How many subgroups are there in a finite group? (joint work with C. M. Roney-Dougal)

Gareth Tracey
University of Warwick

AGTA 2023
Lecce, June 8th 2023

Plan for the talk

1. Counting subgroups in a finite group: where do we start?

Plan for the talk

1. Counting subgroups in a finite group: where do we start?
2. Why do we care about counting subgroups in a finite group?

Plan for the talk

1. Counting subgroups in a finite group: where do we start?
2. Why do we care about counting subgroups in a finite group?
3. A conjecture of Pyber on counting subgroups of finite symmetric groups (+ recent progress).

Plan for the talk

1. Counting subgroups in a finite group: where do we start?
2. Why do we care about counting subgroups in a finite group?
3. A conjecture of Pyber on counting subgroups of finite symmetric groups (+ recent progress).
4. Consequences of subgroup enumeration for "random subgroups" of finite groups.

Section 1. Counting subgroups in a finite group: where do we start?

Notation: For a finite group G, and a group theoretic property $\mathcal{P}$, write

$$\mathrm{Sub}_{\mathcal{P}}(G) := \{H : H \text{ a } \mathcal{P}\text{-subgroup of } G\} \text{ ; and}$$
$$\mathrm{Sub}(G) := \{H : H \text{ a subgroup of } G\}.$$

Section 1. Counting subgroups in a finite group: where do we start?

Notation: For a finite group G, and a group theoretic property $\mathcal{P}$, write

$$\mathrm{Sub}_{\mathcal{P}}(G) := \{H : H \text{ a } \mathcal{P}\text{-subgroup of } G\} \text{ ; and}$$
$$\mathrm{Sub}(G) := \{H : H \text{ a subgroup of } G\}.$$

Example

$|\mathrm{Sub}(S_3)| = 6$

Section 1. Counting subgroups in a finite group: where do we start?

Notation: For a finite group G, and a group theoretic property $\mathcal{P}$, write

$$\mathrm{Sub}_{\mathcal{P}}(G) := \{H : H \text{ a } \mathcal{P}\text{-subgroup of } G\} \text{ ; and}$$
$$\mathrm{Sub}(G) := \{H : H \text{ a subgroup of } G\}.$$

Example

$|\,\mathrm{Sub}(S_3)| = 6$ while $|\,\mathrm{Sub}_{\mathrm{cyclic}}(S_3)| = 5$.

More examples, and a question

Sticking with the theme of symmetric groups

Example

$|\operatorname{Sub}(S_3)| = 6$

$|\operatorname{Sub}(S_4)| = 30$

More examples, and a question

Sticking with the theme of symmetric groups

Example

$|\operatorname{Sub}(S_3)| = 6$

$|\operatorname{Sub}(S_4)| = 30$

$|\operatorname{Sub}(S_5)| = 156$

More examples, and a question

Sticking with the theme of symmetric groups

Example

$|\operatorname{Sub}(S_3)| = 6$

$|\operatorname{Sub}(S_4)| = 30$

$|\operatorname{Sub}(S_5)| = 156$

$\vdots$

More examples, and a question

Sticking with the theme of symmetric groups

Example

$|\operatorname{Sub}(S_3)| = 6$

$|\operatorname{Sub}(S_4)| = 30$

$|\operatorname{Sub}(S_5)| = 156$

$\vdots$

$|\operatorname{Sub}(S_{18})| = 7598016157515302757$ (Holt, 2010).

More examples, and a question

Sticking with the theme of symmetric groups

Example

$|\operatorname{Sub}(S_3)| = 6$

$|\operatorname{Sub}(S_4)| = 30$

$|\operatorname{Sub}(S_5)| = 156$

$\vdots$

$|\operatorname{Sub}(S_{18})| = 7598016157515302757$ (Holt, 2010).

In this talk, we're not going to interested in specific values of $|\operatorname{Sub}(G)|$. We are going to be mainly interested in the following:

Question

Let $(G_i)_{i\in\mathbb{N}}$ be a sequence of finite groups G_i. What can we say (asymptotically) about the functions $|\operatorname{Sub}(G_i)|$ and $\operatorname{Sub}_{\mathcal{P}}(G_i)$ as $i \to \infty$?

Specific sequences of finite groups

Arguably, the easiest natural infinite sequence of finite groups to deal with is the elementary abelian p-groups, for a fixed prime p. So let us compute $|\operatorname{Sub}(\mathbb{F}_p^m)|$.

Specific sequences of finite groups

Arguably, the easiest natural infinite sequence of finite groups to deal with is the elementary abelian p-groups, for a fixed prime p. So let us compute $|\operatorname{Sub}(\mathbb{F}_p^m)|$.

$$|\mathrm{Sub}_{d-\text{dimensional}}(\mathbb{F}_p^m)| = \frac{(p^m-1)(p^m-p)\dots(p^m-p^{d-1})}{(p^d-1)(p^d-p)\dots(p^d-p^{d-1})}$$

Specific sequences of finite groups

Arguably, the easiest natural infinite sequence of finite groups to deal with is the elementary abelian p-groups, for a fixed prime p. So let us compute $|\,\mathrm{Sub}(\mathbb{F}_p^m)|$.

$$|\mathrm{Sub}_{d-\mathrm{dimensional}}(\mathbb{F}_p^m)| = \frac{(p^m-1)(p^m-p)\dots(p^m-p^{d-1})}{(p^d-1)(p^d-p)\dots(p^d-p^{d-1})}$$

$$\sim O(p^{d(m-d)}).$$

Specific sequences of finite groups

Arguably, the easiest natural infinite sequence of finite groups to deal with is the elementary abelian p-groups, for a fixed prime p. So let us compute $|\,\mathrm{Sub}(\mathbb{F}_p^m)|$.

$$|\mathrm{Sub}_{d-\mathrm{dimensional}}(\mathbb{F}_p^m)| = \frac{(p^m-1)(p^m-p)\dots(p^m-p^{d-1})}{(p^d-1)(p^d-p)\dots(p^d-p^{d-1})}$$

$$\sim O(p^{d(m-d)}).$$

The function $p^{d(m-d)}$ is maximised at $d = m/2$. One then easily gets

$$p^{m^2/4} \leq |\,\mathrm{Sub}(\mathbb{F}_p^m)| \leq cp^{m^2/4}$$

for some absolute constant c.

