The probabilistic method in group theory

Hong Yi Huang

University of Bristol

SUSTech, 22 April 2021

Outline

1. The probabilistic method
2. Generation of simple groups
3. Bases for almost simple primitive groups
4. Saxl graphs

The probabilistic method

From Wikipedia:

The probabilistic method is a nonconstructive method, primarily used in combinatorics and pioneered by Paul Erdős, for proving the existence of a prescribed kind of mathematical object.

The probabilistic method

From Wikipedia:
The probabilistic method is a nonconstructive method, primarily used in combinatorics and pioneered by Paul Erdős, for proving the existence of a prescribed kind of mathematical object.

Theorem (Erdös, 1947).
The Ramsey number $R(r, r)$ grows at least exponentially with r.

The probabilistic method

From Wikipedia:
The probabilistic method is a nonconstructive method, primarily used in combinatorics and pioneered by Paul Erdős, for proving the existence of a prescribed kind of mathematical object.

Theorem (Erdös, 1947).

The Ramsey number $R(r, r)$ grows at least exponentially with r.

The probabilistic method describes the **existence** and the **abundance**.

Randomly chosen elements in groups

If G is a non-abelian finite group, then

$$\frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2} \leq \frac{5}{8}.$$

Randomly chosen elements in groups

If G is a non-abelian finite group, then

$$\frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2} \leq \frac{5}{8}.$$

Question.

What if we randomly choose elements satisfying some properties?

Probabilistic methods in group theory

Let G be a finite group. Let E be an event and $\mathbb{P}_E(G)$ be the probability of randomly chosen elements satisfying E. Then

$$\begin{aligned}\text{There exist elements satisfying } E &\iff \mathbb{P}_E(G) > 0\\ &\iff 1 - \mathbb{P}_E(G) < 1.\end{aligned}$$

Probabilistic methods in group theory

Let G be a finite group. Let E be an event and $\mathbb{P}_E(G)$ be the probability of randomly chosen elements satisfying E. Then

$$\begin{aligned} \text{There exist elements satisfying } E &\iff \mathbb{P}_E(G) > 0 \\ &\iff 1 - \mathbb{P}_E(G) < 1. \end{aligned}$$

Remarks:

- Sometimes it is hard to prove $\mathbb{P}_E(G) > 0$ by direct construction.
- We need to find an upper bound of $1 - \mathbb{P}_E(G)$ that is easily obtained.
- We usually have good properties if $1 - \mathbb{P}_E(G) \to 0$.

Probabilistic methods in group theory

Let G be a finite group. Let E be an event and $\mathbb{P}_E(G)$ be the probability of randomly chosen elements satisfying E. Then

$$\text{There exist elements satisfying } E \iff \mathbb{P}_E(G) > 0$$
$$\iff 1 - \mathbb{P}_E(G) < 1.$$

Remarks:

- Sometimes it is hard to prove $\mathbb{P}_E(G) > 0$ by direct construction.
- We need to find an upper bound of $1 - \mathbb{P}_E(G)$ that is easily obtained.
- We usually have good properties if $1 - \mathbb{P}_E(G) \to 0$.

Aim.

Find $\widehat{Q}_E(G) \geq 1 - \mathbb{P}_E(G)$ such that $\widehat{Q}_E(G) < 1$.

Outline

2-generation of simple groups

Let G be a group. Then G is called 2-**generated** if there exists $x, y \in G$ such that $G = \langle x, y \rangle$.

2-generation of simple groups

Let G be a group. Then G is called 2-**generated** if there exists $x, y \in G$ such that $G = \langle x, y \rangle$.

Problem.

Is every finite simple group 2-generated?

2-generation of simple groups

Let G be a group. Then G is called 2-**generated** if there exists $x, y \in G$ such that $G = \langle x, y \rangle$.

Problem.

Is every finite simple group 2-generated?

Example.

- $A_n = \langle (1,2,3), (1,2,\ldots,n) \rangle$ if n is odd.
- $A_n = \langle (1,2,3), (2,3,\ldots,n) \rangle$ if n is even.

2-generation of simple groups

Let G be a group and

$$\mathbb{P}(G) := \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}$$

be the probability of 2 randomly chosen elements in G generate G.

2-generation of simple groups

Let G be a group and

$$\mathbb{P}(G) := \frac{|\{(x, y) \in G \times G \mid \langle x, y \rangle = G\}|}{|G|^2}$$

be the probability of 2 randomly chosen elements in G generate G.

- If $\mathbb{P}(G) > 0$ then G is 2-generated.

2-generation of simple groups

Let G be a group and

$$\mathbb{P}(G) := \frac{|\{(x,y) \in G \times G \mid \langle x,y\rangle = G\}|}{|G|^2}$$

be the probability of 2 randomly chosen elements in G generate G.

- If $\mathbb{P}(G) > 0$ then G is 2-generated.
- If $G \neq \langle x,y\rangle$ then $x, y \in H$ for some maximal subgroup H of G.

