The probability of generating invariably a finite simple group

Eilidh McKemmie (HUJI), joint work with Daniele Garzoni (Padova)

Invariable generation

Definition

Let G be a finite group and let $S = \{s_1, ..., s_k\} \subseteq G$. The subgroup of G invariably generated by S is

$$\bigcap_{g_1,...,g_k \in G} \langle s_1^{g_1}, ..., s_k^{g_k} \rangle$$

Invariable generation

Definition

Let G be a finite group and let $S = \{s_1, ..., s_k\} \subseteq G$. The subgroup of G invariably generated by S is

$$\bigcap_{g_1, ..., g_k \in G} \langle s_1^{g_1}, ..., s_k^{g_k} \rangle$$

Proposition

A set of elements in S_n fails to generate a transitive subgroup if and only if the elements fix a common set.

Invariable generation

Definition

Let G be a finite group and let $S = \{s_1, ..., s_k\} \subseteq G$. The subgroup of G invariably generated by S is

$$\bigcap_{g_1,...,g_k \in G} \langle s_1^{g_1}, ..., s_k^{g_k} \rangle$$

Proposition

A set of elements in S_n fails to invariably generate a transitive subgroup if and only if the elements fix sets of a common size.

Motivation

Given a polynomial $f \in \mathbb{Z}[x]$ of degree n, $Gal(f) \leq S_n$.

Question

Does $Gal(f) = S_n$*?*

Motivation

Given a polynomial $f \in \mathbb{Z}[x]$ of degree n, $Gal(f) \leq S_n$.

Question

Does $Gal(f) = S_n$*?*

- Take a prime $p \nmid disc(f)$.
- f factorises into pairwise distinct irreducible factors modulo p.
- The set of degrees of factors is a partition λ_p of n.
- There is an element of $Gal(f)$ with cycle type λ_p.

Motivation

Given a polynomial $f \in \mathbb{Z}[x]$ of degree n, $Gal(f) \leq S_n$.

Question

Does $Gal(f) = S_n$*?*

- Take a prime $p \nmid disc(f)$.
- f factorises into pairwise distinct irreducible factors modulo p.
- The set of degrees of factors is a partition λ_p of n.
- There is an element of $Gal(f)$ with cycle type λ_p.

Proposition

If there is a set of primes P which do not divide the discriminant such that $\{\lambda_p\}_{p \in P}$ invariably generates S_n then $Gal(f) = S_n$.

Question

How likely is it that we get a false negative after choosing k primes?

Question

How likely is it that we get a false negative after choosing k primes?

Proposition (Frobenius Density Theorem)

Let λ be a partition of n.

$$\left\{ \begin{array}{c} \text{proportion of elements} \\ \text{of } Gal(f) \text{ with cycle} \\ \text{type } \lambda \end{array} \right\} = \left\{ \begin{array}{c} \text{proportion of primes} \\ p \nmid disc(f) \text{ for which} \\ \lambda_p = \lambda \end{array} \right\} + o(1)$$

Question

How likely is it that we get a false negative after choosing k primes?

Proposition (Frobenius Density Theorem)

Let λ be a partition of n.

$$\left\{ \begin{array}{c} \textit{proportion of elements} \\ \textit{of } Gal(f) \textit{ with cycle} \\ \textit{type } \lambda \end{array} \right\} = \left\{ \begin{array}{c} \textit{proportion of primes} \\ p \nmid disc(f) \textit{ for which} \\ \lambda_p = \lambda \end{array} \right\} + o(1)$$

Answer

The probability of getting a false negative is the probability that k random elements of S_n do not invariably generate.

Invariable vs classical generation

Definition

$\mathbb{P}_{(inv)}(G, k) =$ the probability k random elements (invariably) generate G.

Invariable vs classical generation

Definition

$\mathbb{P}_{(inv)}(G,k) =$ the probability k random elements (invariably) generate G.

Theorem (Liebeck-Shalev)

For a finite simple group G, $\lim_{|G|\to\infty} \mathbb{P}(G,2) = 1$

Theorem (Kantor-Lubotzky-Shalev, Guralnick-Malle)

If G is a finite simple group, $\mathbb{P}_{inv}(G,2) > 0$.