Specific sequences of finite groups

Arguably, the easiest natural infinite sequence of finite groups to deal with is the elementary abelian p-groups, for a fixed prime p. So let us compute $|\,\mathrm{Sub}(\mathbb{F}_p^m)|$.

$$|\mathrm{Sub}_{d-\mathrm{dimensional}}(\mathbb{F}_p^m)| = \frac{(p^m-1)(p^m-p)\dots(p^m-p^{d-1})}{(p^d-1)(p^d-p)\dots(p^d-p^{d-1})}$$

$$\sim O(p^{d(m-d)}).$$

The function $p^{d(m-d)}$ is maximised at $d = m/2$. One then easily gets

$$p^{m^2/4} \leq |\,\mathrm{Sub}(\mathbb{F}_p^m)| \leq cp^{m^2/4}$$

for some absolute constant c.

Although this computation is very straightforward, it is very useful for coming up with lower bounds on $|\,\mathrm{Sub}(G)|$ in more interesting classes of finite groups..

Example

Fix an even integer n. Then S_n has a subgroup

$$H := \langle (1,2), (3,4), \ldots, (n-1, n) \rangle \cong \mathbb{F}_2^{n/2}.$$

Example

Fix an even integer n. Then S_n has a subgroup

$$H := \langle (1,2), (3,4), \ldots, (n-1, n) \rangle \cong \mathbb{F}_2^{n/2}.$$

Thus, the above tell us that

$$|\operatorname{Sub}(S_n)| \geq |\operatorname{Sub}(H)| \geq 2^{n^2/16}.$$

Example

Fix an even integer n. Then S_n has a subgroup

$$H := \langle (1,2), (3,4), \ldots, (n-1, n) \rangle \cong \mathbb{F}_2^{n/2}.$$

Thus, the above tell us that

$$|\operatorname{Sub}(S_n)| \geq |\operatorname{Sub}(H)| \geq 2^{n^2/16}.$$

Example

Fix a prime p, and an even integer n. Then $\mathrm{GL}_n(\mathbb{F}_p)$ has a subgroup

$$H := \left\{ \begin{bmatrix} I_{n/2} & A \\ 0_{n/2} & I_{n/2} \end{bmatrix} : A \in M_{n/2}(\mathbb{F}_p) \right\} \cong \mathbb{F}_p^{n^2/4}.$$

Example

Fix an even integer n. Then S_n has a subgroup

$$H := \langle (1,2), (3,4), \ldots, (n-1, n) \rangle \cong \mathbb{F}_2^{n/2}.$$

Thus, the above tell us that

$$|\operatorname{Sub}(S_n)| \geq |\operatorname{Sub}(H)| \geq 2^{n^2/16}.$$

Example

Fix a prime p, and an even integer n. Then $\mathrm{GL}_n(\mathbb{F}_p)$ has a subgroup

$$H := \left\{ \begin{bmatrix} I_{n/2} & A \\ 0_{n/2} & I_{n/2} \end{bmatrix} : A \in M_{n/2}(\mathbb{F}_p) \right\} \cong \mathbb{F}_p^{n^2/4}.$$

Thus, we have

$$|\operatorname{Sub}(\mathrm{GL}_n(\mathbb{F}_p))| \geq |\operatorname{Sub}(H)| \geq p^{n^4/64}.$$

Upper bounds

These lower bounds will come in handy later on..

Upper bounds

These lower bounds will come in handy later on..

What about general techniques for finding upper bounds on $|\mathrm{Sub}(G)|$?

Upper bounds

These lower bounds will come in handy later on..

What about general techniques for finding upper bounds on $|\mathrm{Sub}(G)|$?

Note first that in general, for a normal subgroup N of G, there is not an upper bound on $|\mathrm{Sub}(G)|$ in terms of $|\mathrm{Sub}(N)|$ and $|\mathrm{Sub}(G/N)|$. (One can already see this from elementary abelian groups of order p^2.) This makes reductions difficult..

Upper bounds

These lower bounds will come in handy later on..

What about general techniques for finding upper bounds on $|\operatorname{Sub}(G)|$?

Note first that in general, for a normal subgroup N of G, there is not an upper bound on $|\operatorname{Sub}(G)|$ in terms of $|\operatorname{Sub}(N)|$ and $|\operatorname{Sub}(G/N)|$. (One can already see this from elementary abelian groups of order p^2.) This makes reductions difficult..

We do remark however, that if $G = N \rtimes H$, then we have

$$|\operatorname{Sub}(G)| = \sum_{N_0 \leq N, H_0 \leq N_H(N_0)} |\operatorname{Der}(H_0, N_0)|$$

where $\operatorname{Der}(H_0, N_0)$ is the set of derivations from H_0 to N_0).

Upper bounds (continued)

A surprisingly effective upper bound is a simple one: Suppose that every subgroup of G can be generated by d elements. Then

$$|\operatorname{Sub}(G)| \leq |G|^d.$$

Upper bounds (continued)

A surprisingly effective upper bound is a simple one: Suppose that every subgroup of G can be generated by d elements. Then

$$|\operatorname{Sub}(G)| \leq |G|^d.$$

More generally, if every $\mathcal{P}$-subgroup of G can be generated by $d_{\mathcal{P}}$ elements. Then

$$|\operatorname{Sub}_{\mathcal{P}}(G)| \leq |G|^{d_{\mathcal{P}}}.$$

Upper bounds (continued)

A surprisingly effective upper bound is a simple one: Suppose that every subgroup of G can be generated by d elements. Then

$$|\operatorname{Sub}(G)| \leq |G|^d.$$

More generally, if every $\mathcal{P}$-subgroup of G can be generated by $d_{\mathcal{P}}$ elements. Then

$$|\operatorname{Sub}_{\mathcal{P}}(G)| \leq |G|^{d_{\mathcal{P}}}.$$

Indeed, we have seen that if $G = \mathbb{F}_p^m$, for p prime, then $|\operatorname{Sub}(G)| \sim p^{m^2/4}$.