2-generation of simple groups

Let G be a group and

$$\mathbb{P}(G) := \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}$$

be the probability of 2 randomly chosen elements in G generate G.

- If $\mathbb{P}(G) > 0$ then G is 2-generated.
- If $G \neq \langle x,y \rangle$ then $x,y \in H$ for some maximal subgroup H of G.

Thus, we have

$$1 - \mathbb{P}(G) \leq \sum_{H \text{ maximal}} \frac{|H|^2}{|G|^2}$$

2-generation of simple groups

Let G be a group and

$$\mathbb{P}(G) := \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}$$

be the probability of 2 randomly chosen elements in G generate G.

- If $\mathbb{P}(G) > 0$ then G is 2-generated.
- If $G \neq \langle x,y \rangle$ then $x,y \in H$ for some maximal subgroup H of G.

Thus, we have

$$\begin{aligned} 1 - \mathbb{P}(G) &\leq \sum_{H \text{ maximal}} \frac{|H|^2}{|G|^2} \\ &= \sum_{H \in \mathcal{M}} \frac{|H|^2}{|G|^2} \cdot |G : N_G(H)| \end{aligned}$$

2-generation of simple groups

Let G be a group and

$$\mathbb{P}(G) := \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}$$

be the probability of 2 randomly chosen elements in G generate G.

- If $\mathbb{P}(G) > 0$ then G is 2-generated.
- If $G \neq \langle x,y \rangle$ then $x, y \in H$ for some maximal subgroup H of G.

Thus, we have

$$\begin{aligned} 1 - \mathbb{P}(G) &\leq \sum_{H \text{ maximal}} \frac{|H|^2}{|G|^2} \\ &= \sum_{H \in \mathcal{M}} \frac{|H|^2}{|G|^2} \cdot |G : N_G(H)| \\ &= \sum_{H \in \mathcal{M}} \frac{|H|}{|G|} =: \widehat{Q}(G), \end{aligned}$$

where $\mathcal{M}$ is the set of maximal subgroups in G up to conjugacy.

2-generation of simple groups

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	$\mathscr{C}_6$	$2^{1+2}.\,\mathrm{Sp}_2(2)$

2-generation of simple groups

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,

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

2-generation of simple groups

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,

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

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

2-generation of simple groups

Theorem.

Every finite simple group is 2-generated.

2-generation of simple groups

Theorem.

Every finite simple group is 2-generated.

Problem.

Let $G = \langle x, y \rangle$.

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

Random generation of simple groups

Example.

Let $G = \mathrm{L}_2(q)$. Then maximal subgroups of G are among the following:

- P parabolic of index $q + 1$;
- $D_{q \pm 1}$;
- $\mathrm{L}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$ (subfield subgroups);
- A_4, S_4, A_5.

Random generation of simple groups

Example.

Let $G = \mathrm{L}_2(q)$. Then maximal subgroups of G are among the following:

- P parabolic of index $q+1$;
- $D_{q\pm1}$;
- $\mathrm{L}_2(q_0)$ or $\mathrm{PGL}_2(q_0)$ (subfield subgroups);
- A_4, S_4, A_5.

Note that there are at most $\log_2 \log_2 q$ subfields of $\mathbb{F}_q$. We have

$$\widehat{Q}(G) = (q+1)^{-1} + O(q^{-\frac{3}{2}} \log\log q) = O(q^{-1}).$$

Thus, $\widehat{Q}(G) \to 0$ as $q \to \infty$, and so $\mathbb{P}(G) \to 1$.

Random generation of simple groups

Theorem.

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

Random generation of simple groups

Theorem.

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

Theorem.

We have $\mathbb{P}(G) \geq 53/90$ 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}.

(a, b)-generation

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".

(a, b)-generation

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".

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

(a, b)-generation

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".

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

(a, b)-generation

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".

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

Thus,

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

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

$(2,3)$-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	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

$(2,3)$-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	$\mathscr{C}_6$	$2^{1+2}.\mathrm{Sp}_2(2)$

It follows that

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

$(2, 3)$-generation

Theorem (King, 2017).

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

$(2,3)$-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. The probabilistic method
2. Generation of simple groups
3. Bases for almost simple primitive groups
4. Saxl graphs

Bases

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$.

Definition.

A subset Δ of Ω is a **base** for G if $\cap_{\alpha \in \Delta} G_\alpha = 1$.

Bases

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$.

Definition.

A subset Δ of Ω is a **base** for G if $\cap_{\alpha \in \Delta} G_\alpha = 1$.
The **base size** of G, denoted by $b(G)$, is the minimal cardinality of a base.

Bases

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$.

Definition.

A subset Δ of Ω is a **base** for G if $\cap_{\alpha\in\Delta} G_\alpha = 1$.
The **base size** of G, denoted by $b(G)$, is the minimal cardinality of a base.

- Images of a base determine the whole group G.

Bases

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$.

Definition.