Invariable vs classical generation

Definition

$\mathbb{P}_{(inv)}(G,k)$ = the probability k random elements (invariably) generate G.

Theorem (Liebeck-Shalev)

For a finite simple group G, $\lim_{|G|\to\infty}\mathbb{P}(G,2)=1$

Theorem (Kantor-Lubotzky-Shalev, Guralnick-Malle)

If G is a finite simple group, $\mathbb{P}_{inv}(G,2)>0$.

Theorem (Kantor-Lubotzky-Shalev)

There is an absolute constant ε such that for all G and k, $\mathbb{P}_{inv}(G,k)\leq 1-\varepsilon^k$.

Symmetric group

Theorem (Pemantle-Peres-Rivin, Eberhard-Ford-Green)

There is $\varepsilon > 0$ *such that* $\mathbb{P}_{inv}(S_n, 4) \geq \varepsilon$ *for all* n*.*
$\lim_{n\to\infty} \mathbb{P}_{inv}(S_n, 3) = 0$.

Theorem (McK)

Let $G_r(q)$ *be a finite classical group of rank* r *over a field of* q *elements.*
There is $\varepsilon > 0$ *such that* $\mathbb{P}_{inv}(G_r(q), 4) \geq \varepsilon$ *for all* r *and large enough* q*.*
$\lim_{q\to\infty} \lim_{r\to\infty} \mathbb{P}_{inv}(G_r(q), 3) = 0$.

Invariable vs classical generation

Definition

Let $A \subseteq G$.
$\mathbb{P}_{(inv)}(G, A) =$ the probability that a random element from G (invariably) generates with some element of A.

Invariable vs classical generation

Definition

Let $A \subseteq G$.
$\mathbb{P}_{(inv)}(G, A) =$ the probability that a random element from G (invariably) generates with some element of A.

Theorem (Guralnick-Kantor)

If G is a finite simple group then $\mathbb{P}(G, G) = 1$. This is called 3/2-generation.

Theorem (Burness-Harper)

For infinitely many finite simple groups G, there is a subset A with $|A| = 2$ and $\mathbb{P}(G, A) = 1$.

Results (joint with Daniele Garzoni)

Let G be a finite simple group.

Theorem

There exist $\varepsilon > 0$ and $x \in G$ such that $\mathbb{P}_{inv}(G, \{x\}) \geq \varepsilon$.

Theorem

There exists a set $A \subseteq G$ such that $|A| \leq 6$ and

$$\lim_{|G| \to \infty} \mathbb{P}_{inv}(G, A) = 1$$

unless $G = G_2(3^a), PSp_{2m}(q)$ for q even and bounded, $P\Omega_{2m+1}(q)$ for q odd and bounded. Then $\mathbb{P}_{inv}(G, G)$ is bounded away from 1.

Results (joint with Daniele Garzoni)

Let $G_r(q)$ be a finite group of Lie type of rank r over a field of order q.

Theorem

There is an absolute constant $c > 0$ such that for almost all $x \in G_r(q)$ (or for around half the elements $x \in G_2(3^a)$),

$$\mathbb{P}_{inv}(G, \{x\}) \geq \frac{c}{r} + O\left(\frac{r^r}{q}\right).$$

Corollary

For each rank r there is a constant $\varepsilon_r > 0$ such that $\mathbb{P}_{inv}(G_r(q), 2) \geq \varepsilon_r$ for all q.

Conjecture

For G a finite simple group $\mathbb{P}_{inv}(G, 4)$ is bounded away from 0 as $|G| \to \infty$.

Maximal subgroups

Proposition

Let

$$\mathcal{M}(x) = \cup_{x \in M \leq_{max} G} \cup_{g \in G} M^g.$$

Then

$$1 - \mathbb{P}_{inv}(G, A) = \frac{|\cap_{x \in A} \mathcal{M}(x)|}{|G|}.$$

Aim: find elements x such that $\mathcal{M}(x)$ is small.