Upper bounds (continued)

A surprisingly effective upper bound is a simple one: Suppose that every subgroup of G can be generated by d elements. Then

$$|\operatorname{Sub}(G)| \leq |G|^d.$$

More generally, if every $\mathcal{P}$-subgroup of G can be generated by $d_{\mathcal{P}}$ elements. Then

$$|\operatorname{Sub}_{\mathcal{P}}(G)| \leq |G|^{d_{\mathcal{P}}}.$$

Indeed, we have seen that if $G = \mathbb{F}_p^m$, for p prime, then $|\operatorname{Sub}(G)| \sim p^{m^2/4}$.

If we just noted that every subgroup of G can be generated by m elements, then we'd get the upper bound $|\operatorname{Sub}(G)| \leq p^{m^2}$.

Section 2: Motivation and history

Why do we care about subgroup enumeration?

Section 2: Motivation and history

Why do we care about subgroup enumeration?

Reason 1: Numerous motivations from other areas of mathematics.
For example:

Section 2: Motivation and history

Why do we care about subgroup enumeration?

Reason 1: Numerous motivations from other areas of mathematics.
For example:

- Galois theory: If E/F is a finite Galois extension, then

$$\#\text{Intermediate fields } E/K = |\operatorname{Sub}(\operatorname{Gal}(E/F))|.$$

Section 2: Motivation and history

Why do we care about subgroup enumeration?

Reason 1: Numerous motivations from other areas of mathematics.
For example:

- Galois theory: If E/F is a finite Galois extension, then

$$\#\text{Intermediate fields } E/K = |\,\mathrm{Sub}(\mathrm{Gal}(E/F))|.$$

- Topology: If X is a path connected, locally path connected, and semi-locally simply connected topological space, then

$$\#\text{Isomorphism classes of covers of } X = \#\text{Conjugacy classes of subgroups of } \pi_1(X)$$

Reason 2: Graph enumeration problems. For example, suppose that we want to count the number of vertex-transitive graphs on n vertices.

Reason 2: Graph enumeration problems. For example, suppose that we want to count the number of vertex-transitive graphs on n vertices.

For such a graph Γ, if we know the neighbours of the first vertex; and we know $\mathrm{Aut}(\Gamma)$, then we know every edge, since Γ is vertex-transitive.

Reason 2: Graph enumeration problems. For example, suppose that we want to count the number of vertex-transitive graphs on n vertices.

For such a graph Γ, if we know the neighbours of the first vertex; and we know $\mathrm{Aut}(\Gamma)$, then we know every edge, since Γ is vertex-transitive.

There are 2^{n-1} possibilities for the neighbours of the first vertex.

Reason 2: Graph enumeration problems. For example, suppose that we want to count the number of vertex-transitive graphs on n vertices.

For such a graph Γ, if we know the neighbours of the first vertex; and we know $\mathrm{Aut}(\Gamma)$, then we know every edge, since Γ is vertex-transitive.

There are 2^{n-1} possibilities for the neighbours of the first vertex.

There are $|\mathrm{Sub}_{\text{transitive}}(S_n)|$ possibilities for $\mathrm{Aut}(\Gamma)$.

Reason 2: Graph enumeration problems. For example, suppose that we want to count the number of vertex-transitive graphs on n vertices.

For such a graph Γ, if we know the neighbours of the first vertex; and we know $\mathrm{Aut}(\Gamma)$, then we know every edge, since Γ is vertex-transitive.

There are 2^{n-1} possibilities for the neighbours of the first vertex.

There are $|\mathrm{Sub}_{\text{transitive}}(S_n)|$ possibilities for $\mathrm{Aut}(\Gamma)$.

Thus, there are at most $2^{n-1}|\mathrm{Sub}_{\text{transitive}}(S_n)|$ vertex-transitive graphs on n vertices.

Reason 2: Graph enumeration problems. For example, suppose that we want to count the number of vertex-transitive graphs on n vertices.

For such a graph Γ, if we know the neighbours of the first vertex; and we know a transitive subgroup of $\mathrm{Aut}(\Gamma)$, then we know every edge, since Γ is vertex-transitive.

There are 2^{n-1} possibilities for the neighbours of the first vertex.

There are at most $|\,\mathrm{Sub}_{\text{minimal transitive}}(S_n)|$ possibilities for a minimal transitive subgroup of $\mathrm{Aut}(\Gamma)$.

Thus, there are at most $2^{n-1}|\,\mathrm{Sub}_{\text{minimal transitive}}(S_n)|$ vertex-transitive graphs on n vertices.

Reason 3: Group enumeration. For a positive integer n, let

$$\mathrm{Iso}(n) := \# \text{ Isomorphism classes of groups of order } n.$$

Reason 3: Group enumeration. For a positive integer n, let

$$\mathrm{Iso}(n) := \# \text{ Isomorphism classes of groups of order } n.$$

For example, $\mathrm{Iso}(6) = 2$ and $\mathrm{Iso}(8) = 5$.

Reason 3: Group enumeration. For a positive integer n, let

$$\mathrm{Iso}(n) := \#\ \text{Isomorphism classes of groups of order } n.$$

For example, $\mathrm{Iso}(6) = 2$ and $\mathrm{Iso}(8) = 5$.

What happens to $\mathrm{Iso}(n)$ as $n \to \infty$?

Reason 3: Group enumeration. For a positive integer n, let

$$\mathrm{Iso}(n) := \#\text{ Isomorphism classes of groups of order } n.$$

For example, $\mathrm{Iso}(6) = 2$ and $\mathrm{Iso}(8) = 5$.

What happens to $\mathrm{Iso}(n)$ as $n \to \infty$?

Let's start with the case where n is a prime power..

Reason 3: Group enumeration. For a positive integer n, let

$$\mathrm{Iso}(n) := \#\ \text{Isomorphism classes of groups of order } n.$$

For example, $\mathrm{Iso}(6) = 2$ and $\mathrm{Iso}(8) = 5$.

What happens to $\mathrm{Iso}(n)$ as $n \to \infty$?

Let's start with the case where n is a prime power..

Theorem (Higman & Sims, 1965)

Let p be prime. Then

$$\mathrm{Iso}(p^k) = p^{2k^3/27 + o(k^3)}.$$

Reason 3: Group enumeration. For a positive integer n, let

$$\mathrm{Iso}(n) := \#\ \text{Isomorphism classes of groups of order } n.$$

For example, $\mathrm{Iso}(6) = 2$ and $\mathrm{Iso}(8) = 5$.