A subset Δ of Ω is a **base** for G if $\bigcap_{\alpha\in\Delta} G_\alpha = 1$.
The **base size** of G, denoted by $b(G)$, is the minimal cardinality of a base.

- Images of a base determine the whole group G.
- If G is transitive and $H = G_\alpha$, then $b(G)$ is the minimal cardinality of a subset $S \subseteq G$ such that

$$\bigcap_{x\in S} H^x = 1.$$

Bases

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$.

Definition.

A subset Δ of Ω is a **base** for G if $\cap_{\alpha \in \Delta} G_\alpha = 1$.
The **base size** of G, denoted by $b(G)$, is the minimal cardinality of a base.

- Images of a base determine the whole group G.
- If G is transitive and $H = G_\alpha$, then $b(G)$ is the minimal cardinality of a subset $S \subseteq G$ such that

$$\bigcap_{x \in S} H^x = 1.$$

- There always exists a base by noting that Ω is a base.

Bases

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega| < \infty$.

Definition.

A subset Δ of Ω is a **base** for G if $\cap_{\alpha \in \Delta} G_\alpha = 1$.
The **base size** of G, denoted by $b(G)$, is the minimal cardinality of a base.

- Images of a base determine the whole group G.
- If G is transitive and $H = G_\alpha$, then $b(G)$ is the minimal cardinality of a subset $S \subseteq G$ such that

$$\bigcap_{x \in S} H^x = 1.$$

- There always exists a base by noting that Ω is a base.
- $b(G) = 1 \iff G$ has a regular orbit on Ω.

Examples

Example.

- $G = S_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 1$.

Examples

Example.

- $G = S_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 1$.
- $G = A_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 2$.

Examples

Example.

- $G = S_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 1$.
- $G = A_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 2$.
- $G = D_{2n}$, $\Omega = \{1, \ldots, n\}$: $b(G) = 2$.

Examples

Example.

- $G = S_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 1$.
- $G = A_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 2$.
- $G = D_{2n}$, $\Omega = \{1, \ldots, n\}$: $b(G) = 2$.
- $G = \mathrm{GL}(V)$, $\Omega = V$:
  A subset of Ω is a base iff it contains a basis of V, so $b(G) = \dim V$.

Examples

Example.

- $G = S_n$, $\Omega = \{1, \dots, n\}$: $b(G) = n - 1$.
- $G = A_n$, $\Omega = \{1, \dots, n\}$: $b(G) = n - 2$.
- $G = D_{2n}$, $\Omega = \{1, \dots, n\}$: $b(G) = 2$.
- $G = \mathrm{GL}(V)$, $\Omega = V$:
  A subset of Ω is a base iff it contains a basis of V, so $b(G) = \dim V$.
- $G = \mathrm{PGL}(V)$, $d = \dim V > 1$, $\Omega = P(V)$: $b(G) = d + 1$
  Indeed, a base size set is $\{\langle v_1 \rangle, \dots, \langle v_d \rangle, \langle v_1 + \cdots + v_d \rangle\}$, where $v_1, \dots, v_d$ is a basis of V.

Non-standard groups

A group is called **almost simple** if

$$\mathrm{soc}(G) \cong T \lesssim G \lesssim \mathrm{Aut}(T)$$

for some non-abelian simple group T.

Non-standard groups

A group is called **almost simple** if

$$\mathrm{soc}(G) \cong T \lesssim G \lesssim \mathrm{Aut}(T)$$

for some non-abelian simple group T.
A permutation group is called **primitive** if G_α is maximal in G.

Non-standard groups

A group is called **almost simple** if

$$\mathrm{soc}(G) \cong T \lesssim G \lesssim \mathrm{Aut}(T)$$

for some non-abelian simple group T.
A permutation group is called **primitive** if G_α is maximal in G.
Roughly speaking, an almost simple primitive group is called **standard** if

- $\mathrm{soc}(G) = A_n$ and G_α is primitive on $\{1, \dots, n\}$, or
- G is classical with $G_\alpha \cap \mathrm{soc}(G)$ reducible.

Non-standard groups

A group is called **almost simple** if

$$\mathrm{soc}(G) \cong T \lesssim G \lesssim \mathrm{Aut}(T)$$

for some non-abelian simple group T.
A permutation group is called **primitive** if G_α is maximal in G.
Roughly speaking, an almost simple primitive group is called **standard** if

- $\mathrm{soc}(G) = A_n$ and G_α is primitive on $\{1, \ldots, n\}$, or
- G is classical with $G_\alpha \cap \mathrm{soc}(G)$ reducible.

Other almost simple primitive groups are called **non-standard**.

Cameron's conjecture

Conjecture.

Let G be a non-standard group. Then $b(G) \leq c$ for some constant c.

Cameron's conjecture

Conjecture.

Let G be a non-standard group. Then $b(G) \leq c$ for some constant c.

For a positive integer c, let

$$\mathbb{P}(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : \bigcap_{i=1}^{c} G_{\alpha_i} = 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of points in Ω is a base for G.

