Simple groups, fixed point ratios and applications II

Hong Yi Huang

University of Bristol

8 April 2021

Based on the survey article by Tim Burness[1]

[1] T.C. Burness. *Simple groups, fixed point ratios and applications*. Local representation theory and simple groups, 267–322, EMS Ser. Lect. Math., Eur. Math. Soc., Zürich, 2018.

Overview

This lecture is divided into three parts:

- Introduction to simple groups and fixed point ratios;
- Generation of simple groups;
- Base sizes and Saxl graphs for almost simple groups.

Last time

- Classification of finite simple groups;
- Maximal subgroups of almost simple groups;
- Fixed point ratios.

Problem.

- Classify almost simple primitive groups with soluble stabiliser.
- Classify almost simple primitive groups with stabiliser a p-group.

CFSG

Theorem (CFSG).

Let G be a non-abelian finite simple group. Then G is isomorphic to one of the following groups:

- A_n with $n \geq 5$;
- classical simple groups:
  - linear: $\mathrm{L}_n(q)$ for $n \geq 3$ or $q \geq 4$;
  - symplectic: $\mathrm{PSp}_{2n}(q)$ for $n \geq 2$, except $\mathrm{PSp}_4(2)$;
  - unitary: $\mathrm{U}_n(q)$ for $n \geq 3$, except $\mathrm{U}_3(2)$;
  - orthogonal: $\mathrm{P\Omega}_{2n+1}(q)$ for $n \geq 3$ and q odd, or $\mathrm{P\Omega}^{\pm}_{2n}(q)$ for $n \geq 4$;
- exceptional simple groups of Lie type;
- 26 sporadic groups.

We refer the reader to Proposition 2.9.1 in Kleidman-Liebeck or (1.2) in Wilson for the isomorphisms of finite simple groups.

Alternating groups

By O'Nan-Scott, a maximal subgroup of an almost simple group with socle A_n is in one of the classes below.

Class	Descriptions	Structure in S_n	Conditions
$\mathscr{A}_1$	Intransitive	$S_m \times S_k$	$m+k=n$, $m \neq k$
$\mathscr{A}_2$	Imprimitive	$S_a \wr S_b$	$n=ab$, $a,b \geq 2$
$\mathscr{A}_3$	Affine	$\mathrm{AGL}_d(p)$	$n=p^d$, p prime
$\mathscr{A}_4$	Product action	$S_a \wr S_b$	$n=a^b$, $a \geq 5$, $b \geq 2$
$\mathscr{A}_5$	Diagonal	$T^k.(\mathrm{Out}(T) \times S_k)$	$n=\lvert T\rvert^{k-1}$, $k \geq 2$, T non-abelian simple
$\mathscr{S}$	Almost simple	S	S is primitive on $[n]$

Classical groups

By Aschbacher, a maximal subgroup of an almost simple classical group is in one of the classes below.

Class	Descriptions
$\mathscr{C}_1$	Stabiliser of subspaces, or pairs of subspaces, of V
$\mathscr{C}_2$	Stabilisers of decompositions $V = \bigoplus_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathscr{C}_3$	Stabilisers of prime degree extension fields of $\mathbb{F}_q$
$\mathscr{C}_4$	Stabiliser of decompositions $V = V_1 \otimes V_2$
$\mathscr{C}_5$	Stabilisers of prime index subfields of $\mathbb{F}_q$
$\mathscr{C}_6$	Normalisers of symplectic-type r-groups, $r \neq p$
$\mathscr{C}_7$	Stabilisers of decompositions $V = \bigotimes_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathscr{C}_8$	Stabilisers of nondegenerate forms on V
$\mathscr{S}$	Almost simple absolutely irreducible subgroups

Today

We will introduce the generation problem of simple groups and some related results, which includes

- The 2-generation property of simple groups;
- Random generations of simple groups;
- Spreads and uniform spreads;
- Generating graphs;

and how fixed point ratios are applied to these problems.

Outline

1. Fixed point ratios
2. Generation of simple groups
3. Spreads
4. Generating graphs

Fixed point ratios

Let G be a permutation group on Ω. Recall that the **fixed point ratio** of $x \in G$ is

$$\mathrm{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|},$$

where $C_\Omega(x) = \{\alpha \in \Omega \mid x \in G_\alpha\}$ is the set of fixed point of x.

Fixed point ratios

Let G be a permutation group on Ω. Recall that the **fixed point ratio** of $x \in G$ is

$$\mathrm{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|},$$

where $C_\Omega(x) = \{\alpha \in \Omega \mid x \in G_\alpha\}$ is the set of fixed point of x.
In particular, if G is transitive with stabiliser H, then

$$\mathrm{fpr}(x) = \frac{|x^G \cap H|}{|x^G|}.$$

Outline

1 Fixed point ratios

2 Generation of simple groups

3 Spreads

4 Generating graphs

2-generation of simple groups

A group G is called 2-**generated** if $G = \langle x, y \rangle$ for some $x, y \in G$.