What happens to $\mathrm{Iso}(n)$ as $n \to \infty$?

Let's start with the case where n is a prime power..

Theorem (Higman & Sims, 1965)

Let p be prime. Then

$$\mathrm{Iso}(p^k) = p^{2k^3/27 + o(k^3)}.$$

Following Higman and Sims' results, the big question became: What happens for general n?

Group enumeration continued

We will write the prime factorisation of a positive integer n as $n = \prod_{p \text{ prime}} p^{n(p)}$.

Group enumeration continued

We will write the prime factorisation of a positive integer n as $n = \prod_{p \text{ prime}} p^{n(p)}$. Then define

$$\mu(n) := \max\{n(p) : p \text{ prime}\}$$

to be the largest exponent of a prime power divisor of n.

Group enumeration continued

We will write the prime factorisation of a positive integer n as $n = \prod_{p \text{ prime}} p^{n(p)}$. Then define

$$\mu(n) := \max\{n(p) : p \text{ prime}\}$$

to be the largest exponent of a prime power divisor of n. Thus, for p an odd prime, $\mu(2p^k) = k$, for example.

Group enumeration continued

We will write the prime factorisation of a positive integer n as $n = \prod_{p \text{ prime}} p^{n(p)}$. Then define

$$\mu(n) := \max\{n(p) : p \text{ prime}\}$$

to be the largest exponent of a prime power divisor of n. Thus, for p an odd prime, $\mu(2p^k) = k$, for example.

The Higman–Sims result, in this language, states:

Theorem (Higman & Sims, 1965)

Let p be prime, $n := p^k$. Then

$$\mathrm{Iso}(n) = n^{2\mu(n)^2/27 + o(\mu(n)^2)} \text{ as } \mu(n) \to \infty.$$

Group enumeration continued

We will write the prime factorisation of a positive integer n as $n = \prod_{p \text{ prime}} p^{n(p)}$. Then define

$$\mu(n) := \max\{n(p) : p \text{ prime}\}$$

to be the largest exponent of a prime power divisor of n. Thus, for p an odd prime, $\mu(2p^k) = k$, for example.

The Higman–Sims result, in this language, states:

Theorem (Higman & Sims, 1965)

Let p be prime, $n := p^k$. Then

$$\mathrm{Iso}(n) = n^{2\mu(n)^2/27 + o(\mu(n)^2)} \text{ as } \mu(n) \to \infty.$$

Theorem (Pyber, 1993)

Let n be a positive integer. Then

$$\mathrm{Iso}(n) = n^{2\mu(n)^2/27 + o(\mu(n)^2)} \text{ as } \mu(n) \to \infty.$$

Group enumeration continued

But.. what has all of this got to with subgroup enumeration?!

Group enumeration continued

But.. what has all of this got to with subgroup enumeration?!

The answer lies in a key step from Pyber's proof..

Group enumeration continued

But.. what has all of this got to with subgroup enumeration?!

The answer lies in a key step from Pyber's proof..

Key step from Pyber's proof: Let G be a finite group of order n, and let N be a "nice" self-centralising normal subgroup of G. Then

$$G/Z(N) \hookrightarrow \mathrm{Aut}(N)$$

Group enumeration continued

But.. what has all of this got to with subgroup enumeration?!

The answer lies in a key step from Pyber's proof..

Key step from Pyber's proof: Let G be a finite group of order n, and let N be a "nice" self-centralising normal subgroup of G. Then

$$G/Z(N) \hookrightarrow \mathrm{Aut}(N) \hookrightarrow S_{|N|-1}.$$

Group enumeration continued

But.. what has all of this got to with subgroup enumeration?!

The answer lies in a key step from Pyber's proof..

Key step from Pyber's proof: Let G be a finite group of order n, and let N be a "nice" self-centralising normal subgroup of G. Then

$$G/Z(N) \hookrightarrow \mathrm{Aut}(N) \hookrightarrow S_{|N|-1}.$$

Thus, if we can count the number of possibilities for N, then we can determine the number of possibilities for $G/Z(N)$ by counting the subgroups of $S_{|N|-1}$.

Group enumeration continued

But.. what has all of this got to with subgroup enumeration?!

The answer lies in a key step from Pyber's proof..

Key step from Pyber's proof: Let G be a finite group of order n, and let N be a "nice" self-centralising normal subgroup of G. Then

$$G/Z(N) \hookrightarrow \mathrm{Aut}(N) \hookrightarrow S_{|N|-1}.$$

Thus, if we can count the number of possibilities for N, then we can determine the number of possibilities for $G/Z(N)$ by counting the subgroups of $S_{|N|-1}$.

Finally, to count the number of possibilities for G given $G/Z(N)$, one needs a relatively straightforward calculation with the second cohomology group of G acting on $Z(N)$.

Group enumeration continued: What is "nice"?

By "nice" here, we mean that the possibilities for N should be easy to count.

Group enumeration continued: What is "nice"?

By "nice" here, we mean that the possibilities for N should be easy to count.

Pyber takes N to be the generalised Fitting subgroup $F^*(G)$ of G.

Group enumeration continued: What is "nice"?

By "nice" here, we mean that the possibilities for N should be easy to count.

Pyber takes N to be the generalised Fitting subgroup $F^*(G)$ of G.

The group $F^*(G)$ is a central product of nilpotent and quasisimple groups, so one can count the possibilities for $F^*(G)$ by using the Higman-Sims result, together with the classification of finite simple groups.

Group enumeration continued: What is "nice"?

By "nice" here, we mean that the possibilities for N should be easy to count.

Pyber takes N to be the generalised Fitting subgroup $F^*(G)$ of G.

The group $F^*(G)$ is a central product of nilpotent and quasisimple groups, so one can count the possibilities for $F^*(G)$ by using the Higman-Sims result, together with the classification of finite simple groups.

So from

$$G/Z(N) \hookrightarrow \mathrm{Aut}(N) \hookrightarrow S_{|N|-1},$$

we are now (leaving a lot of details, and another important step out..) reduced to counting the number of subgroups of a finite symmetric group!

This led Pyber to a theorem, and a conjecture.

This led Pyber to a theorem, and a conjecture.

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

This led Pyber to a theorem, and a conjecture.

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Conjecture (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

This led Pyber to a theorem, and a conjecture.

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Conjecture (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

This led Pyber to a theorem, and a conjecture.