Cameron's conjecture

Conjecture.

Let G be a non-standard group. Then $b(G) \leq c$ for some constant c.

For a positive integer c, let

$$\mathbb{P}(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c : \bigcap_{i=1}^c G_{\alpha_i} = 1\}|}{|\Omega|^c}$$

be the probability that a random c-tuple of points in Ω is a base for G.

- $b(G) \leq c \iff \mathbb{P}(G,c) > 0$.
- A c-tuple is not a base if and only if it is fixed by some $x \in G$ of prime order.
- The probability of a random c-tuple is fixed by x is $\mathrm{fpr}(x)^c$, where

$$\mathrm{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|} = \frac{|x^G \cap G_\alpha|}{|x^G|}$$

is the **fixed point ratio** of x.

Cameron's conjecture

From above, we have

$$\begin{aligned} 1 - \mathbb{P}(G, c) &\leq \sum_{x \in \mathcal{P}} \mathrm{fpr}(x)^c \\ &= \sum_{i=1}^{m} \mathrm{fpr}(x_i)^c |x_i^G| \\ &= \sum_{i=1}^{m} \left(\frac{|x_i^G \cap G_\alpha|}{|x_i^G|} \right)^c \cdot |x_i^G| =: \widehat{Q}(G, c), \end{aligned}$$

where $\mathcal{P}$ is the set of elements of prime order in G, and $\{x_1, \ldots, x_m\}$ are representatives of $\mathcal{P}$ up to G-conjugacy.

Cameron's conjecture

From above, we have

$$\begin{aligned}
1 - \mathbb{P}(G,c) &\leq \sum_{x\in\mathcal{P}} \mathrm{fpr}(x)^c \\
&= \sum_{i=1}^{m} \mathrm{fpr}(x_i)^c |x_i^G| \\
&= \sum_{i=1}^{m} \left(\frac{|x_i^G \cap G_\alpha|}{|x_i^G|}\right)^c \cdot |x_i^G| =: \widehat{Q}(G,c),
\end{aligned}$$

where $\mathcal{P}$ is the set of elements of prime order in G, and $\{x_1, \dots, x_m\}$ are representatives of $\mathcal{P}$ up to G-conjugacy.

- $b(G) \leq c$ if $\widehat{Q}(G,c) < 1$.

Cameron's conjecture

From above, we have

$$\begin{aligned}1-\mathbb{P}(G,c) &\leq \sum_{x\in\mathcal{P}} \mathrm{fpr}(x)^c \\ &= \sum_{i=1}^{m} \mathrm{fpr}(x_i)^c |x_i^G| \\ &= \sum_{i=1}^{m} \left(\frac{|x_i^G \cap G_\alpha|}{|x_i^G|}\right)^c \cdot |x_i^G| =: \widehat{Q}(G,c),\end{aligned}$$

where $\mathcal{P}$ is the set of elements of prime order in G, and $\{x_1,\ldots,x_m\}$ are representatives of $\mathcal{P}$ up to G-conjugacy.

- $b(G) \leq c$ if $\widehat{Q}(G,c) < 1$.
- In particular, $b(G) \leq 2$ if

$$|G_\alpha|^2 \max_{1\neq x\in G_\alpha} |C_G(x)| = |G_\alpha|^2 \max_{\substack{x\in G_\alpha \\ |x| \text{ prime}}} |C_G(x)| < |G|.$$

A base-two example

Example.

Suppose $\mathrm{soc}(G) = \mathrm{L}_3^{\epsilon}(q)$ with $q = p \equiv \epsilon \pmod 3$ and $H = G_\alpha$ is of type $3^{1+2}.\mathrm{Sp}_2(3)$. Then $|H| \leq 432$ and

$$|C_G(x)| \leq \frac{|G|}{(q-1)(q^3-1)}$$

for all $x \in G$ of prime order (maximal if $\epsilon = +$ and x is unipotent with Jordan form $[J_2, J_1]$). This gives $b(G) = 2$ for all $q > 23$. When $q \leq 23$ we can also check using MAGMA that $b(G) = 2$.

Cameron's conjecture for exceptional groups

Theorem (Liebeck & Saxl, 1991).

Let G be a transitive almost simple exceptional group over $\mathbb{F}_q$. Then

$$\max_{1 \neq x \in G} \mathrm{fpr}(x) \leq \frac{4}{3q}.$$

Cameron's conjecture for exceptional groups

Theorem (Liebeck & Saxl, 1991).

