Conjectures and miracles in finite simple groups

Aner Shalev
Hebrew University Jerusalem

Colloquium Talk
Permutation Groups Workshop
Fischer Fest
Bielefeld, January 12 2017

Main themes:

Main themes:

Generation in finite simple groups and special primes

Main themes:

Generation in finite simple groups and special primes

Approximate subgroups, growth and normal growth

Main themes:

Generation in finite simple groups and special primes

Approximate subgroups, growth and normal growth

Ore's conjecture and Thompson's conjecture

Main themes:

Generation in finite simple groups and special primes

Approximate subgroups, growth and normal growth

Ore's conjecture and Thompson's conjecture

Mixing, complexity and conjectures of Gowers and Viola

The unbearable easiness of generating FSG

$d(G)$ = minimal number of generators of a finite group G

FSG = nonabelian finite simple group

The unbearable easiness of generating FSG

$d(G) =$ minimal number of generators of a finite group G

FSG $=$ nonabelian finite simple group

Assume CFSG:
Every FSG is Alternating A_n $(n \geq 5)$, or
Classical of Lie type, e.g. $PSL_n(q)$, or
Exceptional of Lie type, e.g. $E_8(q)$, or
one of 26 Sporadic Groups, e.g. Fischer Groups $Fi_{22}, Fi_{23}, Fi'_{24}$.

The unbearable easiness of generating FSG

$d(G)$ = minimal number of generators of a finite group G

FSG = nonabelian finite simple group

Assume CFSG:
Every FSG is Alternating A_n $(n \geq 5)$, or
Classical of Lie type, e.g. $PSL_n(q)$, or
Exceptional of Lie type, e.g. $E_8(q)$, or
one of 26 Sporadic Groups, e.g. Fischer Groups $Fi_{22}, Fi_{23}, Fi_{24}'$.

Steinberg, Aschbacher-Guralnick 1984: $d(G) = 2$ for all FSG G.

The unbearable easiness of generating FSG

$d(G)$ = minimal number of generators of a finite group G

FSG = nonabelian finite simple group

Assume CFSG:
Every FSG is Alternating A_n $(n \geq 5)$, or
Classical of Lie type, e.g. $PSL_n(q)$, or
Exceptional of Lie type, e.g. $E_8(q)$, or
one of 26 Sporadic Groups, e.g. Fischer Groups $Fi_{22}, Fi_{23}, Fi'_{24}$.

Steinberg, Aschbacher-Guralnick 1984: $d(G) = 2$ for all FSG G.

Can we deduce this from simplicity without CFSG? Probably not

The unbearable easiness of generating FSG

$d(G)$ = minimal number of generators of a finite group G

FSG = nonabelian finite simple group

Assume CFSG:
Every FSG is Alternating A_n $(n \geq 5)$, or
Classical of Lie type, e.g. $PSL_n(q)$, or
Exceptional of Lie type, e.g. $E_8(q)$, or
one of 26 Sporadic Groups, e.g. Fischer Groups $Fi_{22}, Fi_{23}, Fi'_{24}$.

Steinberg, Aschbacher-Guralnick 1984: $d(G) = 2$ for all FSG G.

Can we deduce this from simplicity without CFSG? Probably not

Malle-Saxl-Weigel 1994: Every FSG is generated by an involution and another element.

The unbearable easiness of generating FSG

$d(G)$ = minimal number of generators of a finite group G

FSG = nonabelian finite simple group

Assume CFSG:
Every FSG is Alternating A_n ($n \geq 5$), or
Classical of Lie type, e.g. $PSL_n(q)$, or
Exceptional of Lie type, e.g. $E_8(q)$, or
one of 26 Sporadic Groups, e.g. Fischer Groups $Fi_{22}, Fi_{23}, Fi'_{24}$.

Steinberg, Aschbacher-Guralnick 1984: $d(G) = 2$ for all FSG G.

Can we deduce this from simplicity without CFSG? Probably not

Malle-Saxl-Weigel 1994: Every FSG is generated by an involution and another element.

Guralnick-Kantor 2000: For any FSG G and any $1 \neq x \in G$ there is $y \in G$ s.t. $\langle x, y \rangle = G$ (3/2-generation)

Proofs use counting and probabilistic methods

1882 Netto's conjecture: A_n is randomly generated by 2 elements.

1882 Netto's conjecture: A_n is randomly generated by 2 elements.

1969 Dixon's conjecture: Same for all FSG.

1882 Netto's conjecture: A_n is randomly generated by 2 elements.

1969 Dixon's conjecture: Same for all FSG.

Dixon, Kantor-Lubotzky, Liebeck-Sh 1995:
Dixon's conjecture holds.
Proof idea: study $\zeta_1^G(s) = \sum_{M \ max \ G} |G : M|^{-s}$ and its abscissa of convergence. Show $\zeta_1^G(2) \to 0$ as $|G| \to \infty$.