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Conjecture (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Note that $1/16 = 0.0625$.

This led Pyber to a theorem, and a conjecture.

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Conjecture (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Note that $1/16 = 0.0625$. Also, recall from earlier in the talk that

$$|\operatorname{Sub}(S_n)| \geq |\operatorname{Sub}(\langle(1,2),(3,4),\ldots\rangle)| \geq 2^{(n-1)^2/16}.$$

This led Pyber to a theorem, and a conjecture.

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Conjecture (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Note that $1/16 = 0.0625$. Also, recall from earlier in the talk that

$$|\operatorname{Sub}(S_n)| \geq |\operatorname{Sub}(\langle(1,2),(3,4),\ldots\rangle)| \geq 2^{(n-1)^2/16}.$$

So in a certain sense, Pyber's conjecture states that the subgroups of S_n are "dominated" by elementary abelian 2-groups.

Section 3. Pyber's conjecture

So how can we tackle Pyber's conjecture?

Section 3. Pyber's conjecture

So how can we tackle Pyber's conjecture? Let's first look at Pyber's proof of the $2^{cn^2+o(n^2)}$ bound..

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\,\mathrm{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Section 3. Pyber's conjecture

So how can we tackle Pyber's conjecture? Let's first look at Pyber's proof of the $2^{cn^2+o(n^2)}$ bound..

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641...$

Sketch proof: The proof uses the following highly ubiquitous result of Aschbacher and Guralnick:

Section 3. Pyber's conjecture

So how can we tackle Pyber's conjecture? Let's first look at Pyber's proof of the $2^{cn^2+o(n^2)}$ bound..

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\operatorname{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641\ldots$

Sketch proof: The proof uses the following highly ubiquitous result of Aschbacher and Guralnick:

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

Section 3. Pyber's conjecture

So how can we tackle Pyber's conjecture? Let's first look at Pyber's proof of the $2^{cn^2+o(n^2)}$ bound..

Theorem (Pyber, 1990)

Let n be a positive integer. Then

$$|\mathrm{Sub}(S_n)| \leq 2^{cn^2+o(n^2)}$$

where $c := (\log_2 24)/6 = 0.7641...$

Sketch proof: The proof uses the following highly ubiquitous result of Aschbacher and Guralnick:

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

The proof then has four ingredients:

The proof then has four ingredients:

- $|\mathrm{Sub}(G)| \leq |\mathrm{Sub}_{\mathsf{soluble}}(G)||G|$ (Aschbacher & Guralnick).

The proof then has four ingredients:

- $|\mathrm{Sub}(G)| \leq |\mathrm{Sub}_{\mathrm{soluble}}(G)||G|$ (Aschbacher & Guralnick).
- The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

The proof then has four ingredients:

- $|\mathrm{Sub}(G)| \leq |\mathrm{Sub}_{\mathsf{soluble}}(G)||G|$ (Aschbacher & Guralnick).
- The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).
- A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).

The proof then has four ingredients:

- $|\mathrm{Sub}(G)| \leq |\mathrm{Sub}_{\text{soluble}}(G)||G|$ (Aschbacher & Guralnick).
- The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).
- A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).
- For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987).

The proof then has four ingredients:

- $|\mathrm{Sub}(G)| \leq |\mathrm{Sub}_{\mathrm{soluble}}(G)||G|$ (Aschbacher & Guralnick).
- The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).
- A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).
- For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987).

It follows that

$$
\begin{aligned}
|\mathrm{Sub}(S_n)| \leq n!|\mathrm{Sub}_{\mathrm{soluble}}(S_n)| &\leq n! \sum_{M <_{\text{max sol}} S_n} |\mathrm{Sub}(M)| \\
&\leq n! \sum_{M <_{\text{max sol}} S_n} |M|^{n/2} \\
&\leq n! \sum_{M <_{\text{max sol}} S_n} 24^{n^2/6} \\
&\leq n! 2^{17n+n\log n} 24^{n^2/6} = 2^{cn^2+o(n^2)}
\end{aligned}
$$

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps..

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element (Aschbacher & Guralnick, 1982).

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987).

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987).

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible: For n even, $H := \langle (1,2), \ldots, (n-1,n) \rangle \leq S_n$ needs exactly $n/2$ generators.

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967).

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible.

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967). Best possible: If $n = 4^t$, then $|S_4^{\wr t}| = 24^{(n-1)/3}$.

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible.

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

- Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).
- Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990).
- Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967). Best possible.
- Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible.

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990). Possibly not best possible, but it doesn't matter! This gets swallowed by the $o(n^2)$ term anyway..

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967). Best possible.

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible.

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

- Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982).
- Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990). Possibly not best possible, but it doesn't matter!
- Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967). Best possible.
- Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible.

In considering Pyber's conjecture, a natural first step is to look at Pyber's proof, and see if there are any "gains" to be made from any of the steps.. So let's look at the steps again:

Step 1: Every finite group can be generated by a soluble subgroup + one other element. (Aschbacher & Guralnick, 1982). Best possible, but.. Could we replace soluble by something stronger, like nilpotent?

Step 2: The number of maximal soluble subgroups of S_n is bounded above by $2^{17n+n\log n} = 2^{o(n^2)}$ (Pyber, 1990). Possibly not best possible, but it doesn't matter!

Step 3: A soluble subgroup of S_n has order at most $24^{(n-1)/3}$ (Dixon, 1967). Best possible.

Step 4: For $n > 3$, every subgroup of S_n can be generated by $n/2$ elements (McIver & Neumann, 1987). Best possible.

The Aschbacher–Guralnick theorem

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

The Aschbacher–Guralnick theorem

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

Can we replace "soluble" by "nilpotent"?

The Aschbacher–Guralnick theorem

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

Can we replace "soluble" by "nilpotent"? NO!

Example (Aschbacher, 1991)

Let H be any non-nilpotent group, and let p be a prime with $p \nmid |H|$.

The Aschbacher–Guralnick theorem

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

Can we replace "soluble" by "nilpotent"? NO!

Example (Aschbacher, 1991)

Let H be any non-nilpotent group, and let p be a prime with $p \nmid |H|$.

Let $\mathbb{F}$ be a finite field of characteristic p, and let V be a non-cyclic $\mathbb{F}[H]$-module with $C_V(h) = 0$ for all $1 \neq h \in H$.