2-generation of simple groups

A group G is called 2-**generated** if $G = \langle x, y \rangle$ for some $x, y \in G$.

Theorem.

Every finite simple group is 2-generated.

2-generation of simple groups

A group G is called 2-**generated** if $G = \langle x, y \rangle$ for some $x, y \in G$.

Theorem.

Every finite simple group is 2-generated.

Example.

- $A_n = \langle (123), (12 \cdots n) \rangle$ if n is odd;
- $A_n = \langle (123), (23 \cdots n) \rangle$ if n is even.

2-generation of simple groups

A group G is called 2-**generated** if $G = \langle x, y \rangle$ for some $x, y \in G$.

Theorem.

Every finite simple group is 2-generated.

Example.

- $A_n = \langle (123), (12 \cdots n) \rangle$ if n is odd;
- $A_n = \langle (123), (23 \cdots n) \rangle$ if n is even.

It follows the following problems

- How abundant are such pairs (x, y)?
- What if we restrict $|x|$ and $|y|$?
- What if we fix $x \neq 1$?

Random generation

Let G be a finite group, let $k \in \mathbb{N}^*$ and let

$$\mathbb{P}(G,k) = \frac{|\{(x_1,\ldots,x_k) \in G^k : G = \langle x_1,\ldots,x_k\rangle\}|}{|G|^k}$$

be the probability that k randomly chosen elements generate G.

Random generation

Let G be a finite group, let $k \in \mathbb{N}^*$ and let

$$\mathbb{P}(G,k) = \frac{|\{(x_1,\ldots,x_k) \in G^k : G = \langle x_1,\ldots,x_k\rangle\}|}{|G|^k}$$

be the probability that k randomly chosen elements generate G.
If $G \neq \langle x, y\rangle$, then $x, y \in H$ for some maximal subgroup H of G.

Random generation

Let G be a finite group, let $k \in \mathbb{N}^*$ and let

$$\mathbb{P}(G,k) = \frac{|\{(x_1,\dots,x_k) \in G^k : G = \langle x_1,\dots,x_k\rangle\}|}{|G|^k}$$

be the probability that k randomly chosen elements generate G.
If $G \neq \langle x, y\rangle$, then $x, y \in H$ for some maximal subgroup H of G. Thus,

$$1 - \mathbb{P}(G,2) \leq \sum_{H\in\mathcal{M}} \frac{|H|^2}{|G|^2} = \sum_{H\in\mathcal{M}} |G:H|^{-2} =: Q(G),$$

where $\mathcal{M}$ is the set of maximal subgroups of G.

Random generation

Let G be a finite group, let $k \in \mathbb{N}^*$ and let

$$\mathbb{P}(G,k) = \frac{|\{(x_1,\dots,x_k) \in G^k : G = \langle x_1,\dots,x_k\rangle\}|}{|G|^k}$$

be the probability that k randomly chosen elements generate G.
If $G \neq \langle x, y\rangle$, then $x, y \in H$ for some maximal subgroup H of G. Thus,

$$1 - \mathbb{P}(G,2) \leq \sum_{H \in \mathcal{M}} \frac{|H|^2}{|G|^2} = \sum_{H \in \mathcal{M}} |G:H|^{-2} =: Q(G),$$

where $\mathcal{M}$ is the set of maximal subgroups of G.
To prove G is 2-generated, it suffices to show that

$$Q(G) = \sum_{H \in \mathcal{M}} |G:H|^{-2} < 1.$$

Random generation

Example.

Let $G = A_5$. Then maximal subgroups of G up to conjugacy are

- Intransitive: $(S_3 \times S_2) \cap A_5$, $(S_4 \times S_1) \cap A_5$;
- Primitive: $\mathrm{AGL}_1(5) \cap A_5$.

Random generation

Example.

Let $G = A_5$. Then maximal subgroups of G up to conjugacy are

- Intransitive: $(S_3 \times S_2) \cap A_5$, $(S_4 \times S_1) \cap A_5$;
- Primitive: $\mathrm{AGL}_1(5) \cap A_5$.

Thus,

$$Q(G) = \sum_{H \in \mathcal{M}} |G : H|^{-2} = \frac{6}{60} + \frac{12}{60} + \frac{10}{60} = \frac{7}{15} < 1.$$

Random generation

Example.

Let $G = A_5$. Then maximal subgroups of G up to conjugacy are

- Intransitive: $(S_3 \times S_2) \cap A_5$, $(S_4 \times S_1) \cap A_5$;
- Primitive: $\mathrm{AGL}_1(5) \cap A_5$.

Thus,

$$Q(G) = \sum_{H \in \mathcal{M}} |G : H|^{-2} = \frac{6}{60} + \frac{12}{60} + \frac{10}{60} = \frac{7}{15} < 1.$$

Indeed, $\mathbb{P}(G, 2) = 19/30$.

Random generation

Example.