1882 Netto's conjecture: A_n is randomly generated by 2 elements.

1969 Dixon's conjecture: Same for all FSG.

Dixon, Kantor-Lubotzky, Liebeck-Sh 1995:
Dixon's conjecture holds.
Proof idea: study $\zeta_1^G(s) = \sum_{M \ max \ G} |G:M|^{-s}$ and its abscissa of convergence. Show $\zeta_1^G(2) \to 0$ as $|G| \to \infty$.

G is randomly (2,3)-generated if random $x, y \in G$ with $x^2 = y^3 = 1$ generate G with probability $\to 1$ as $|G| \to \infty$.

Liebeck-Sh 1996 (Annals), Guralnick-Sh 2006 (unpublished):
FSG $\neq Sz(q), PSp_4(q)$ are randomly (2,3)-generated.

1882 Netto's conjecture: A_n is randomly generated by 2 elements.

1969 Dixon's conjecture: Same for all FSG.

Dixon, Kantor-Lubotzky, Liebeck-Sh 1995:
Dixon's conjecture holds.
Proof idea: study $\zeta_1^G(s) = \sum_{M \ max \ G} |G : M|^{-s}$ and its abscissa of convergence. Show $\zeta_1^G(2) \to 0$ as $|G| \to \infty$.

G is randomly (2,3)-generated if random $x, y \in G$ with $x^2 = y^3 = 1$ generate G with probability $\to 1$ as $|G| \to \infty$.

Liebeck-Sh 1996 (Annals), Guralnick-Sh 2006 (unpublished):
FSG $\neq Sz(q), PSp_4(q)$ are randomly (2,3)-generated.

Main step in proof: show $\zeta_1^G(66/65) \to 0$ as $|G| \to \infty$.
Liebeck-Martin-Sh 2005: Same for $\zeta_1^G(s)$ for any $s > 1$.

1882 Netto's conjecture: A_n is randomly generated by 2 elements.

1969 Dixon's conjecture: Same for all FSG.

Dixon, Kantor-Lubotzky, Liebeck-Sh 1995:
Dixon's conjecture holds.
Proof idea: study $\zeta_1^G(s) = \sum_{M \ max \ G} |G : M|^{-s}$ and its abscissa of convergence. Show $\zeta_1^G(2) \to 0$ as $|G| \to \infty$.

G is randomly (2,3)-generated if random $x, y \in G$ with $x^2 = y^3 = 1$ generate G with probability $\to 1$ as $|G| \to \infty$.

Liebeck-Sh 1996 (Annals), Guralnick-Sh 2006 (unpublished):
FSG $\neq Sz(q), PSp_4(q)$ are randomly (2,3)-generated.

Main step in proof: show $\zeta_1^G(66/65) \to 0$ as $|G| \to \infty$.
Liebeck-Martin-Sh 2005: Same for $\zeta_1^G(s)$ for any $s > 1$.

Consequence: All large FSG except $Sz(2^k)$, $PSp_4(2^k)$, $PSp_4(3^k)$ are images of the modular group $PSL_2(\mathbb{Z})$.

Lübeck-Malle 1997: Exceptional groups of Lie type.

Subgroups of FSG

For subgroups H of FSG G, $d(H)$ may be arbitrarily large.

Subgroups of FSG

For subgroups H of FSG G, $d(H)$ may be arbitrarily large.

Theorem (Burness-Liebeck-Sh 2013)

All maximal subgroups of FSG are generated by ≤ 4 elements.

4 is best possible

Subgroups of FSG

For subgroups H of FSG G, $d(H)$ may be arbitrarily large.

Theorem (Burness-Liebeck-Sh 2013)

All maximal subgroups of FSG are generated by ≤ 4 elements.

4 is best possible

Application to permutation groups:

If G is a finite permutation group, $H < G$ a point-stabilizer, then $d(G) - 1 \leq d(H) \leq d(G) + 4$.

Subgroups of FSG

For subgroups H of FSG G, $d(H)$ may be arbitrarily large.

Theorem (Burness-Liebeck-Sh 2013)

All maximal subgroups of FSG are generated by ≤ 4 elements.

4 is best possible

Application to permutation groups:

If G is a finite permutation group, $H < G$ a point-stabilizer, then $d(G) - 1 \leq d(H) \leq d(G) + 4$.

Theorem (Burness-Liebeck-Sh 2013)

For every $\epsilon > 0$ there exists $c = c(\epsilon)$ such that if M is a maximal subgroup of a FSG then the probability that c random elements of M generate M exceeds $1 - \epsilon$.