The Aschbacher–Guralnick theorem

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

Can we replace "soluble" by "nilpotent"? NO!

Example (Aschbacher, 1991)

Let H be any non-nilpotent group, and let p be a prime with $p \nmid |H|$.

Let $\mathbb{F}$ be a finite field of characteristic p, and let V be a non-cyclic $\mathbb{F}[H]$-module with $C_V(h) = 0$ for all $1 \neq h \in H$.

Let $G = V \rtimes H$. Then G cannot be generated by two nilpotent subgroups.

The Aschbacher–Guralnick theorem

Theorem (Aschbacher & Guralnick, 1982)

Every finite group can be generated by a soluble subgroup together with one other element.

Can we replace "soluble" by "nilpotent"? NO!

Example (Aschbacher, 1991)

Let H be any non-nilpotent group, and let p be a prime with $p \nmid |H|$.

Let $\mathbb{F}$ be a finite field of characteristic p, and let V be a non-cyclic $\mathbb{F}[H]$-module with $C_V(h) = 0$ for all $1 \neq h \in H$.

Let $G = V \rtimes H$. Then G cannot be generated by two nilpotent subgroups.

E.g. The group $H := \mathrm{SL}_2(3) < \mathrm{SL}_2(5)$ acts regularly on the non-zero elements of $W := \mathbb{F}_5^2$. Take $V := W \oplus W \oplus W$, with H acting diagonally.

So in general, a finite group cannot be generated by a nilpotent subgroup + one other element..

So in general, a finite group cannot be generated by a nilpotent subgroup + one other element..

However, let's think back to how the Aschbacher-Guralnick theorem was used in Pyber's proof. We had

$$|\operatorname{Sub}(S_n)| \leq |\operatorname{Sub}_{\mathsf{soluble}}(S_n)||S_n|.$$

The point was that $|S_n| = n! \leq 2^{n \log n} = 2^{o(n^2)}$.

So in general, a finite group cannot be generated by a nilpotent subgroup + one other element..

However, let's think back to how the Aschbacher-Guralnick theorem was used in Pyber's proof. We had

$$|\mathrm{Sub}(S_n)| \leq |\mathrm{Sub}_{\text{soluble}}(S_n)||S_n|.$$

The point was that $|S_n| = n! \leq 2^{n \log n} = 2^{o(n^2)}$.

So in fact, for Pyber's proof, it would have sufficed to have a result that said that every finite group G can be generated by a soluble subgroup, $+ f(G)$ other elements, where $f(G) n \log n = o(n^2)$ for all $G \leq S_n$.

So in general, a finite group cannot be generated by a nilpotent subgroup + one other element..

However, let's think back to how the Aschbacher-Guralnick theorem was used in Pyber's proof. We had

$$|\mathrm{Sub}(S_n)| \leq |\mathrm{Sub}_{\mathrm{soluble}}(S_n)||S_n|.$$

The point was that $|S_n| = n! \leq 2^{n \log n} = 2^{o(n^2)}$.

So in fact, for Pyber's proof, it would have sufficed to have a result that said that every finite group G can be generated by a soluble subgroup, + $f(G)$ other elements, where $f(G) n \log n = o(n^2)$ for all $G \leq S_n$.

With this in mind..

So in general, a finite group cannot be generated by a nilpotent subgroup + one other element..

However, let's think back to how the Aschbacher-Guralnick theorem was used in Pyber's proof. We had

$$|\operatorname{Sub}(S_n)| \leq |\operatorname{Sub}_{\mathsf{soluble}}(S_n)||S_n|.$$

The point was that $|S_n| = n! \leq 2^{n \log n} = 2^{o(n^2)}$.

So in fact, for Pyber's proof, it would have sufficed to have a result that said that every finite group G can be generated by a soluble subgroup, $+ f(G)$ other elements, where $f(G)n \log n = o(n^2)$ for all $G \leq S_n$.

With this in mind.. Can we prove that every finite group can be generated by a nilpotent subgroup, together with some "small" bunch of other elements?

An alternative for nilpotent subgroups

The *socle length* of a finite group G is defined to be the minimal r such that $\operatorname{soc}^r(G) = G$, where $\operatorname{soc}^0(G) := 1$, and $\operatorname{soc}^i(G)/\operatorname{soc}^{i-1}(G) := \operatorname{soc}(G/\operatorname{soc}^{i-1}(G))$ for $i \geq 1$.

An alternative for nilpotent subgroups

The *socle length* of a finite group G is defined to be the minimal r such that $\mathrm{soc}^r(G) = G$, where $\mathrm{soc}^0(G) := 1$, and $\mathrm{soc}^i(G)/\mathrm{soc}^{i-1}(G) := \mathrm{soc}(G/\mathrm{soc}^{i-1}(G))$ for $i \geq 1$.

Theorem (Roney-Dougal & T., 2022)

For a finite group G, let $A(G)$ be the order of the largest abelian section of G, and let $\mathrm{sl}(G)$ be the socle length of G. Every finite group G can be generated by a nilpotent subgroup, together with $4\mathrm{sl}(G)\sqrt{\log A(G)} + 1$ other elements.

An alternative for nilpotent subgroups

The *socle length* of a finite group G is defined to be the minimal r such that $\mathrm{soc}^r(G) = G$, where $\mathrm{soc}^0(G) := 1$, and $\mathrm{soc}^i(G)/\mathrm{soc}^{i-1}(G) := \mathrm{soc}(G/\mathrm{soc}^{i-1}(G))$ for $i \geq 1$.

Theorem (Roney-Dougal & T., 2022)

For a finite group G, let $A(G)$ be the order of the largest abelian section of G, and let $\mathrm{sl}(G)$ be the socle length of G. Every finite group G can be generated by a nilpotent subgroup, together with $4\mathrm{sl}(G)\sqrt{\log A(G)} + 1$ other elements.

The proof first reduces to the case where $\Phi(G) = 1$, and then uses the theory of crowns in finite groups.

An alternative for nilpotent subgroups

The *socle length* of a finite group G is defined to be the minimal r such that $\mathrm{soc}^r(G) = G$, where $\mathrm{soc}^0(G) := 1$, and $\mathrm{soc}^i(G)/\mathrm{soc}^{i-1}(G) := \mathrm{soc}(G/\mathrm{soc}^{i-1}(G))$ for $i \geq 1$.