Let G be a transitive almost simple exceptional group over $\mathbb{F}_q$. Then

$$\max_{1\neq x\in G} \mathrm{fpr}(x) \leq \frac{4}{3q}.$$

If $\mathrm{soc}(G)$ exceptional then $|G| < q^{249}$ and so $b(G) \leq 500$ since

$$\begin{aligned}
\widehat{Q}(G,500) &= \sum_{i=1}^{m} \mathrm{fpr}(x_i)^{500}|x_i^G| \\
&\leq \left(\frac{4}{3q}\right)^{500} \sum_{i=1}^{m} |x_i^G| \\
&< \left(\frac{4}{3q}\right)^{500} |G| \\
&< \left(\frac{4}{3q}\right)^{500} q^{249} < \frac{1}{q}.
\end{aligned}$$

Cameron's conjecture

Theorem (Burness, Liebeck & Shalev, 2009).

Let G be a non-standard group. Then $b(G) \leq 7$, with the equality iff $G = \mathrm{M}_{24}$ in its natural action.

Cameron's conjecture

Theorem (Burness, Liebeck & Shalev, 2009).

Let G be a non-standard group. Then $b(G) \leq 7$, with the equality iff $G = \mathrm{M}_{24}$ in its natural action.

Burness 2018: Determined non-standard groups G with $b(G) = 6$.

Cameron's conjecture

Theorem (Burness, Liebeck & Shalev, 2009).

Let G be a non-standard group. Then $b(G) \leq 7$, with the equality iff $G = \mathrm{M}_{24}$ in its natural action.

Burness 2018: Determined non-standard groups G with $b(G) = 6$.
Burness 2021: Determined exact base sizes when G_α is soluble.

Cameron's conjecture

Theorem (Burness, Liebeck & Shalev, 2009).

Let G be a non-standard group. Then $b(G) \leq 7$, with the equality iff $G = \mathrm{M}_{24}$ in its natural action.

Burness 2018: Determined non-standard groups G with $b(G) = 6$.
Burness 2021: Determined exact base sizes when G_α is soluble.

Problem.

Determine exact base sizes for non-standard groups. In particular, classify those with $b(G) = 2$.

Saxl's base-two project

Problem.

Determine finite primitive groups G with $b(G) = 2$.

Saxl's base-two project

Problem.

Determine finite primitive groups G with $b(G) = 2$.

- Affine: $G = V{:}H$. Then

$$b(G) = 2 \iff V \neq \bigcup_{1 \neq h \in H} C_V(h),$$

where $C_V(h) = \{v : v^h = v\}$ is the 1-eigenspace of h on V, leading

Problem.

Determine pairs (V, H), where H is a finite group, V is a faithful irreducible $\mathbb{F}_p H$-module and H has a regular orbit on V.

Saxl's base-two project

Problem.

Determine finite primitive groups G with $b(G) = 2$.

- Affine: $G = V{:}H$. Then

$$b(G) = 2 \iff V \neq \bigcup_{1 \neq h \in H} C_V(h),$$

where $C_V(h) = \{v : v^h = v\}$ is the 1-eigenspace of h on V, leading

Problem.

Determine pairs (V, H), where H is a finite group, V is a faithful irreducible $\mathbb{F}_p H$-module and H has a regular orbit on V.

- Almost simple: nearly done.

Saxl's base-two project

Problem.

Determine finite primitive groups G with $b(G) = 2$.

- Affine: $G = V{:}H$. Then

$$b(G) = 2 \iff V \neq \bigcup_{1 \neq h \in H} C_V(h),$$

where $C_V(h) = \{v : v^h = v\}$ is the 1-eigenspace of h on V, leading

Problem.

Determine pairs (V, H), where H is a finite group, V is a faithful irreducible $\mathbb{F}_p H$-module and H has a regular orbit on V.

- Almost simple: nearly done.
- Diagonal and twisted wreath: partial results **(Fawcett, 2013/21)**.

Saxl's base-two project

Problem.

Determine finite primitive groups G with $b(G) = 2$.

- Affine: $G = V{:}H$. Then

$$b(G) = 2 \iff V \neq \bigcup_{1 \neq h \in H} C_V(h),$$

where $C_V(h) = \{v : v^h = v\}$ is the 1-eigenspace of h on V, leading

Problem.

Determine pairs (V, H), where H is a finite group, V is a faithful irreducible $\mathbb{F}_p H$-module and H has a regular orbit on V.

- Almost simple: nearly done.
- Diagonal and twisted wreath: partial results **(Fawcett, 2013/21)**.
- Product type: no result.

Outline

Saxl graphs

Definition.

Let $G \leq \mathrm{Sym}(\Omega)$ be a base-two permutation group.
The **Saxl graph** $\Sigma(G)$: vertices Ω, $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

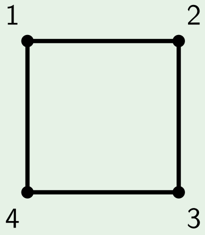
Saxl graphs

Definition.

Let $G \leq \mathrm{Sym}(\Omega)$ be a base-two permutation group.
The **Saxl graph** $\Sigma(G)$: vertices Ω, $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example.

- $G = D_8$, $\Omega = \{1, 2, 3, 4\}$: $\Sigma(G) \cong C_4$.