Let $G = \mathrm{L}_2(13)$. Then maximal subgroups of G up to conjugacy are

Group	Class	Type
13:6	$\mathscr{C}_1$	P_1
D_{12}	$\mathscr{C}_2$	$\mathrm{GL}_1(13) \wr S_2$
D_{14}	$\mathscr{C}_3$	$\mathrm{GL}_1(13^2)$
A_4	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

Random generation

Example.

Let $G = \mathrm{L}_2(13)$. Then maximal subgroups of G up to conjugacy are

Group	Class	Type
$13{:}6$	$\mathscr{C}_1$	P_1
D_{12}	$\mathscr{C}_2$	$\mathrm{GL}_1(13) \wr S_2$
D_{14}	$\mathscr{C}_3$	$\mathrm{GL}_1(13^2)$
A_4	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

Thus,

$$Q(G) = \sum_{H \in \mathcal{M}} |G : H|^{-2} = \frac{72}{1092} + \frac{12}{1092} + \frac{14}{1092} + \frac{12}{1092} = \frac{29}{273} < 1.$$

Random generation

Example.

Let $G = \mathrm{L}_2(13)$. Then maximal subgroups of G up to conjugacy are

Group	Class	Type
13:6	$\mathscr{C}_1$	P_1
D_{12}	$\mathscr{C}_2$	$\mathrm{GL}_1(13) \wr S_2$
D_{14}	$\mathscr{C}_3$	$\mathrm{GL}_1(13^2)$
A_4	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

Thus,

$$Q(G) = \sum_{H \in \mathcal{M}} |G:H|^{-2} = \frac{72}{1092} + \frac{12}{1092} + \frac{14}{1092} + \frac{12}{1092} = \frac{29}{273} < 1.$$

Indeed, $\mathbb{P}(G, 2) = 165/182$.

MAGMA functions

```
Q:=function(G);
m:=0;
X:=MaximalSubgroups(G);
for i in [1..#X] do
  m:=m+1/Index(G,H);
end for;
return m;
end function;
```

Magma functions

```
P:=function(G);
m:=0;
g:=#G;
for x in G do
   for y in G do
      if #sub<x|y> eq g then
         m:=m+1;
      end if;
   end for;
end for;
return m/g/g;
end function;
```

Random generation

Theorem.

Let (G_n) be any sequence of finite simple groups such that $|G_n| \to \infty$ with n. Then $\lim_{n\to\infty} Q(G_n) = 0$ and so $\lim_{n\to\infty} \mathbb{P}(G, 2) = 1$.

Random generation

Theorem.

Let (G_n) be any sequence of finite simple groups such that $|G_n| \to \infty$ with n. Then $\lim_{n\to\infty} Q(G_n) = 0$ and so $\lim_{n\to\infty} \mathbb{P}(G,2) = 1$.

Theorem.

We have $\mathbb{P}(G,2) \geq 53/90$ for every finite simple group G, with the equality if and only if $G = A_6$.

(a, b)-generation

Let G be a finite group. Then G is called (a, b)-**generated** if $G = \langle x, y \rangle$ for some $|x| = a$ and $|y| = b$.

(a, b)-generation

Let G be a finite group. Then G is called (a, b)-**generated** if $G = \langle x, y \rangle$ for some $|x| = a$ and $|y| = b$.

Example.

- S_n is $(2, n)$-generated.
- A_n is $(3, n)$-generated if n is odd, and $(3, n-1)$-generated if n is even.
- D_{2n} is both $(2, 2)$-generated and $(2, n)$-generated.
- A $(2, 2)$-generated group is isomorphic to D_{2n}.

Probabilistic methods

Let G be a finite group and $\mathbb{P}_{a,b}(G)$ be the probability of

"G is generated by randomly chosen elements of order a and b".

Then G is (a, b)-generated $\iff \mathbb{P}_{a,b}(G) > 0$.

Probabilistic methods

Let G be a finite group and $\mathbb{P}_{a,b}(G)$ be the probability of

"G is generated by randomly chosen elements of order a and b".

Then G is (a,b)-generated $\iff \mathbb{P}_{a,b}(G) > 0$.
Suppose $|x| = a$ and $|y| = b$. If $G \neq \langle x, y \rangle$ then $x, y \in H$ for some maximal subgroup H of G.

Probabilistic methods

Let G be a finite group and $\mathbb{P}_{a,b}(G)$ be the probability of

"G is generated by randomly chosen elements of order a and b".

Then G is (a, b)-generated $\iff \mathbb{P}_{a,b}(G) > 0$.
Suppose $|x| = a$ and $|y| = b$. If $G \neq \langle x, y \rangle$ then $x, y \in H$ for some maximal subgroup H of G. Thus,

$$1 - \mathbb{P}_{a,b}(G) \leq \sum_{H \in \mathcal{M}} \frac{i_a(H) i_b(H)}{i_a(G) i_b(G)},$$

where $i_m(X)$ denotes the number of elements of order m in X.

Probabilistic methods

Example.