Subgroups of FSG

For subgroups H of FSG G, $d(H)$ may be arbitrarily large.

Theorem (Burness-Liebeck-Sh 2013)

All maximal subgroups of FSG are generated by ≤ 4 elements.

4 is best possible

Application to permutation groups:

If G is a finite permutation group, $H < G$ a point-stabilizer, then $d(G) - 1 \leq d(H) \leq d(G) + 4$.

Theorem (Burness-Liebeck-Sh 2013)

For every $\epsilon > 0$ there exists $c = c(\epsilon)$ such that if M is a maximal subgroup of a FSG then the probability that c random elements of M generate M exceeds $1 - \epsilon$.

Do non-maximal subgroups of FSG share similar properties?

Go down the subgroup lattice. Definition: $M \leq G$ is t-maximal if $M = M_t < M_{t-1} < \ldots < M_0 = G$ such that M_i max M_{i-1}.

Second maximal subgroups

Second maximal $=$ 2-maximal

Bad Example:
$G = L_2(2^k) = PSL_2(2^k)$ with $2^k - 1$ a Mersenne prime
$B =$ Borel subgroup of G. $H = C_2^k$ is a maximal subgroup of B.
So H is second maximal in G, and $d(H) = k$.

Second maximal subgroups

Second maximal = 2-maximal

Bad Example:
$G = L_2(2^k) = PSL_2(2^k)$ with $2^k - 1$ a Mersenne prime
$B =$ Borel subgroup of G. $H = C_2^k$ is a maximal subgroup of B.
So H is second maximal in G, and $d(H) = k$.

Conclusion:
If there are infinitely many Mersenne primes, then the numbers of generators of second maximal subgroups of FSG are unbounded.

Second maximal subgroups

Second maximal = 2-maximal

Bad Example:
$G = L_2(2^k) = PSL_2(2^k)$ with $2^k - 1$ a Mersenne prime
B = Borel subgroup of G. $H = C_2^k$ is a maximal subgroup of B.
So H is second maximal in G, and $d(H) = k$.

Conclusion:
If there are infinitely many Mersenne primes, then the numbers of generators of second maximal subgroups of FSG are unbounded.

Largest currently known prime is a Mersenne prime with $k = 74207281$.
Hence there exists a second maximal subgroup H of a FSG with $d(H) = 74207281$.

New joint work with Tim Burness and Martin Liebeck

New joint work with Tim Burness and Martin Liebeck

If G is a FSG of rank > 1 then the numbers of generators of second maximal subgroups of G are bounded.

New joint work with Tim Burness and Martin Liebeck

If G is a FSG of rank > 1 then the numbers of generators of second maximal subgroups of G are bounded.

Theorem (Burness-Liebeck-Sh 2016$^+$)

Let G be a FSG and let H be a second maximal subgroup of G. Then one of the following holds:
(i) $d(H) \leq 12$;
(ii) $d(H) \leq 70$, G is exceptional of Lie type, and H is a maximal subgroup of a parabolic subgroup of G;
(iii) $G_0 = \mathrm{L}_2(q)$, ${}^2B_2(q)$ or ${}^2G_2(q)$, and H is maximal in a Borel subgroup of G.

Long proof using subgroup structure of FSG, e.g. Aschbacher's Theorem, representations and other tools.
We also show: if H is not as in (iii) then H is randomly generated by boundedly many elements.

Special Primes

Can $d(H)$ be arbitrarily large for the groups in part (iii)?

We show this depends on a formidable open problem in Number Theory:

Special Primes

Can $d(H)$ be arbitrarily large for the groups in part (iii)?

We show this depends on a formidable open problem in Number Theory:

(*) Are there infinitely many k for which there is a prime power q such that $(q^k - 1)/(q - 1)$ is prime?

It is believed that (*) holds, but no clue how to prove it.

It's not even known whether $\frac{q^k-1}{q-1}$ has a large prime divisor.

Special Primes

Can $d(H)$ be arbitrarily large for the groups in part (iii)?

We show this depends on a formidable open problem in Number Theory:

(*) Are there infinitely many k for which there is a prime power q such that $(q^k - 1)/(q - 1)$ is prime?

It is believed that (*) holds, but no clue how to prove it.
It's not even known whether $\frac{q^k-1}{q-1}$ has a large prime divisor.

Theorem (Burness-Liebeck-Sh 2016^+)

The following are equivalent.
(i) There is a constant c such that all second maximal subgroups of FSG are generated by $\leq c$ elements.
(ii) There is a constant c such that all second maximal subgroups of $\mathrm{L}_2(q)$ (q a prime power) are generated by $\leq c$ elements.
(iii) Question (*) has a negative answer.

Third maximal subgroups

In view of the difficulty of question (*), the validity of part (i) of the Theorem is likely to remain open.