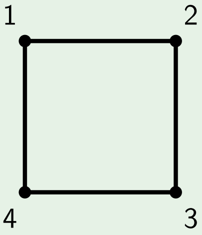
Saxl graphs

Definition.

Let $G \leq \mathrm{Sym}(\Omega)$ be a base-two permutation group.
The **Saxl graph** $\Sigma(G)$: vertices Ω, $\alpha \sim \beta \iff \{\alpha, \beta\}$ is a base.

Example.

- $G = D_8$, $\Omega = \{1, 2, 3, 4\}$: $\Sigma(G) \cong C_4$.

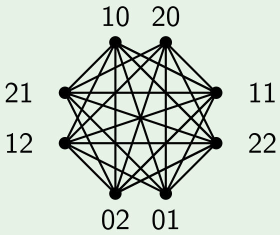


- $G = D_{10}$, $\Omega = \{1, 2, 3, 4, 5\}$: $\Sigma(G) \cong K_5$.

Some further examples

Example.

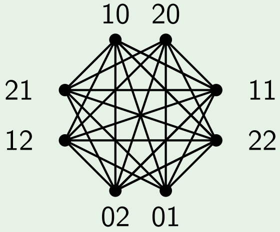
- Let $G = \mathrm{GL}_2(q)$ and $\Omega = \mathbb{F}_q^2 \setminus \{0\}$. Then $\alpha \sim \beta$ iff $\{\alpha, \beta\}$ is linearly independent. Thus, $\Sigma(G)$ is **complete multipartite** with $q+1$ parts of size $q-1$. For example, when $q = 3$ we have $\Sigma(G) \cong K_8 - 4K_2$.



Some further examples

Example.

- Let $G = \mathrm{GL}_2(q)$ and $\Omega = \mathbb{F}_q^2 \setminus \{0\}$. Then $\alpha \sim \beta$ iff $\{\alpha, \beta\}$ is linearly independent. Thus, $\Sigma(G)$ is **complete multipartite** with $q+1$ parts of size $q-1$. For example, when $q = 3$ we have $\Sigma(G) \cong K_8 - 4K_2$.



- Let $G = \mathrm{PGL}_2(q)$ and Ω be the set of distinct pairs of 1-spaces in $\mathbb{F}_q^2$. Then α and β form a base iff they share a common 1-space. Hence, $\Sigma(G) \cong J(q+1, 2)$ is a **Johnson graph**.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.
2. $\Sigma(G)$ is connected if G is primitive.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.
2. $\Sigma(G)$ is connected if G is primitive.
3. $\Sigma(G)$ is complete if and only if G is Frobenius.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.
2. $\Sigma(G)$ is connected if G is primitive.
3. $\Sigma(G)$ is complete if and only if G is Frobenius.
4. $\Sigma(G)$ is G-arc-semiregular.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.
2. $\Sigma(G)$ is connected if G is primitive.
3. $\Sigma(G)$ is complete if and only if G is Frobenius.
4. $\Sigma(G)$ is G-arc-semiregular.
5. $\Sigma(G)$ is the union of all regular orbital graphs of G.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.
2. $\Sigma(G)$ is connected if G is primitive.
3. $\Sigma(G)$ is complete if and only if G is Frobenius.
4. $\Sigma(G)$ is G-arc-semiregular.
5. $\Sigma(G)$ is the union of all regular orbital graphs of G.
6. $\Sigma(G)$ has valency $r|G_\alpha|$, where r is the number of regular suborbits.

First observations

Proposition.

Suppose G is transitive with $b(G) = 2$ and $\Sigma(G)$ is the Saxl graph of G.

1. $\Sigma(G)$ is G-vertex-transitive.
2. $\Sigma(G)$ is connected if G is primitive.
3. $\Sigma(G)$ is complete if and only if G is Frobenius.
4. $\Sigma(G)$ is G-arc-semiregular.
5. $\Sigma(G)$ is the union of all regular orbital graphs of G.
6. $\Sigma(G)$ has valency $r|G_\alpha|$, where r is the number of regular suborbits.
7. If $K \leq G \leq \mathrm{Sym}(\Omega)$, then $\Sigma(G)$ is a subgraph of $\Sigma(K)$.

Probabilistic methods

Let $G \leq \mathrm{Sym}(\Omega)$ be a base-two transitive permutation group with degree n. Let $\mathrm{val}(G)$ be the valency of $\Sigma(G)$. Set

$$Q(G,2) := 1 - \mathbb{P}(G,2) = \frac{|\{(\alpha,\beta) \in \Omega^2 : G_{\alpha\beta} \neq 1\}|}{n^2} = 1 - \frac{\mathrm{val}(G)}{n}.$$

Probabilistic methods

Let $G \leq \mathrm{Sym}(\Omega)$ be a base-two transitive permutation group with degree n. Let $\mathrm{val}(G)$ be the valency of $\Sigma(G)$. Set

$$Q(G,2) := 1 - \mathbb{P}(G,2) = \frac{|\{(\alpha,\beta) \in \Omega^2 : G_{\alpha\beta} \neq 1\}|}{n^2} = 1 - \frac{\mathrm{val}(G)}{n}.$$

Lemma.