Alternating groups

Example

Let $n = 2m + 1$ be odd, and $G = A_n$.
$x =$ an n-cycle.
$\mathcal{M}(x) =$ union of all transitive subgroups.
Łuczak and Pyber show

$$\lim_{m\to\infty} \frac{|\mathcal{M}(x)|}{|A_{2m+1}|} = 0.$$

Groups of Lie type with fixed rank

X is a linear algebraic group	$X = SL_n(\overline{\mathbb{F}_p})$
W is the Weyl group of X	$W \cong S_n$
σ is a Steinberg endomorphism of X	$\sigma(x_{ij}) = (x_{ij}^q)$
G is the set of fixed points X_σ	$G = SL_n(q)$
$W.\langle\sigma\rangle$ is the extended Weyl group	$W.\langle\sigma\rangle \cong S_n$

Definition

A regular semisimple element s in X is a diagonalisable element contained in a unique σ-stable maximal torus $T = C_X(s)^\circ$ of X.

$$\Delta := \{x \in G \text{ regular semisimple} \mid \text{maximal overgroups have maximal rank}\}$$

Proposition (Fulman-Guralnick)

The proportion of elements of G in Δ is $1 - O\left(\frac{r^r}{q}\right)$.

Maximal tori

Definition

$\mathcal{T}(x)$ is the set of conjugates of maximal tori of G contained in some K_σ° for K a maximal subgroup of X containing x.

Theorem

If $\bigcap_{a\in A}\mathcal{T}(a) = \emptyset$ *then for every* $x \in \Delta$ *there is some* $a \in A$ *such that* x, a *invariably generate* G.

Exceptional groups

Example

$G = E_8(q)$. Guralnick and Malle identify a cyclic maximal torus $T = \langle a \rangle$ of order $\Phi_{30}(q)$ whose only maximal overgroup is $N_G(T)$. So $\mathcal{T}(a) = T^G$.
Pick a' not in any conjugate of $N_G(T)$. For example, there is an element of order $\Phi_{30}(-q)$ which, by its order alone, cannot be in $N_G(T)$.

The Weyl group

There is a natural bijection

$$\left\{\begin{array}{c} G\text{-conjugacy classes of} \\ \sigma\text{-stable maximal tori of} \\ X \end{array}\right\} \leftrightarrow \left\{\begin{array}{c} W\text{-conjugacy classes in} \\ \text{the coset } \sigma W \text{ of } \sigma \text{ in} \\ \sigma.W \end{array}\right\}$$

$$T_w \leftrightarrow \sigma w$$

Write T_w for $(T_w)_\sigma$.

More exceptional groups

Example

$G_2(q)$ has Weyl group D_{12} and so it has 6 conjugacy classes of maximal tori, called $T_1, ...T_6$.
T_1, T_2 contain around half the elements in the group.
If $q \nmid 3$ we can pick x_1, x_2 such that $\mathcal{T}(x_1) =$ conjugates of T_1, T_3, T_5 and $\mathcal{T}(x_2) =$ conjugates of T_2, T_4, T_6.
In characteristic 3, there is a graph automorphism which conjugates T_1 to T_2.

Classical groups with fixed rank

Example

$G = SL_n(q)$, $W \cong S_n$. Let a be a regular semisimple element in $T_{(n-1,1)}$. Then $\mathcal{T}(a) = T^G_{(n-1,1)}$. If $a' \in T_{(n)}$ is regular semisimple then its overgroups are extension field subgroups $SL_{\frac{n}{b}}(q^b)$ which do not fix any 1-spaces.
So $\mathcal{T}(a) \cap \mathcal{T}(a') = \emptyset$.

Large rank

Example

$G = SL_{2m+1}(q)$ with q fixed and $m \to \infty$.
Guralnick and Kantor give an element a such that $\mathcal{M}(a)$ is the union of groups which fix an m-space and an $m+1$-space.
Fulman and Guralnick show that the proportion of elements in $SL_n(q)$ fixing a k-space is at most

$$\frac{A}{k^{0.005}}$$

for an absolute constant A.

Example

Let $G = Sp_{2m}(q)$ where q is even and fixed and $m \to \infty$.
Let $R^{\pm}$ be the union of the stabilisers of hyperplanes of $\pm$-type.
Then $G = R^+ \cup R^-$ but

$$\frac{|R^+ \cap R^-|}{|G|} \geq \frac{1}{4q^3}$$

and so $\mathbb{P}_{inv}(G, G) \leq 1 - \frac{1}{4q^3}$.