Third maximal subgroups

In view of the difficulty of question (*), the validity of part (i) of the Theorem is likely to remain open.

However, if we go further down the subgroup lattice and consider third maximal subgroups, we can show unconditionally:

For each c there is a third maximal subgroup H of a FSG such that $d(H) > c$.

Growth and approximate subgroups

G a group, $X \subset G$, $X^k = \{x_1 \cdots x_k : x_i \in X\}$.
Growth of $|X^k|$? In particular, for $k = 2, 3$.
X is c-approximate subgroup if $|X^3| \leq c|X|$.

Growth and approximate subgroups

G a group, $X \subset G$, $X^k = \{x_1 \cdots x_k : x_i \in X\}$.
Growth of $|X^k|$? In particular, for $k = 2, 3$.
X is c-approximate subgroup if $|X^3| \leq c|X|$.

2008 Helfgott: Let $G = \mathrm{SL}_2(p)$ and A any generating set for G. Then either $A^3 = G$ or $|A^3| \geq |A|^{1+\epsilon}$, where $\epsilon > 0$ is some absolute constant.
Generalize to other matrix groups? E.g. $\mathrm{SL}_r(q)$?
Helfgott: $r = 3, q = p$, very long proof

Growth and approximate subgroups

G a group, $X \subset G$, $X^k = \{x_1 \cdots x_k : x_i \in X\}$.
Growth of $|X^k|$? In particular, for $k = 2, 3$.
X is c-approximate subgroup if $|X^3| \leq c|X|$.

2008 Helfgott: Let $G = \mathrm{SL}_2(p)$ and A any generating set for G. Then either $A^3 = G$ or $|A^3| \geq |A|^{1+\epsilon}$, where $\epsilon > 0$ is some absolute constant.
Generalize to other matrix groups? E.g. $\mathrm{SL}_r(q)$?
Helfgott: $r = 3, q = p$, very long proof

The Product Theorem:

Theorem (Pyber-Szabó, Breuillard-Green-Tao)

Let G be any finite simple group of Lie type, and A any generating set for G. Then either $A^3 = G$ or $|A^3| \geq |A|^{1+\epsilon}$, where $\epsilon > 0$ depends only on the rank of G.

The proof of BGT also rely on related results of Hrushovski using model theory.

Normal growth

$A \subseteq G$ is normal if it's closed under conjugation by elements of G (i.e. A is a union of conjugacy classes).

Rapid 2-step growth for such subsets:

Theorem (Liebeck-Schul-Sh 2016^{+})

Given any $\epsilon > 0$, there exists $\delta > 0$ such that if A is a normal subset of a finite simple group G satisfying $|A| \leq |G|^{\delta}$, then $|A^2| \geq |A|^{2-\epsilon}$.

Normal growth

$A \subseteq G$ is normal if it's closed under conjugation by elements of G (i.e. A is a union of conjugacy classes).

Rapid 2-step growth for such subsets:

Theorem (Liebeck-Schul-Sh 2016^+)

Given any $\epsilon > 0$, there exists $\delta > 0$ such that if A is a normal subset of a finite simple group G satisfying $|A| \leq |G|^\delta$, then $|A^2| \geq |A|^{2-\epsilon}$.

Remarks:

1. $|A^2| \leq |A|^2$, so A grows almost as fast as possible.
2. Normality assumption is essential: otherwise $|A^2|$ may be very close to $|A|$.
3. Strengthens a result of Gill-Pyber-Short-Szabó 2013 yielding $|A^2| \geq |A|^{1+\epsilon}$.
4. A version for two normal subsets: $|A_1 A_2| \geq (|A_1||A_2|)^{1-\epsilon}$.
5. A version for simple algebraic groups: $\dim A^2 \geq (2-\epsilon) \dim A$.

Proof ideas

Want to prove $|A^2| \geq |A|^{2-\epsilon}$.

Proof ideas

Want to prove $|A^2| \geq |A|^{2-\epsilon}$.

Stage 1: Enough to show this for alternating groups of large degree and for classical group of large rank.

Proof ideas

Want to prove $|A^2| \geq |A|^{2-\epsilon}$.

Stage 1: Enough to show this for alternating groups of large degree and for classical group of large rank.

Stage 2: Reduction to the case where A is a conjugacy class.
This is done by showing that a normal subset $A \subseteq G$ contains a conjugacy class C of comparable size: $|C| \geq |A|^{1-\epsilon}$.
Main tool: a "zeta function" $\zeta_2^G(s) = \sum_{C \text{ class of } G} |C|^{-s}$ encoding class sizes and its abscissa of convergence.

Proof ideas

Want to prove $|A^2| \geq |A|^{2-\epsilon}$.

