Character methods and probabilistic methods in groups

Lecture by Aner Shalev
Notes by Dustan Levenstein

Alternative title: Applications of representations in probabilistic group theory.
We can translate some ideas from representation theory into statements in probabilistic group theory.
We use words $w \in F_d$ in the free group on d letters, $w = w(x_1, \ldots, x_d)$.

I. Toy case: commutator word
$$[x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2.$$

II. General words (Larsen-Tiep-Shalev).

1 Commutators

Let G be a finite group,
$$\alpha : G \times G \to G,$$
$$\alpha(x, y) = [x, y].$$

Frobenius in 1896:
$$|\alpha^{-1}(g)| = |G| \sum_{\chi \in \operatorname{Irr} G} \frac{\chi(g)}{\chi(1)}.$$
$$P(g) := P_{\alpha,G}(g) = \frac{|\alpha^{-1}(g)|}{|G|} = \operatorname{Prob}(g = [x, y]),$$
given random elements $x, y \in G$.

So
$$P(g) = |G|^{-1} \sum_{\chi} \frac{\chi(g)}{\chi(1)}.$$

Sarnak (2006): Cancellation phenomenon which says that the value of $\sum_{\chi} \frac{\chi(g)}{\chi(1)}$ is approximately 1, much smaller than $\sum_{\chi} \left| \frac{\chi(g)}{\chi(1)} \right|$.
$$F_G(g) = \sum_{\chi \in \operatorname{Irr} G} \frac{\chi(g)}{\chi(1)}.$$

Remark $F_G(1) = k(G)$.

Shalev (2007) conjecture: If G is a finite simple group (FSG), and $g \in G$, then

I. $F_G(g) \geq 1 - o(1)$,

II. If G is of Lie type of bounded rank and $1 \neq g \in G$ then $F_G(g) \leq 1 + o(1)$.

Liebeck-Shalev (2009): No! Counterexamples:

$$PSL_3(q) \ni g \text{ transvection}$$

$$F_G(g) = 2 + O(q^{-1})$$

$$PSU_3(q) \ni g \text{ transvection}$$

$$F_G(g) = O(q^{-1})$$

Conjecture: $F_G(g) \leq C$ for all FSG's G and $1 \neq g \in G$.

Wrong. Counterexamples:

Theorem 1.1 *(Tiep-Shalev, 2017)*

I. *There is $b > 0$ such that for $g \in S_n$, if $\operatorname{supp}(g) \leq b\sqrt{n}/\log n$, then $F_{S_n}(g) \geq c^{\sqrt{n}}$ for any value of $c < e^{\pi\sqrt{2/3}}$, provided $n \gg 0$.*

II. *There is $b > 0$ such that for $g \in SL_n(q)$ a transvection.*

Hence in both cases $F_G(g) \to \infty$ as $n \to \infty$.

Remark

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2/3}\sqrt{n}} = k(S_n) = F_G(1)$$

is a result of Hardy and Ramanujan from 1918, where $p(n)$ is the number of partitions of n.

Conjecture 1.2

$$F_G(g) \leq C(r)$$

if G is a FSG of Lie type of rank r and $1 \neq g \in G$.

Garion-Shalev (2009): α is almost uniform on FSG's: $\|P - U\|_2^2 \to 0$ as $|G| \to \infty$, where U is the uniform distribution on G.

$$P = |G|^{-1} \sum_{\chi} a_\chi \chi$$

where

$$a_\chi = \frac{1}{\chi(1)}.$$

$$\|P - U\|_2^2 = \sum_{\chi \neq 1} |a_\chi|^2$$

for all G finite.

In the case $P = P_{\alpha,G}$, we have

$$\begin{aligned}\|P - U\|_2^2 &= \sum_{\chi \neq 1} \chi(1)^{-2} \\ &= \zeta_G(2) - 1 \to 0\end{aligned}$$

where

$$\zeta_G(s) = \sum \chi(1)^{-s}.$$

Corollary 1.3 *For G a FSG,*

$$\frac{\operatorname{Im}\alpha}{|G|} \to 1$$

as

$$|G| \to \infty,$$

i.e. almost all elements $g \in G$ are commutators.

Conjecture 1.4 *(Ore 1951)*
All elements of FSG's are commutators.