If $Q(G,2) < \frac{1}{t} \leq \frac{1}{2}$, then $\Sigma(G)$ has all of the following properties:

- Any t vertices in $\Sigma(G)$ has a common neighbour;
- $\Sigma(G)$ has diameter at most 2;
- $\Sigma(G)$ has clique number at least $t+1$;
- $\Sigma(G)$ is Hamiltonian.

Probabilistic methods

Recall that

$$Q(G,2) = \frac{|\{(\alpha,\beta) \in \Omega^2 : G_{\alpha\beta} \neq 1\}|}{n^2}$$

is the probability of a random chosen pairs in Ω do not form a base.

Probabilistic methods

Recall that

$$Q(G,2) = \frac{|\{(\alpha,\beta) \in \Omega^2 : G_{\alpha\beta} \neq 1\}|}{n^2}$$

is the probability of a random chosen pairs in Ω do not form a base.

- $Q(G,2) < 1 \implies b(G) \leq 2$.
- $Q(G,2) < \frac{1}{t} \implies \Sigma(G)$ satisfies all statements in the above lemma.

Probabilistic methods

Recall that

$$Q(G,2) = \frac{|\{(\alpha,\beta) \in \Omega^2 : G_{\alpha\beta} \neq 1\}|}{n^2}$$

is the probability of a random chosen pairs in Ω do not form a base.

- $Q(G,2) < 1 \implies b(G) \leq 2$.
- $Q(G,2) < \frac{1}{t} \implies \Sigma(G)$ satisfies all statements in the above lemma.

We have

$$Q(G,2) \leq \sum_{i=1}^{m} \frac{|x_i \cap H|^2}{|x_i^G|} = \widehat{Q}(G,2),$$

where $H = G_\alpha$ and $\{x_1, \ldots, x_m\}$ is the set of representatives of G-conjugacy classes of prime-ordered elements in G.

Burness-Giudici Conjecture

Conjecture (Burness & Giudici, 2020).

Let G be a primitive permutation group. Then $\Sigma(G)$ has diameter ≤ 2.

Burness-Giudici Conjecture

Conjecture (Burness & Giudici, 2020).

Let G be a primitive permutation group. Then $\Sigma(G)$ has diameter ≤ 2.

Note that if $Q(G, 2) < \frac{1}{2}$, then the conjecture holds.

Burness-Giudici Conjecture

Conjecture (Burness & Giudici, 2020).

Let G be a primitive permutation group. Then $\Sigma(G)$ has diameter ≤ 2.

Note that if $Q(G,2) < \frac{1}{2}$, then the conjecture holds.

Example.

Let $G = \mathrm{PGL}_2(q)$ and Ω be the set of distinct pairs of 1-spaces in $\mathbb{F}_q^2$. Then $\Sigma(G) \cong J(q+1,2)$ has valency $2(q+1)$ and thus

$$Q(G,2) = 1 - \frac{\mathrm{val}(G)}{n} = 1 - \frac{4(q-1)}{q(q+1)} \to 1 \text{ as } q \to \infty$$

Burness-Giudici Conjecture

Conjecture (Burness & Giudici, 2020).

Let G be a primitive permutation group. Then $\Sigma(G)$ has diameter ≤ 2.

Note that if $Q(G,2) < \frac{1}{2}$, then the conjecture holds.

Example.

Let $G = \mathrm{PGL}_2(q)$ and Ω be the set of distinct pairs of 1-spaces in $\mathbb{F}_q^2$. Then $\Sigma(G) \cong J(q+1,2)$ has valency $2(q+1)$ and thus

$$Q(G,2) = 1 - \frac{\mathrm{val}(G)}{n} = 1 - \frac{4(q-1)}{q(q+1)} \to 1 \text{ as } q \to \infty$$

but $\Sigma(G) \cong J(q+1,2)$ still satisfies the Burness-Giudici Conjecture.

An evidence

Example.

Suppose $\mathrm{soc}(G) = \mathrm{L}_3^{\epsilon}(q)$ with $q = p \equiv \epsilon \pmod 3$ and $H = G_{\alpha}$ is of type $3^{1+2}.\mathrm{Sp}_2(3)$. Then $|H| \leq 432$ and

$$|C_G(x)| \leq \frac{|G|}{(q-1)(q^3-1)}$$

for all $x \in G$ of prime order (maximal if $\epsilon = +$ and x is unipotent with Jordan form $[J_2, J_1]$). This gives $\widehat{Q}(G,2) < 8q^{-1}$ for all $q > 23$. When $q \leq 23$ we can also check using MAGMA that the conjecture holds.