Stage 1: Enough to show this for alternating groups of large degree and for classical group of large rank.

Stage 2: Reduction to the case where A is a conjugacy class.
This is done by showing that a normal subset $A \subseteq G$ contains a conjugacy class C of comparable size: $|C| \geq |A|^{1-\epsilon}$.
Main tool: a "zeta function" $\zeta_2^G(s) = \sum_{C \text{ class of } G} |C|^{-s}$ encoding class sizes and its abscissa of convergence.

Stage 3: connect the class size $|C|$ with the "support" of its elements.

Proof ideas

Want to prove $|A^2| \geq |A|^{2-\epsilon}$.

Stage 1: Enough to show this for alternating groups of large degree and for classical group of large rank.

Stage 2: Reduction to the case where A is a conjugacy class.
This is done by showing that a normal subset $A \subseteq G$ contains a conjugacy class C of comparable size: $|C| \geq |A|^{1-\epsilon}$.
Main tool: a "zeta function" $\zeta_2^G(s) = \sum_{C \text{ class of } G} |C|^{-s}$ encoding class sizes and its abscissa of convergence.

Stage 3: connect the class size $|C|$ with the "support" of its elements.

Stage 4: find a class $C \subseteq A^2$ of large enough support and use stage 3 to show $|C| \geq |A|^{2-\epsilon}$.

Ore's Conjecture 1951: Every element of a FSG is a commutator.

Ore's Conjecture 1951: Every element of a FSG is a commutator.

Liebeck-O'Brien-Sh-Tiep 2010: Ore's Conjecture holds.

Ore's Conjecture 1951: Every element of a FSG is a commutator.

Liebeck-O'Brien-Sh-Tiep 2010: Ore's Conjecture holds.

Thompson's Conjecture: Every FSG G has a conjugacy class C such that $C^2 = G$. This implies Ore's Conjecture: $C^2 = G \Rightarrow 1 \in C^2 \Rightarrow C = C^{-1} \Rightarrow C^{-1}C = G$ so each $g \in G$ is $x^{-1}x^y = [x, y]$ for some $x \in C$.

Ore's Conjecture 1951: Every element of a FSG is a commutator.

Liebeck-O'Brien-Sh-Tiep 2010: Ore's Conjecture holds.

Thompson's Conjecture: Every FSG G has a conjugacy class C such that $C^2 = G$. This implies Ore's Conjecture:
$C^2 = G \Rightarrow 1 \in C^2 \Rightarrow C = C^{-1} \Rightarrow C^{-1}C = G$ so each $g \in G$ is $x^{-1}x^y = [x, y]$ for some $x \in C$.

WIDE OPEN for classical groups over small fields.
Larsen-Sh-Tiep (Annals 2011, large G)
Guralnick-Malle (JAMS 2012, all G):
There are classes $C_1, C_2 \subset G$ with $C_1 C_2 \supseteq G \setminus \{1\}$

Ore's Conjecture 1951: Every element of a FSG is a commutator.

Liebeck-O'Brien-Sh-Tiep 2010: Ore's Conjecture holds.

Thompson's Conjecture: Every FSG G has a conjugacy class C such that $C^2 = G$. This implies Ore's Conjecture:
$C^2 = G \Rightarrow 1 \in C^2 \Rightarrow C = C^{-1} \Rightarrow C^{-1}C = G$ so each $g \in G$ is $x^{-1}x^y = [x, y]$ for some $x \in C$.

WIDE OPEN for classical groups over small fields.
Larsen-Sh-Tiep (Annals 2011, large G)
Guralnick-Malle (JAMS 2012, all G):
There are classes $C_1, C_2 \subset G$ with $C_1 C_2 \supseteq G \setminus \{1\}$
Probabilistic approximations to Thompson's Conjecture:

Theorem (Sh 2008, 2016)

Let G be a FSG. For random $x \in G$ we have $|(x^G)^2| = (1 - o(1))|G|$. Moreover, for any $\epsilon > 0$ there is $r(\epsilon)$ such that, if $r \geq r(\epsilon)$ and G is classical group of rank r over the field with q elements, then there exists a conjugacy class C of G such that $|C^2| \geq (1 - q^{-(2-\epsilon)r})|G|$.

Proof ideas

For $x, y, g \in G$ define $p_{x,y}(g) =$ probability that g is a product of a random conjugate of x with a random conjugate of y.

$p_{x,y}$ is a distribution on G. Study $||p_{x,y}||_2^2 := \sum_{g \in G} p_{x,y}(g)^2$.

Proof ideas

For $x, y, g \in G$ define $p_{x,y}(g) =$ probability that g is a product of a random conjugate of x with a random conjugate of y.
$p_{x,y}$ is a distribution on G. Study $||p_{x,y}||_2^2 := \sum_{g \in G} p_{x,y}(g)^2$.