Let $G = \mathrm{L}_2(13)$. Then maximal subgroups of G up to conjugacy are

Group	Class	Type
13:6	$\mathscr{C}_1$	P_1
D_{12}	$\mathscr{C}_2$	$\mathrm{GL}_1(13) \wr S_2$
D_{14}	$\mathscr{C}_3$	$\mathrm{GL}_1(13^2)$
A_4	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

Probabilistic methods

Example.

Let $G = \mathrm{L}_2(13)$. Then maximal subgroups of G up to conjugacy are

Group	Class	Type
13:6	$\mathscr{C}_1$	P_1
D_{12}	$\mathscr{C}_2$	$\mathrm{GL}_1(13) \wr S_2$
D_{14}	$\mathscr{C}_3$	$\mathrm{GL}_1(13^2)$
A_4	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

It follows that

$$
\begin{aligned}
1 - \mathbb{P}_{2,3}(G) &\leq \sum_{H \in \mathcal{M}} \frac{i_2(H) i_3(H)}{i_2(G) i_3(G)} \\
&= \frac{338}{16562} \times 14 + \frac{14}{16562} + 0 + \frac{24}{16562} \times 14 \\
&= 45/91 < 1.
\end{aligned}
$$

MAGMA functions

```
ii:=function(G,r);
S:=Subgroups(G:OrderEqual:=r);
m:=0;
for j in [1..#S] do
   H:=S[j]`subgroup;
   m:=m+(r-1)*Index(G,Normalizer(G,H));
end for;
return m;
end function;
```

Magma functions

```
Qi:=function(G,r,s);
X:=MaximalSubgroups(G);
m:=0;
iGr:=ii(G,r);
iGs:=ii(G,s);
for j in [1..#X] do
   H:=X[j]`subgroup;
   m:=m+Index(G,H)*(ii(H,r)*ii(H,s))/(iGr*iGs);
end for;
return m, RealField(4)!m;
end function;
```

$(2,3)$-generation of simple groups

- Miller, 1901: A_n is $(2,3)$-generated unless $n = 6, 7, 8$.

$(2,3)$-generation of simple groups

- Miller, 1901: A_n is $(2,3)$-generated unless $n = 6, 7, 8$.
- Liebeck and Shalev, 1996:
  - All but finitely many finite simple classical groups other than $\mathrm{PSp}_4(2^f)$ or $\mathrm{PSp}_4(3^f)$ are $(2,3)$-generated.
  - $\mathrm{PSp}_4(2^f)$ and $\mathrm{PSp}_4(3^f)$ are not $(2,3)$-generated.

$(2,3)$-generation of simple groups

- Miller, 1901: A_n is $(2,3)$-generated unless $n = 6, 7, 8$.
- Liebeck and Shalev, 1996:
  - All but finitely many finite simple classical groups other than $\mathrm{PSp}_4(2^f)$ or $\mathrm{PSp}_4(3^f)$ are $(2,3)$-generated.
  - $\mathrm{PSp}_4(2^f)$ and $\mathrm{PSp}_4(3^f)$ are not $(2,3)$-generated.
- Lübeck and Malle, 1999: Every simple exceptional group of Lie type is $(2,3)$-generated, except for $G_2(2)' \cong \mathrm{U}_3(3)$ and Suzuki groups ${}^2B_2(2^{2n+1})$, which is $(2,5)$-generated.

$(2,3)$-generation of simple groups

- Miller, 1901: A_n is $(2,3)$-generated unless $n = 6, 7, 8$.
- Liebeck and Shalev, 1996:
  - All but finitely many finite simple classical groups other than $\mathrm{PSp}_4(2^f)$ or $\mathrm{PSp}_4(3^f)$ are $(2,3)$-generated.
  - $\mathrm{PSp}_4(2^f)$ and $\mathrm{PSp}_4(3^f)$ are not $(2,3)$-generated.
- Lübeck and Malle, 1999: Every simple exceptional group of Lie type is $(2,3)$-generated, except for $G_2(2)' \cong \mathrm{U}_3(3)$ and Suzuki groups ${}^2B_2(2^{2n+1})$, which is $(2,5)$-generated.
- Wolder, 1989: Every sporadic simple group is $(2,3)$-generated, except for M_{11}, M_{22}, M_{23} and McL.

$(2,3)$-generation of simple groups

- Miller, 1901: A_n is $(2,3)$-generated unless $n = 6, 7, 8$.
- Liebeck and Shalev, 1996:
  - All but finitely many finite simple classical groups other than $\mathrm{PSp}_4(2^f)$ or $\mathrm{PSp}_4(3^f)$ are $(2,3)$-generated.
  - $\mathrm{PSp}_4(2^f)$ and $\mathrm{PSp}_4(3^f)$ are not $(2,3)$-generated.
- Lübeck and Malle, 1999: Every simple exceptional group of Lie type is $(2,3)$-generated, except for $G_2(2)' \cong \mathrm{U}_3(3)$ and Suzuki groups ${}^2B_2(2^{2n+1})$, which is $(2,5)$-generated.
- Wolder, 1989: Every sporadic simple group is $(2,3)$-generated, except for M_{11}, M_{22}, M_{23} and McL.

