The number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2}{4}$ and expectation $\frac{4}{2}$.

$$c(G) = e(G) = \frac{4}{3} + \frac{4}{2} = \frac{10}{3} \quad \text{and} \quad \frac{c(G)}{\sqrt{G}} = \frac{5}{3}.$$

Theorem (G. Tracey, AL 2016)

If G is a finite soluble group, then

$$\frac{c(G)}{\sqrt{G}} \leq \frac{5}{3},$$

with equality if and only if $G = C_2 \times C_2$.

Some ideas from the proof

Let $\mathcal{V}$ be a set of representatives of the irreducible G-module that are G-isomorphic to some complemented chief factor of G.

Given $V \in \mathcal{V}$, let Ω_V be the set of the maximal subgroups M of G with the property that $\mathrm{soc}(G/M_G) \cong_G V$.

Given $k \in \mathbb{N}$ and $V \in \mathcal{V}$, denote by $P_V(k)$ the probability that k randomly chosen elements of G belong to $\cup_{g \in G} M^g$ for some $M \in \Omega_V$ and let

$$\gamma_V = \sum_k P_V(k).$$

Proposition

If G is a finite soluble group, then $c(G) \leq \sum_{V \in \mathcal{V}} \gamma_V$.

Some ideas from the proof

Let $V \in \mathcal{V}$. The number $\delta_G(V)$ of complemented factors G-isomorphic to V in any chief series of G does not depend on the series. Let $H_V = G/C_G(V)$ and let $q_V = |\mathrm{End}_G(V)|$. Moreover define $\theta_V = 0$ if $\delta_G(V) = 1$, $\theta_V = 1$ otherwise and let p_V be the probability that an element of H_V fixes a non zero vector of V.

Proposition

$$\gamma_V \leq \begin{cases} \sum_{0 \leq i \leq \delta_G(V)-1} \frac{q_V^{\delta_G(V)}}{q_V^{\delta_G(V)} - q_V^i} \leq \delta_G(V) + \frac{q_V}{(q_V-1)^2} & \text{if } H_V = 1 \\ \left(\delta_G(V)\cdot\theta_V + \frac{q_V}{q_V-1}\right)\frac{1}{p_V} \leq \left(\delta_G(V)\cdot\theta_V + \frac{q_V}{q_V-1}\right)|V| & \text{if } |H_V| \geq |V| \\ \left(\delta_G(V)\cdot\theta_V + \frac{|V|}{|V|-1}\right)|H_V| & \text{if } 1 \neq |H_V| \leq |V| \end{cases}$$

The quantity $P_V(k)$ can be estimated using the notion of crown, introduced by Gaschütz.

Let $R_G(V) = \bigcap_{M \in \Omega_V} M$.

- $P_V(k)$ can be computed working in $G/R_G(V)$.
- $G/R_G(V) \cong V^{\delta_G(V)} \rtimes H_V$.

Proposition

Let H be a soluble group acting faithfully and irreducibly on V. For a positive integer δ, consider the semidirect product $G = V^\delta \rtimes H$. View V as a vector space over $\mathrm{End}_H(V)$. Let $h_1, \ldots, h_k \in H$, and $w_1, \ldots, w_k \in V^\delta$, and write $w_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,\delta})$. Assume that $h_1 w_1, h_2 w_2, \ldots, h_k w_k$ belong to $\cup_g M^g$ for some $M \in \Omega_V$. Then for $1 \leq j \leq \delta$, the vectors $r_j := (w_{1,j}, w_{2,j}, \ldots, w_{k,j})$ of V^k are linearly dependent modulo $\{(u_1, u_2, \ldots, u_k) \mid u_i \in [h_i, V] \text{ for } 1 \leq i \leq k\}$.

Arbitrary finite groups

Theorem (G. Tracey, AL 2016)

For any positive real number ϵ, there exists a constant c_ϵ such that

$$c(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$$

for any finite group G.

Sketch of the proof

Let Ω be the set of the maximal subgroups M of G with the property that $\mathrm{soc}(G/M_G)$ is nonabelian.

Given $k \in \mathbb{N}$, denote by $P^*(k)$ the probability that k randomly chosen elements of G belong to $\cup_g M^g$ for some $M \in \Omega$ and let

$$\gamma^* = \sum_k P^*(k).$$

Proposition

If G is a finite group, then $c(G) \leq \gamma^* + \sum_{v \in \mathcal{V}} \gamma_v$.

Proposition

There exists a constant c such that $\gamma^* \leq c(\log |G|)^2$.

This depends on some consequences of the classification of the finite simple groups:

- There exists an absolute constant c_1 such that any finite group G has at most $c_1|G|^{3/2}$ maximal subgroups (Liebeck, Pyber, Shalev).
- The proportion of fixed-point-free permutations in a non-affine primitive group of degree n is at least $c_2/\log n$, for some absolute constant $c_2 > 0$. This last result in turn relies on a conjecture made independently by Boston and Shalev, stating that there exists an absolute constant $\epsilon > 0$ such that the proportion of fixed-point-free elements in any finite simple transitive permutation group is at least ϵ. This conjecture was proved for alternating groups by Łuczak and Pyber and for the simple groups of Lie type by Fulman and Guralnick.

Let $V \in \mathcal{V}$. The number $\delta_G(V)$ of complemented factors G-isomorphic to V in any chief series of G does not depend on the series. Let $H_V = G/C_G(V)$ and let $q_V = |\mathrm{End}_G(V)|$. Moreover define $\theta_V = 0$ if $\delta_G(V) = 1$, $\theta_V = 1$ otherwise and let p_V be the probability that an element of H_V fixes a non zero vector of V. Finally let $m_V = \dim_{\mathrm{End}_G(V)} \mathrm{H}^1(H_V, V)$.

Proposition

$$\gamma_V \leq \begin{cases} \sum_{0 \leq i \leq \delta_G(V)-1} \frac{q_V^{\delta_G(V)}}{q_V^{\delta_G(V)} - q_V^i} \leq \delta_G(V) + \frac{q_V}{(q_V-1)^2} & \text{if } H_V = 1 \\ \left(\delta_G(V) \cdot \theta_V + m_V + \frac{q_V}{q_V - 1}\right) \frac{1}{p_V} & \text{if } |H_V| \geq |V| \\ \left(\delta_G(V) \cdot \theta_V + \frac{|V|}{|V|-1}\right) |H_V| & \text{if } 1 \neq |H_V| \leq |V| \end{cases}$$

We need an upper bound for m_V when $|V| \leq |H_V|$.

Guralnick and Aschbacher proved that if V is an irreducible faithful H-module over a finite field, then $|\mathrm{H}^1(H, V)| < |V|$. Unfortunately this is not completely sufficient for our purposes.

Guralnick made a conjecture that there should be a universal bound on the dimension of the first cohomology groups $\mathrm{H}^1(H, V)$, where H is a finite group and V is an absolutely irreducible faithful H-module. The conjecture reduces to the case where H is a finite simple group. Very recently, computer calculations of Frank Lübeck, complemented by those of Leonard Scott and Tim Sprowl, have provided strong evidence that the Guralnick conjecture may unfortunately be false.

However for our purpose is not necessary that the Guralnick conjecture is true. A much weaker result is enough.

PROPOSITION

If V is large enough and $|V| \leq |H_V|$, then $p_V \cdot |H_V| \geq 2 \cdot (m_V + 1)^2$.