Theorem (Sh 2016)

Let G be a finite simple group. Choose uniformly $x, y \in G$ possibly dependent (e.g. we may have $x = y$). Then, with probability $1 - o(1)$, we have $||p_{x,y}||_2^2 = |G|^{-1}(1 + o(1))$, where the $o(1)$ is explicit.

For most x, y $p_{x,y}$ is almost uniform so $|x^G y^G| = (1 - o(1))|G|$.

Proof ideas

For $x, y, g \in G$ define $p_{x,y}(g) =$ probability that g is a product of a random conjugate of x with a random conjugate of y.
$p_{x,y}$ is a distribution on G. Study $||p_{x,y}||_2^2 := \sum_{g \in G} p_{x,y}(g)^2$.

Theorem (Sh 2016)

Let G be a finite simple group. Choose uniformly $x, y \in G$ possibly dependent (e.g. we may have $x = y$). Then, with probability $1 - o(1)$, we have $||p_{x,y}||_2^2 = |G|^{-1}(1 + o(1))$, where the $o(1)$ is explicit.

For most x, y $p_{x,y}$ is almost uniform so $|x^G y^G| = (1 - o(1))|G|$.
The character connection:

$$||p_{x,y}||_2^2 = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2.$$

Bounding character values and using the Witten zeta function $\zeta_3^G(s) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s}$ and its abscissa of convergence we prove the theorem.

Complexity and Gowers-Viola conjecutres

G a finite group, $t \geq 2$, $a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t) \in G^t$.
Their interleaved product is defined by
$a \bullet b = a_1 b_1 a_2 b_2 \cdots a_t b_t \in G$.

Complexity and Gowers-Viola conjecutres

G a finite group, $t \geq 2$, $a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t) \in G^t$.
Their interleaved product is defined by
$a \bullet b = a_1 b_1 a_2 b_2 \cdots a_t b_t \in G$.

1984 Even-Selman-Yacobi: Alice receives $a \in G^t$, Bob receives $b \in G^t$. Suppose $a \bullet b \in \{g, h\}$ for given $g, h \in G$. Alice and Bob have to decide whether $a \bullet b = g$ or $a \bullet b = h$. What is the communication complexity of this problem?
Trivial upper bound: $O(t \log |G|)$ (Alice sends a to Bob).
Various partial results over the years

Complexity and Gowers-Viola conjecutres

G a finite group, $t \geq 2$, $a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t) \in G^t$. Their interleaved product is defined by
$a \bullet b = a_1 b_1 a_2 b_2 \cdots a_t b_t \in G$.

1984 Even-Selman-Yacobi: Alice receives $a \in G^t$, Bob receives $b \in G^t$. Suppose $a \bullet b \in \{g, h\}$ for given $g, h \in G$. Alice and Bob have to decide whether $a \bullet b = g$ or $a \bullet b = h$. What is the communication complexity of this problem?
Trivial upper bound: $O(t \log |G|)$ (Alice sends a to Bob).
Various partial results over the years

Theorem (Gowers-Viola 2015)

The above communication complexity is at least $\Omega(t \log |G|)$ for $G = \mathrm{SL}_2(q)$.

Namely, complexity $\geq ct \log |G|$ for some $c > 0$.

This is deduced from: Let $G = \mathrm{SL}_2(q)$. Let $P : G^t \times G^t \to \{0, 1\}$ be a (randomized public-coin) c-bit communication protocol. For $g \in G$ $p_g :=$ the probability that $P(a, b) = 1$ assuming $a \bullet b = g$. Then for $g, h \in G$ we have $|p_g - p_h| \le 2^c |G|^{-\Omega(t)}$.

Long tricky proof, using trace method for SL_2, Lang-Weil etc

This is deduced from: Let $G = \mathrm{SL}_2(q)$. Let $P : G^t \times G^t \to \{0,1\}$ be a (randomized public-coin) c-bit communication protocol. For $g \in G$ $p_g :=$ the probability that $P(a,b) = 1$ assuming $a \bullet b = g$. Then for $g, h \in G$ we have $|p_g - p_h| \le 2^c |G|^{-\Omega(t)}$.

Long tricky proof, using trace method for SL_2, Lang-Weil etc

Conjecture (Gowers-Viola 2015)

Let G be any FSG.

(i) With the above notation $|p_g - p_h| \le 2^c (\log |G|)^{-\Omega(t)}$.

(ii) The above communication complexity is $\ge \Omega(t \log\log |G|)$.

This is deduced from: Let $G = \mathrm{SL}_2(q)$. Let $P : G^t \times G^t \to \{0,1\}$ be a (randomized public-coin) c-bit communication protocol. For $g \in G$ $p_g :=$ the probability that $P(a,b) = 1$ assuming $a \bullet b = g$. Then for $g, h \in G$ we have $|p_g - p_h| \leq 2^c |G|^{-\Omega(t)}$.