Theorem.

All sufficiently large non-abelian finite simple groups are $(2,3)$-generated, with the exception of $\mathrm{PSp}_4(2^f)$, $\mathrm{PSp}_4(3^f)$ and ${}^2B_2(2^{2n+1})$.

Classical Groups

Theorem (Liebeck and Shalev, 1996).

For finite simple classical groups G, as $|G| \to \infty$ we have

$$\mathbb{P}_{2,3}(G) \to \begin{cases} 0 & \text{if } G = \mathrm{PSp}_4(p^f) \text{ with } p = 2 \text{ or } 3 \\ \frac{1}{2} & \text{if } G = \mathrm{PSp}_4(p^f) \text{ with } p \neq 2, 3 \\ 1 & \text{otherwise.} \end{cases}$$

Theorem (Liebeck and Shalev, 2002).

If a, b are primes, not both equal to 2, then $\mathbb{P}_{a,b}(G) \to 1$ as $|G| \to \infty$, for all simple classical groups G of sufficiently large rank.

$(2, r)$-generation

Theorem (King, 2017).

Every non-abelian finite simple group is $(2, r)$-generated for some prime $r \geq 3$.

$(2, r)$-generation

Theorem (King, 2017).

Every non-abelian finite simple group is $(2, r)$-generated for some prime $r \geq 3$.

Conjecture.

Let G be a non-abelian finite simple group. Then one of the following cases occurs:

1. G is $(2, 3)$-generated;
2. G is $(2, 5)$-generated and G is one of the folloing groups:
   a. A_6, A_7, A_8;
   b. M_{11}, M_{22}, M_{23}, McL;
   c. $\mathrm{Sp}_4(2^f)$, $\mathrm{PSp}_4(3^f)$, $\mathrm{Sz}(q)$;
   d. $\mathrm{L}_2(9)$, $\mathrm{L}_3(4)$, $\mathrm{L}_4(2)$;
   e. $\mathrm{U}_3(5)$, $\mathrm{U}_4(2)$, $\mathrm{U}_4(3)$, $\mathrm{U}_5(2)$;
   f. $\mathrm{P}\Omega_8^+(2)$, $\mathrm{P}\Omega_8^+(3)$;
3. $G = \mathrm{U}_3(3)$ and G is $(2, 7)$-generated.

Outline

1. Fixed point ratios
2. Generation of simple groups
3. Spreads
4. Generating graphs

Spreads

Let G be a finite group.

Definition (Spreads).

G has **spread** k if for any $x_1, \ldots, x_k \in G \setminus \{1\}$, there exists $y \in G$ such that $\langle x_i, y \rangle = G$ for all i.

Spreads

Let G be a finite group.

Definition (Spreads).

G has **spread** k if for any $x_1, \ldots, x_k \in G \setminus \{1\}$, there exists $y \in G$ such that $\langle x_i, y \rangle = G$ for all i.
Let $s(G) \geq 0$ be the **exact spread** of G.

Spreads

Let G be a finite group.

Definition (Spreads).

G has **spread** k if for any $x_1, \dots, x_k \in G \setminus \{1\}$, there exists $y \in G$ such that $\langle x_i, y \rangle = G$ for all i.
Let $s(G) \geq 0$ be the **exact spread** of G.

Definition (Uniform spreads).

G has **uniform spread** k if there exists a conjugacy class C of G such that for any $x_1, \dots, x_k \in G \setminus \{1\}$, there exists $y \in C$ such that $\langle x_i, y \rangle = G$ for all i.

Spreads

Let G be a finite group.

Definition (Spreads).

G has **spread** k if for any $x_1, \dots, x_k \in G \setminus \{1\}$, there exists $y \in G$ such that $\langle x_i, y \rangle = G$ for all i.
Let $s(G) \geq 0$ be the **exact spread** of G.

Definition (Uniform spreads).

G has **uniform spread** k if there exists a conjugacy class C of G such that for any $x_1, \dots, x_k \in G \setminus \{1\}$, there exists $y \in C$ such that $\langle x_i, y \rangle = G$ for all i.
Let $u(G) \geq 0$ be the **exact uniform spread** of G.

Spreads

Let G be a finite group.

Definition (Spreads).

G has **spread** k if for any $x_1, \ldots, x_k \in G \setminus \{1\}$, there exists $y \in G$ such that $\langle x_i, y \rangle = G$ for all i.
Let $s(G) \geq 0$ be the **exact spread** of G.

Definition (Uniform spreads).

G has **uniform spread** k if there exists a conjugacy class C of G such that for any $x_1, \ldots, x_k \in G \setminus \{1\}$, there exists $y \in C$ such that $\langle x_i, y \rangle = G$ for all i.
Let $u(G) \geq 0$ be the **exact uniform spread** of G.

- $u(G) \leq s(G)$.
- $s(G) = \infty \iff u(G) = \infty \iff G$ is cyclic.

Spreads

Let G be a finite group.