More evidences

- All primitive groups with degree $n \leq 4095$

More evidences

- All primitive groups with degree $n \leq 4095$
- All non-standard groups with socle A_n

More evidences

- All primitive groups with degree $n \leq 4095$
- All non-standard groups with socle A_n
- "Most" sporadic groups

More evidences

- All primitive groups with degree $n \leq 4095$
- All non-standard groups with socle A_n
- "Most" sporadic groups
- $\mathrm{soc}(G) = \mathrm{L}_2(q)$ **(Chen & Du, 2020)**

More evidences

- All primitive groups with degree $n \leq 4095$
- All non-standard groups with socle A_n
- "Most" sporadic groups
- $\mathrm{soc}(G) = \mathrm{L}_2(q)$ **(Chen & Du, 2020)**
- All almost simple primitive groups with soluble stabilisers **(Burness & H, in progress)**

More evidences

- All primitive groups with degree $n \leq 4095$
- All non-standard groups with socle A_n
- "Most" sporadic groups
- $\mathrm{soc}(G) = \mathrm{L}_2(q)$ **(Chen & Du, 2020)**
- All almost simple primitive groups with soluble stabilisers **(Burness & H, in progress)**
- Asymptotic results for many diagonal and twisted wreath type groups **(Fawcett, 2013/21)**

Other invariants

Clique number: maximal size of complete subgraph.

Other invariants

Clique number: maximal size of complete subgraph.

Theorem (Burness & H, in progress).

Let G be an almost simple primitive group with soluble stabiliser H. Suppose $G_0 \neq \mathrm{L}_2(q)$. Then one of the following holds:

- $\Sigma(G)$ has clique number at least 5.
- $G = A_5$ and $H = S_3$, the clique number of $\Sigma(G)$ is 4.

Other invariants

Clique number: maximal size of complete subgraph.

Theorem (Burness & H, in progress).

Let G be an almost simple primitive group with soluble stabiliser H. Suppose $G_0 \neq \mathrm{L}_2(q)$. Then one of the following holds:

- $\Sigma(G)$ has clique number at least 5.
- $G = A_5$ and $H = S_3$, the clique number of $\Sigma(G)$ is 4.

Independent number: maximal size of empty subgraph.

Other invariants

Clique number: maximal size of complete subgraph.

Theorem (Burness & H, in progress).

Let G be an almost simple primitive group with soluble stabiliser H. Suppose $G_0 \neq \mathrm{L}_2(q)$. Then one of the following holds:

- $\Sigma(G)$ has clique number at least 5.
- $G = A_5$ and $H = S_3$, the clique number of $\Sigma(G)$ is 4.

Independent number: maximal size of empty subgraph.

Theorem (Burness & H, in progress).

Let $\alpha(G)$ be the independence number of $\Sigma(G)$. Then almost simple transitive groups G with $\alpha(G) = 2$ or 3 are known.

Problems

- **Connectedness.** Characterise transitive groups with connected Saxl graph. G quasiprimitive?
- **Automorphisms.**
  - When do we have $G = \mathrm{Aut}(\Sigma(G))$?
  - When is $\Sigma(G)$ Cayley?
- **Cycles.** Eulerian cycle? Hamiltonian cycle?
- **Unique regular suborbit.** Can we classify groups with $r = 1$?
- **Other invariants.** Chromatic numbers? Spectrum?

Thank you for your attention!

Some references I

1. T.C. Burness. *Base sizes for primitive groups with soluble stabilisers*, submitted (2020), arXiv:2006.10510.
2. 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.
3. T.C. Burness and M. Giudici. *On the Saxl graph of a permutation group*, Math. Proc. Cambridge Philos. Soc. **168** (2020), 219–248.
4. T.C. Burness and H.Y. Huang. *On the Saxl graph of primitive groups with soluble stabilisers*, in preparation.
5. T.C. Burness, M.W. Liebeck and A. Shalev. *Base sizes for simple groups and a conjecture of Cameron*, Proc. Lond. Math. Soc. **98** (2009), 116–162.
6. H. Chen and S. Du. *On the Burness-Giudici conjecture*, submitted (2020), arXiv:2008.04233.

Some references II

7. J. Chen and H.Y. Huang. *On valency problems of Saxl graphs*, submitted (2020), arXiv:2012.13747.
8. J.D. Dixon. *Probabilistic group theory*. C. R. Math. Acad. Sci. Soc. R. Can. **24** (2002), no. 1, 1–15.
9. P. Erdös. *Graph theory and probability*. Canadian J. Math. **11** (1959), 34–38.
10. P. Erdös. *Graph theory and probability. II*. Canadian J. Math. **13** (1961), 346–352.
11. P. Erdös and A. Rényi. *Probabilistic methods in group theory*. J. Analyse Math. **14** (1965), 127–138.
12. C.H. Li and H. Zhang. *The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc-transitive graphs*, Proc. Lond. Math. Soc. **103** (2011), 441–472.
13. M.W. Liebeck. *Probabilistic and asymptotic aspects of finite simple groups*. Probabilistic group theory, combinatorics, and computing, 1–34, Lecture Notes in Math., 2070, Springer, London, 2013.