Long tricky proof, using trace method for SL_2, Lang-Weil etc

Conjecture (Gowers-Viola 2015)

Let G be any FSG.
(i) With the above notation $|p_g - p_h| \leq 2^c (\log |G|)^{-\Omega(t)}$.
(ii) The above communication complexity is $\geq \Omega(t \log\log |G|)$.

Theorem

(i) Both conjectures hold.
(ii) Any FSG G of Lie type of bounded rank behaves like $\mathrm{SL}_2(q)$, namely, $|p_g - p_h| \leq 2^c |G|^{-\Omega(t)}$, and the communication complexity is $\geq \Omega(t \log |G|)$.

These bounds are tight.

Stages of proofs:

1. A reduction by Gowers and Viola to a certain mixing phenomenon:
Recall: $p_{x,y}(g)$ = probability that g is a product of a random conjugate of x with a random conjugate of y.

It suffices to show that, fixing any $a \in G$, and choosing $x \in G$ uniformly, $||p_{x,x^{-1}a}||_2$ is small with high probability.

In bounded rank we have to show that, for some $c > 0$, the probability that $||p_{x,x^{-1}a}||_2^2 \leq |G|^{-1}(1 + |G|^{-c})$ is $\geq 1 - |G|^{-c}$.

Stages of proofs:

1. A reduction by Gowers and Viola to a certain mixing phenomenon:
Recall: $p_{x,y}(g) =$ probability that g is a product of a random conjugate of x with a random conjugate of y.

It suffices to show that, fixing any $a \in G$, and choosing $x \in G$ uniformly, $||p_{x,x^{-1}a}||_2$ is small with high probability.

In bounded rank we have to show that, for some $c > 0$, the probability that $||p_{x,x^{-1}a}||_2^2 \leq |G|^{-1}(1 + |G|^{-c})$ is $\geq 1 - |G|^{-c}$.

2. A proof of this mixing phenomenon using our previous Theorem, which was meant to help proving Thompson's Conjecture, but instead helped proving Gowers-Viola's Conjectures.

Quasi-Random Groups

G a finite group, k the minimal dimension of a non-trivial irreducible character of G.

Gowers 2008: G is quasi-random if k is large.

If $A, B, C \subseteq G$ with $|A|, |B|, |C| > |G|k^{-1/3}$ then $ABC = G$.

G a finite group, k the minimal dimension of a non-trivial irreducible character of G.
Gowers 2008: G is quasi-random if k is large.
If $A, B, C \subseteq G$ with $|A|, |B|, |C| > |G|k^{-1/3}$ then $ABC = G$.
This is known as Gowers' trick, deduced by Nikolov-Pyber 2011, and widely used by them and others since then.
Example: $G = \mathrm{SL}_2(q)$ of size $\sim q^3$. $k \sim q$.
Hence $|A|, |B|, |C| > cq^{8/3}$ implies $ABC = G$.

G a finite group, k the minimal dimension of a non-trivial irreducible character of G.
Gowers 2008: G is quasi-random if k is large.
If $A, B, C \subseteq G$ with $|A|, |B|, |C| > |G|k^{-1/3}$ then $ABC = G$.
This is known as Gowers' trick, deduced by Nikolov-Pyber 2011, and widely used by them and others since then.
Example: $G = \mathrm{SL}_2(q)$ of size $\sim q^3$. $k \sim q$.
Hence $|A|, |B|, |C| > cq^{8/3}$ implies $ABC = G$.
However, we may have $AB \neq G$ even if $|A| = \alpha|G|, |B| = \beta|G|$ for fixed $\alpha, \beta > 0$ and $|G| \gg 0$.

G a finite group, k the minimal dimension of a non-trivial irreducible character of G.
Gowers 2008: G is quasi-random if k is large.
If $A, B, C \subseteq G$ with $|A|, |B|, |C| > |G|k^{-1/3}$ then $ABC = G$.
This is known as Gowers' trick, deduced by Nikolov-Pyber 2011, and widely used by them and others since then.
Example: $G = \mathrm{SL}_2(q)$ of size $\sim q^3$. $k \sim q$.
Hence $|A|, |B|, |C| > cq^{8/3}$ implies $ABC = G$.
However, we may have $AB \neq G$ even if $|A| = \alpha|G|, |B| = \beta|G|$ for fixed $\alpha, \beta > 0$ and $|G| \gg 0$.
Question: When can we conclude that $A \bullet B = G$ for $A, B \subseteq G^t$ where $t \geq 2$?
Gowers-Viola 2015: If $t \geq 2$, $G = \mathrm{SL}_2(q)$, A, B have positive proportions in G^t and $|G| \gg 0$, then $A \bullet B = G$ almost uniformly in ℓ_∞.
Extension to all finite simple groups:

Uniformity of interleaved products

Theorem

Let G be a FSG and $t \geq 2$. Let $A, B \subseteq G^t$ with $|A|/|G|^t = \alpha > 0$ and $|B|/|G|^t = \beta > 0$. Choose $a \in A$ and $b \in B$ uniformly. Then for each $g \in G$, $Prob(a \bullet b = g) = (1 + o(1))|G|^{-1}$.
In particular, if G is sufficiently large (given α and β), then $A \bullet B = G$.