Definition (Spreads).

G has **spread** k if for any $x_1, \dots, x_k \in G \setminus \{1\}$, there exists $y \in G$ such that $\langle x_i, y \rangle = G$ for all i.
Let $s(G) \geq 0$ be the **exact spread** of G.

Definition (Uniform spreads).

G has **uniform spread** k if there exists a conjugacy class C of G such that for any $x_1, \dots, x_k \in G \setminus \{1\}$, there exists $y \in C$ such that $\langle x_i, y \rangle = G$ for all i.
Let $u(G) \geq 0$ be the **exact uniform spread** of G.

- $u(G) \leq s(G)$.
- $s(G) = \infty \iff u(G) = \infty \iff G$ is cyclic.
- $u(S_6) = 0$ and $s(S_6) = 2$.
- $u(A_5) = s(A_5) = 2$.

Spreads

G is $\frac{3}{2}$-**generated** $\iff s(G) \geq 0 \implies G/N$ cyclic for any $1 \neq N \lhd G$.

Example.

If G is abelian, then

- $s(G) \geq 0 \iff G$ is cyclic or $G \cong \mathbb{Z}_p^2$;
- $u(G) \geq 0 \iff G$ is cyclic.

Spreads

G is $\frac{3}{2}$-**generated** $\iff s(G) \geq 0 \implies G/N$ cyclic for any $1 \neq N \lhd G$.

Example.

If G is abelian, then

- $s(G) \geq 0 \iff G$ is cyclic or $G \cong \mathbb{Z}_p^2$;
- $u(G) \geq 0 \iff G$ is cyclic.

We have also

- $s(S_3) = 3$, $u(S_3) = 2$;
- $s(A_4) = 4$, $u(A_4) = 3$;
- $s(D_4) = 2$, $u(D_4) = 0$;
- $s(D_{2p}) = p$, $u(D_{2p}) = p - 1$, where p is an odd prime;
- $s(S_4) = u(S_4) = 0$;
- $s(D_{2n}) = u(D_{2n}) = 0$ if n composite.

Probabilistic methods

Theorem (Breuer, Guralnick & Kantor, 2008).

G simple $\implies u(G) \geq 2$.

Probabilistic methods

Theorem (Breuer, Guralnick & Kantor, 2008).

G simple $\implies u(G) \geq 2$.

Let G be a finite group. For $x, y \in G$, let

$$\mathbb{P}(x,y) = \frac{|\{z \in y^G : G = \langle x, z\rangle\}|}{|y^G|}$$

be the probability that a randomly chosen $z \in y^G$ generates G with x. Set

$$Q(x,y) = 1 - \mathbb{P}(x,y).$$

Probabilistic methods

Lemma.

Suppose there exists an element $y \in G$ and $k \in \mathbb{N}^*$ such that $Q(x,y) < 1/k$ for all $1 \neq x \in G$. Then $u(G) \geq k$.

Probabilistic methods

Lemma.

Suppose there exists an element $y \in G$ and $k \in \mathbb{N}^*$ such that $Q(x, y) < 1/k$ for all $1 \neq x \in G$. Then $u(G) \geq k$.

Proof.

Let $x_1, \ldots, x_k \in G \setminus \{1\}$ and let E denote the event $E_1 \cap \cdots \cap E_k$, where E_i is the event that $G = \langle x_i, z \rangle$ for a randonly chosen conjugate $z \in y^G$.

Probabilistic methods

Lemma.

Suppose there exists an element $y \in G$ and $k \in \mathbb{N}^*$ such that $Q(x, y) < 1/k$ for all $1 \neq x \in G$. Then $u(G) \geq k$.

Proof.

Let $x_1, \ldots, x_k \in G \setminus \{1\}$ and let E denote the event $E_1 \cap \cdots \cap E_k$, where E_i is the event that $G = \langle x_i, z \rangle$ for a randonly chosen conjugate $z \in y^G$. We need to show that $\mathbb{P}(E) > 0$. Indeed,

$$\begin{aligned}\mathbb{P}(E) = 1 - \mathbb{P}(\bar{E}) &= 1 - \mathbb{P}(\bar{E}_1 \cup \cdots \cup \bar{E}_k) \\ &\geq 1 - \sum_{i=1}^{k} \mathbb{P}(\bar{E}_i) = 1 - \sum_{i=1}^{k} Q(x_i, y) \\ &> 1 - k \cdot \frac{1}{k} = 0.\end{aligned}$$

This completes the proof. $\square$

Probabilistic methods

Let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y.

Corollary.

Suppose there is an element $y \in G$ and $k \in \mathbb{N}^*$ such that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) < \frac{1}{k}$$

for all elements $x \in G$ of prime order. Then $u(G) \geq k$.

Probabilistic methods

Let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y.

Corollary.

Suppose there is an element $y \in G$ and $k \in \mathbb{N}^*$ such that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) < \frac{1}{k}$$

for all elements $x \in G$ of prime order. Then $u(G) \geq k$.

Proof.