Theorem 1.5 *(Liebeck-O'Brien-Shalev-Tiep "LOST" 2010)*
Ore's conjecture holds.

Theorem 1.6 *(Guralnick-LOST "GLOST" 2018)*
If $n = p^a q^b$ for primes p, q, then $x^n y^n$ is surjective on ALL FSG's.

Remark Recall Burnside's theorem that groups of this order n are solvable.

2 Word Maps

Let $w \in F_d$, $w = w(x_1, \ldots, x_d)$. If G is a group, then we associate the word map

$$w = w_G : G^d \to G$$

$$(g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d).$$

Theorem 2.1 *(Borel 1983)*
Word maps on simple algebraic groups are dominant.

Theorem 2.2 *(Larsen-Tiep-Shalev 2011)*
If $w_1, w_2 \neq 1$ are words in disjoint sets of variables, then there exists an $N = N(w_1, w_2)$ such that if G is a FSG with $|G| \geq N$ then

$$G = w_1(G) \cdot w_2(G).$$

(Note that $w_1(G)$ should be taken as shorthand for $w_1(G^d)$ for d appropriate.)

Probabilistic aspects:
Let $w \in F_d$, $g \in G$ finite group.

$$P_{w,G}(g) = \frac{|w^{-1}(g)|}{|G|^d} = \operatorname{Prob}(w(g_1, \ldots, g_d) = g).$$

Theorem 2.3 *(Larsen-Shalev 2012)*

$$|P_{w,G}(g)| \leq |G|^{-\epsilon + o(1)}$$

for G a FSG and some $\epsilon = \epsilon(w) > 0$.

Question: Which words are almost uniform on all FSG's?
Namely, for which words w we have $||p_{w,G} - U_G||_1 \to 0$ as $|G| \to \infty$ (we use the L^1 norm).
Probabilistic Waring Problem: Let $w_1, w_2 \neq 1$ be words in disjoint sets of variables. Then $w_1 w_2$ is almost uniform on FSG's.
Positive evidence:

I. True for $x^2 y^2$ (Garion-Shalev 2009),

II. True for $x^m y^n$ (Larsen-Shalev 2016)

Theorem 2.4 *(Larsen-Tiep-Shalev, 2018$^+$)*
True in general: for w_1, w_2 as above,

$$\|P_{w_1 w_2, G} - U\|_1 \to 0$$

as

$$|G| \to \infty$$

for G a FSG.

Proof (sketch)

I. Case A_n: 2008 Larsen-Shalev uses new character bounds and & free probability (Nica's Theorem).

II. Groups of Lie type of bounded rank: Ingredients

(a) most elements are regular semisimple,

(b) $w_i(g_1, \ldots, g_d)$ is regular semisimple with probability approaching 1 (Borel & Lang-Weil),

(c) We compute the probability that $x_1 x_2 = g$, for random $x_i \in C_i$, conjugacy classes of G.

$$p(C_1, C_2, g) = |G|^{-1} \sum_{\chi} \chi(C_1)\chi(C_2)\chi(g^{-1})/\chi(1)$$

(d) $|\chi(g)| \leq c(r)$ where g is regular semisimple and $c(r)$ is the rank.

Putting these pieces together and using $\zeta_G(s)$ eventually gives the proof in bounded rank.

III. Classical groups of rank $r \to \infty$

Important tool: two new papers by Guralnick-Larsen-Tiep 2017-2018 (Character levels & Character bounds).

What is needed is: for every $\epsilon, c > 0$ there exists $f(\epsilon, c)$ such that for $G = G_r(q)$ classical of rank $r \geq f(\epsilon, c)$ and for $g \in G$ with $|C_G(g)| \leq q^{cr}$, we have $|\chi(g)| \leq \chi(1)^\epsilon$ for every χ.

The strategy extends the bounded rank case. Let $w = w_1 w_2$ as before. We show that

$$C_G(w_i(g_1, \ldots, g_d))| \leq q^{cr}$$

almost surely, and conclude that

$$|\chi(w_i(g_1, \ldots, g_d))| \leq \chi(1)^\epsilon$$

for all χ almost surely.

We fix $0 < \epsilon < 1/3$ and proceed in a similar manner, using the fact that
$\zeta_G(1 - 3\epsilon) \to 1$ if $r \gg 0$.