Theorem (Roney-Dougal & T., 2022)

For a finite group G, let $A(G)$ be the order of the largest abelian section of G, and let $\mathrm{sl}(G)$ be the socle length of G. Every finite group G can be generated by a nilpotent subgroup, together with $4\mathrm{sl}(G)\sqrt{\log A(G)} + 1$ other elements.

The proof first reduces to the case where $\Phi(G) = 1$, and then uses the theory of crowns in finite groups.

But how does this help us with Pyber's conjecture?

An alternative for nilpotent subgroups

The *socle length* of a finite group G is defined to be the minimal r such that $\mathrm{soc}^r(G) = G$, where $\mathrm{soc}^0(G) := 1$, and $\mathrm{soc}^i(G)/\mathrm{soc}^{i-1}(G) := \mathrm{soc}(G/\mathrm{soc}^{i-1}(G))$ for $i \geq 1$.

Theorem (Roney-Dougal & T., 2022)

For a finite group G, let $A(G)$ be the order of the largest abelian section of G, and let $\mathrm{sl}(G)$ be the socle length of G. Every finite group G can be generated by a nilpotent subgroup, together with $4\mathrm{sl}(G)\sqrt{\log A(G)} + 1$ other elements.

The proof first reduces to the case where $\Phi(G) = 1$, and then uses the theory of crowns in finite groups.

But how does this help us with Pyber's conjecture?

Recall that we need $|S_n|^{4\mathrm{sl}(G)\sqrt{\log A(G)}+1}$ to be $2^{o(n^2)}$..

For a positive integer m, let $\mathrm{Sub}_{(m)}(S_n)$ be the set of subgroups of S_n which have all of their orbits of length at most m.

For a positive integer m, let $\mathrm{Sub}_{(m)}(S_n)$ be the set of subgroups of S_n which have all of their orbits of length at most m.

Proposition

There exists an absolute constant c such that if $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, *then* $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

For a positive integer m, let $\mathrm{Sub}_{(m)}(S_n)$ be the set of subgroups of S_n which have all of their orbits of length at most m.

Proposition

There exists an absolute constant c such that if $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, then $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

Point of this proposition: If $G \in \mathrm{Sub}_{(m)}(S_n)$, then $\mathrm{sl}(G)$ is bounded above by a function of m.

For a positive integer m, let $\mathrm{Sub}_{(m)}(S_n)$ be the set of subgroups of S_n which have all of their orbits of length at most m.

Proposition

There exists an absolute constant c such that if $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, then $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

Point of this proposition: If $G \in \mathrm{Sub}_{(m)}(S_n)$, then $\mathrm{sl}(G)$ is bounded above by a function of m.

Our previous result states that every finite group G can be generated by a nilpotent subgroup + $4\mathrm{sl}(G)\sqrt{A(G)} + 1$ other elements.

For a positive integer m, let $\mathrm{Sub}_{(m)}(S_n)$ be the set of subgroups of S_n which have all of their orbits of length at most m.

Proposition

There exists an absolute constant c such that if $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, then $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

Point of this proposition: If $G \in \mathrm{Sub}_{(m)}(S_n)$, then $\mathrm{sl}(G)$ is bounded above by a function of m.

Our previous result states that every finite group G can be generated by a nilpotent subgroup $+ \; 4\mathrm{sl}(G)\sqrt{A(G)} + 1$ other elements.

Since $A(G) \leq (\log 3/3)n$ for all $G \leq S_n$ (Kovács & Praeger, 1989), the groups G we need to count have the property that $4\mathrm{sl}(G)\sqrt{A(G)} + 1 \leq O(\sqrt{n})$.

For a positive integer m, let $\mathrm{Sub}_{(m)}(S_n)$ be the set of subgroups of S_n which have all of their orbits of length at most m.

Proposition

There exists an absolute constant c such that if $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, *then* $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

Point of this proposition: If $G \in \mathrm{Sub}_{(m)}(S_n)$, then $\mathrm{sl}(G)$ is bounded above by a function of m.

Our previous result states that every finite group G can be generated by a nilpotent subgroup $+ \; 4\mathrm{sl}(G)\sqrt{A(G)} + 1$ other elements.

Since $A(G) \leq (\log 3/3)n$ for all $G \leq S_n$ (Kovács & Praeger, 1989), the groups G we need to count have the property that $4\mathrm{sl}(G)\sqrt{A(G)} + 1 \leq O(\sqrt{n})$.

And... $|S_n|^{O(\sqrt{n})} = 2^{o(n^2)}$.

Thus, we have reduced Pyber's conjecture to proving that

$$|\mathrm{Sub}_{\mathsf{nilpotent},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Thus, we have reduced Pyber's conjecture to proving that

$$|\mathrm{Sub}_{\text{nilpotent},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

This in fact quickly reduces to proving that

$$|\mathrm{Sub}_{\text{2-group},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Thus, we have reduced Pyber's conjecture to proving that

$$|\mathrm{Sub}_{\text{nilpotent},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

This in fact quickly reduces to proving that

$$|\mathrm{Sub}_{\text{2-group},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Theorem (Roney-Dougal & T., 2023)

Pyber's conjecture holds. In fact,

$$|\,\mathrm{Sub}(S_n)| \leq 2^{n^2/16+O(n^{3/2})}.$$

Some remarks on the proof

Of course, the main step is getting down to the problem of showing

$$|\mathrm{Sub}_{\text{2-group},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Some remarks on the proof

Of course, the main step is getting down to the problem of showing

$$|\mathrm{Sub}_{\text{2-group},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Now, if $G \in \mathrm{Sub}_{\text{2-group},(c)}(S_n)$, then G is S_n-conjugate to a subgroup of

$$G_1 \times \ldots \times G_t$$

where G_i is a transitive permutation 2-group of degree at most c.

Some remarks on the proof

Of course, the main step is getting down to the problem of showing

$$|\mathrm{Sub}_{\text{2-group},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Now, if $G \in \mathrm{Sub}_{\text{2-group},(c)}(S_n)$, then G is S_n-conjugate to a subgroup of

$$G_1 \times \ldots \times G_t$$

where G_i is a transitive permutation 2-group of degree at most c.