Fix $1 \neq x \in G$ and let $z \in y^G$. Then $G \neq \langle x, z \rangle \iff \langle x', y \rangle \leq H$ for some $x' \in x^G$ and $H \in \mathcal{M}(y)$.

Probabilistic methods

Let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y.

Corollary.

Suppose there is an element $y \in G$ and $k \in \mathbb{N}^*$ such that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) < \frac{1}{k}$$

for all elements $x \in G$ of prime order. Then $u(G) \geq k$.

Proof.

Fix $1 \neq x \in G$ and let $z \in y^G$. Then $G \neq \langle x, z \rangle \iff \langle x', y \rangle \leq H$ for some $x' \in x^G$ and $H \in \mathcal{M}(y)$. So

$$Q(x, y) \leq \sum_{H \in \mathcal{M}(y)} \frac{|x^G \cap H|}{|x^G|} = \sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H). \qquad \square$$

Probabilistic methods

Example.

Let $G = A_{2m}$ with $m \geq 4$ and $k = m - (2, m-1)$. Set

$$y = (1, \dots, k)(k+1, \dots, n) \in G.$$

Probabilistic methods

Example.

Let $G = A_{2m}$ with $m \geq 4$ and $k = m - (2, m-1)$. Set

$$y = (1, \ldots, k)(k+1, \ldots, n) \in G.$$

Observe that

- $(k, 2m-k) = 1 \implies$ if $H \in \mathcal{M}(y)$ is transitive, then H is primitive;

Probabilistic methods

Example.

Let $G = A_{2m}$ with $m \geq 4$ and $k = m - (2, m-1)$. Set

$$y = (1, \ldots, k)(k+1, \ldots, n) \in G.$$

Observe that

- $(k, 2m-k) = 1 \implies$ if $H \in \mathcal{M}(y)$ is transitive, then H is primitive;
- y^{2m-k} is a k-cycle with $1 < k < 2m/2 \implies H \in \mathcal{M}(y)$ cannot be primitive (Marggraf 1892);

Probabilistic methods

Example.

Let $G = A_{2m}$ with $m \geq 4$ and $k = m - (2, m-1)$. Set

$$y = (1, \dots, k)(k+1, \dots, n) \in G.$$

Observe that

- $(k, 2m-k) = 1 \implies$ if $H \in \mathcal{M}(y)$ is transitive, then H is primitive;
- y^{2m-k} is a k-cycle with $1 < k < 2m/2 \implies H \in \mathcal{M}(y)$ cannot be primitive (Marggraf 1892);
- $H \in \mathcal{M}(y)$ is intransitive $\implies H = (S_k \times S_{2m-k}) \cap G$;

Probabilistic methods

Example.

Let $G = A_{2m}$ with $m \geq 4$ and $k = m - (2, m-1)$. Set

$$y = (1, \ldots, k)(k+1, \ldots, n) \in G.$$

Observe that

- $(k, 2m-k) = 1 \implies$ if $H \in \mathcal{M}(y)$ is transitive, then H is primitive;
- y^{2m-k} is a k-cycle with $1 < k < 2m/2 \implies H \in \mathcal{M}(y)$ cannot be primitive (Marggraf 1892);
- $H \in \mathcal{M}(y)$ is intransitive $\implies H = (S_k \times S_{2m-k}) \cap G$;
- $\mathrm{fpr}(x, G/H) < 1/3 \implies u(G) \geq 3$.

Outline

1. Fixed point ratios

2. Generation of simple groups

3. Spreads

4. Generating graphs

Generating graphs

Let G be a finite group.
Generating graph $\Gamma(G)$: vertex set $G \setminus \{1\}$, $x \sim y$ if $\langle x, y \rangle = G$.

Generating graphs

Let G be a finite group.
Generating graph $\Gamma(G)$: vertex set $G \setminus \{1\}$, $x \sim y$ if $\langle x, y \rangle = G$.

Example.

$\langle x, y \rangle \neq S_3$ iff $x, y \in \{(123), (132)\}$. So $\Gamma(S_3) \cong K_5 - K_2$.

Generating graphs

Let G be a finite group.
Generating graph $\Gamma(G)$: vertex set $G \setminus \{1\}$, $x \sim y$ if $\langle x, y\rangle = G$.

Example.

$\langle x, y\rangle \neq S_3$ iff $x, y \in \{(123), (132)\}$. So $\Gamma(S_3) \cong K_5 - K_2$.

- G is 2-generated $\iff$ $\Gamma(G)$ is non-empty;
- G is $\frac{3}{2}$-generated $\iff$ $\Gamma(G)$ has no isolated vertex;
- $\Gamma(G)$ is complete $\iff$ $G \cong \mathbb{Z}_p$ or $\mathbb{Z}_2^2$;

Generating graphs

Let G be a finite group.
Generating graph $\Gamma(G)$: vertex set $G \setminus \{1\}$, $x \sim y$ if $\langle x, y \rangle = G$.

Example.