Thus $a \bullet b$ (for $a \in A$ and $b \in B$) is almost uniformly distributed in the ℓ_∞-norm.

Uniformity of interleaved products

Theorem

Let G be a FSG and $t \geq 2$. Let $A, B \subseteq G^t$ with $|A|/|G|^t = \alpha > 0$ and $|B|/|G|^t = \beta > 0$. Choose $a \in A$ and $b \in B$ uniformly. Then for each $g \in G$, $Prob(a \bullet b = g) = (1 + o(1))|G|^{-1}$.
In particular, if G is sufficiently large (given α and β), then $A \bullet B = G$.

Thus $a \bullet b$ (for $a \in A$ and $b \in B$) is almost uniformly distributed in the ℓ_∞-norm.

Quantitative bounds:

For $G = A_n$, $|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1} n^{-ct} |G|^{-1}$.

For G of Lie type of rank r over a field with q elements $|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1} q^{-crt} |G|^{-1}$.

Theorem

Let G be a FSG and $t \geq 2$. Let $A, B \subseteq G^t$ with $|A|/|G|^t = \alpha > 0$ and $|B|/|G|^t = \beta > 0$. Choose $a \in A$ and $b \in B$ uniformly. Then for each $g \in G$, $Prob(a \bullet b = g) = (1 + o(1))|G|^{-1}$.
In particular, if G is sufficiently large (given α and β), then $A \bullet B = G$.

Thus $a \bullet b$ (for $a \in A$ and $b \in B$) is almost uniformly distributed in the ℓ_∞-norm.

Quantitative bounds:

For $G = A_n$, $|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1} n^{-ct} |G|^{-1}$.

For G of Lie type of rank r over a field with q elements $|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1} q^{-crt} |G|^{-1}$.

Moreover, it follows from these bounds that if G has bounded rank, then there is $\epsilon > 0$ such that $|A|, |B| \geq |G|^{t-\epsilon}$ already implies that $A \bullet B = G$ almost uniformly in ℓ_∞.

Summary

We discussed:

Summary

We discussed:

1. Generation miracles – so easy to generate FSG
Even their maximal subgroups require few generators
Second maximal subgroups: open, reduction to $PSL_2(q)$

Summary

We discussed:

1. Generation miracles – so easy to generate FSG
Even their maximal subgroups require few generators
Second maximal subgroups: open, reduction to $PSL_2(q)$

2. Growth miracles (from $SL_2(p)$ to all FSG of bounded rank)
Fastest normal growth (for all FSG)

Summary

We discussed:

1. Generation miracles – so easy to generate FSG
Even their maximal subgroups require few generators
Second maximal subgroups: open, reduction to $PSL_2(q)$

2. Growth miracles (from $SL_2(p)$ to all FSG of bounded rank)
Fastest normal growth (for all FSG)

3. Commutator miracles (Ore's Conjecture)

Summary

We discussed:

1. Generation miracles – so easy to generate FSG
Even their maximal subgroups require few generators
Second maximal subgroups: open, reduction to $PSL_2(q)$

2. Growth miracles (from $SL_2(p)$ to all FSG of bounded rank)
Fastest normal growth (for all FSG)

3. Commutator miracles (Ore's Conjecture)

4. Complexity miracles (from $SL_2(q)$ to all FSG of bounded rank)
Potential cryptography applications
Fast mixing miracles (in all FSG)

Summary

We discussed:

1. Generation miracles – so easy to generate FSG
Even their maximal subgroups require few generators
Second maximal subgroups: open, reduction to $PSL_2(q)$

2. Growth miracles (from $SL_2(p)$ to all FSG of bounded rank)
Fastest normal growth (for all FSG)

3. Commutator miracles (Ore's Conjecture)

4. Complexity miracles (from $SL_2(q)$ to all FSG of bounded rank)
Potential cryptography applications
Fast mixing miracles (in all FSG)

Leitmotiv: What's true for $SL_2(q)$ is true for all finite simple groups (sometimes of bounded rank)

Most importantly

Happy Birthday Professor Fischer!