$\langle x, y \rangle \neq S_3$ iff $x, y \in \{(123), (132)\}$. So $\Gamma(S_3) \cong K_5 - K_2$.

- G is 2-generated $\iff$ $\Gamma(G)$ is non-empty;
- G is $\frac{3}{2}$-generated $\iff$ $\Gamma(G)$ has no isolated vertex;
- $\Gamma(G)$ is complete $\iff$ $G \cong \mathbb{Z}_p$ or $\mathbb{Z}_2^2$;
- $s(G) \geq 2 \implies \Gamma(G)$ is connected of diameter 2;

Generating graphs

Let G be a finite group.
Generating graph $\Gamma(G)$: vertex set $G \setminus \{1\}$, $x \sim y$ if $\langle x, y \rangle = G$.

Example.

$\langle x, y \rangle \neq S_3$ iff $x, y \in \{(123), (132)\}$. So $\Gamma(S_3) \cong K_5 - K_2$.

- G is 2-generated $\iff$ $\Gamma(G)$ is non-empty;
- G is $\frac{3}{2}$-generated $\iff$ $\Gamma(G)$ has no isolated vertex;
- $\Gamma(G)$ is complete $\iff$ $G \cong \mathbb{Z}_p$ or $\mathbb{Z}_2^2$;
- $s(G) \geq 2 \implies \Gamma(G)$ is connected of diameter 2;

If G is non-abelian simple then

- $\Gamma(G)$ has no isolated vertex;
- $\Gamma(G)$ is connected of diameter at most 2.

Problems

Conjecture.

Let G be a finite group with $|G| \geq 4$. Then the following are equivalent:

1. G has spread 1.
2. G has spread 2.
3. G/N is cyclic for every non-trivial normal subgroup N.
4. $\Gamma(G)$ has no isolated vertices.
5. $\Gamma(G)$ is connected.
6. $\Gamma(G)$ is connected with diameter at most 2.
7. $\Gamma(G)$ is Hamiltonian.

[2] Burness, Timothy; Guralnick, Robert; Harper, Scott; *The spread of a finite group*. Ann. of Math. (2) **193** (2021), no. 2, 619–687.

Problems

Conjecture.

Let G be a finite group with $|G| \geq 4$. Then the following are equivalent:

1. G has spread 1.
2. G has spread 2.
3. G/N is cyclic for every non-trivial normal subgroup N.
4. $\Gamma(G)$ has no isolated vertices.
5. $\Gamma(G)$ is connected.
6. $\Gamma(G)$ is connected with diameter at most 2.
7. $\Gamma(G)$ is Hamiltonian.

$(2) \implies (6) \implies (5) \implies (4) \iff (1) \implies (3) \impliedby (7)$ is obvious.

[2]Burness, Timothy; Guralnick, Robert; Harper, Scott; *The spread of a finite group*. Ann. of Math. (2) **193** (2021), no. 2, 619–687.

Problems

Conjecture.

Let G be a finite group with $|G| \geq 4$. Then the following are equivalent:

1. G has spread 1.
2. G has spread 2.
3. G/N is cyclic for every non-trivial normal subgroup N.
4. $\Gamma(G)$ has no isolated vertices.
5. $\Gamma(G)$ is connected.
6. $\Gamma(G)$ is connected with diameter at most 2.
7. $\Gamma(G)$ is Hamiltonian.

$(2) \implies (6) \implies (5) \implies (4) \iff (1) \implies (3) \impliedby (7)$ is obvious.
Burness, Guralnick & Harper, 2021[2]: $(3) \implies (2)$.

[2] Burness, Timothy; Guralnick, Robert; Harper, Scott; *The spread of a finite group*. Ann. of Math. (2) **193** (2021), no. 2, 619–687.

Problems

Conjecture.

Let G be a finite group with $|G| \geq 4$. Then the following are equivalent:

1. G has spread 1.
2. G has spread 2.
3. G/N is cyclic for every non-trivial normal subgroup N.
4. $\Gamma(G)$ has no isolated vertices.
5. $\Gamma(G)$ is connected.
6. $\Gamma(G)$ is connected with diameter at most 2.
7. $\Gamma(G)$ is Hamiltonian.

$(2) \implies (6) \implies (5) \implies (4) \iff (1) \implies (3) \impliedby (7)$ is obvious.
Burness, Guralnick & Harper, 2021[2]: $(3) \implies (2)$.
$(3) \implies (7)$ is still open for insoluble groups.

[2] Burness, Timothy; Guralnick, Robert; Harper, Scott; *The spread of a finite group*. Ann. of Math. (2) **193** (2021), no. 2, 619–687.

Next time

In the next talk, we will introduce the bases for a permutation group, mainly in the almost simple primitive case. This includes

- Base sizes and Cameron's conjecture;
- Base sizes for almost simple primitive groups with soluble stabilisers;
- The Saxl graph of base-two permutation groups;
- Results and open problems on Saxl graphs.

We will also see how the fixed point ratio method is applied, and introduce some computational methods with MAGMA.

Thank you for your attention!