So we "just" have to count subgroups of a direct product of 2-groups of bounded size.

Some remarks on the proof

Of course, the main step is getting down to the problem of showing

$$|\mathrm{Sub}_{2\text{-group},(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}.$$

Now, if $G \in \mathrm{Sub}_{2\text{-group},(c)}(S_n)$, then G is S_n-conjugate to a subgroup of

$$G_1 \times \ldots \times G_t$$

where G_i is a transitive permutation 2-group of degree at most c.

So we "just" have to count subgroups of a direct product of 2-groups of bounded size.

Our first attempt: This is surely doable if c is small?! For example, if $c = 2$, then we are just counting subgroups of a finite vector space over $\mathbb{F}_2$, and as we saw earlier in the talk, this is easy.

So we looked back at our proof of

Proposition

There exists an absolute constant c such that if $|\operatorname{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, *then* $|\operatorname{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

to see if we could get a reasonable estimate for c..

So we looked back at our proof of

Proposition

There exists an absolute constant c *such that if* $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$, *then* $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

to see if we could get a reasonable estimate for c..

.. The best we could do with $c = 2^{16^2}$.

So we looked back at our proof of

Proposition

There exists an absolute constant c such that if $|\mathrm{Sub}_{(c)}(S_n)| \leq 2^{n^2/16+o(n^2)}$*, then* $|\mathrm{Sub}(S_n)| \leq 2^{n^2/16+o(n^2)}$.

to see if we could get a reasonable estimate for c..

.. The best we could do with $c = 2^{16^2}$.

Our next attempt: The important idea for progress came from the following: If we want to count subgroups of a direct product $G_1 \times G_2$ of permutation groups $G_1 \leq S_{n_1}$, $G_2 \leq S_{n_2}$ with $n_1 + n_2 = n$, then Goursat's lemma tells us that $|\mathrm{Sub}(G_1 \times G_2)|$ is at most

$$|\mathrm{Sub}(G_1)||\mathrm{Sub}(G_2)| \max\{|\mathrm{Hom}(Y, X)| : Y \leq G_2,\ X \text{ a section of } G_1\}.$$

So we looked back at our proof of

Proposition

There exists an absolute constant c such that if $|\operatorname{Sub}_{(c)}(S_n)| \le 2^{n^2/16+o(n^2)}$, *then* $|\operatorname{Sub}(S_n)| \le 2^{n^2/16+o(n^2)}$.

to see if we could get a reasonable estimate for c..

.. The best we could do with $c = 2^{16^2}$.

Our next attempt: The important idea for progress came from the following: If we want to count subgroups of a direct product $G_1 \times G_2$ of permutation groups $G_1 \le S_{n_1}$, $G_2 \le S_{n_2}$ with $n_1 + n_2 = n$, then Goursat's lemma tells us that $|\operatorname{Sub}(G_1 \times G_2)|$ is at most

$$|\operatorname{Sub}(G_1)||\operatorname{Sub}(G_2)| \max\{|\operatorname{Hom}(Y, X)| : Y \le G_2,\ X \text{ a section of } G_1\}.$$

Induction gives $|\operatorname{Sub}(G_i)| \le 2^{n_i^2/16+O(n_i^{3/2})}$, so if $|\operatorname{Hom}(Y, X)| \le 2^{n_1 n_2/8}$, for X a 2-section of S_{n_1}, Y a 2-subgroup of S_{n_2}, then we'd be done.

Goursat's lemma tells us that $|\operatorname{Sub}(G_1 \times G_2)|$ is at most

$$|\operatorname{Sub}(G_1)||\operatorname{Sub}(G_2)| \max\{|\operatorname{Hom}(Y, X)| : Y \leq G_2, X \text{ a section of } G_1\}.$$

Induction gives $|\operatorname{Sub}(G_i)| \leq 2^{n_i^2/16 + O(n_i^{3/2})}$, so if $|\operatorname{Hom}(Y, X)| \leq 2^{n_1 n_2/8}$, for X a 2-section of S_{n_1}, Y a 2-subgroup of S_{n_2}, then we'd be done.

Goursat's lemma tells us that $|\operatorname{Sub}(G_1 \times G_2)|$ is at most

$|\operatorname{Sub}(G_1)||\operatorname{Sub}(G_2)| \max\{|\operatorname{Hom}(Y, X)| : Y \leq G_2,\ X \text{ a section of } G_1\}$.

Induction gives $|\operatorname{Sub}(G_i)| \leq 2^{n_i^2/16 + O(n_i^{3/2})}$, so if $|\operatorname{Hom}(Y, X)| \leq 2^{n_1 n_2/8}$, for X a 2-section of S_{n_1}, Y a 2-subgroup of S_{n_2}, then we'd be done.

With careful reordering of the groups in our large direct product, and various small improvements on current results on generator numbers in permutation groups, we managed to get what we need.

Section 4. Applications to random subgroups, and random finite groups

Now that we have an approach to enumerating subgroups of finite groups, a natural next question is:

Question

What does a random subgroup of a given finite group G look like?

Section 4. Applications to random subgroups, and random finite groups

Now that we have an approach to enumerating subgroups of finite groups, a natural next question is:

Question

What does a random subgroup of a given finite group G look like?

We also have:

Question

What does a random finite group look like?

Section 4. Applications to random subgroups, and random finite groups

Now that we have an approach to enumerating subgroups of finite groups, a natural next question is:

Question

What does a random subgroup of a given finite group G look like?

We also have:

Question

What does a random finite group look like?

Definition

Let $\mathcal{P}$ be a group theoretic property.

1. Let $(G_i)_{i\in\mathbb{N}}$ be a sequence of finite groups. We say that a random subgroup of the (G_i) has property $\mathcal{P}$ if

$$\frac{|\mathrm{Sub}_{\mathcal{P}}(G_i)|}{|\,\mathrm{Sub}(G_i)|} \to 1 \text{ as } i \to \infty.$$

2. Let $\mathrm{Iso}^*(n)$ [respectively $\mathrm{Iso}^*_{\mathcal{P}}(n)$] be the number of isomorphism classes of finite groups [resp. finite $\mathcal{P}$-groups] of order at most n. We say that a random finite group has property $\mathcal{P}$ if

$$\frac{\mathrm{Iso}^*{}_{\mathcal{P}}(G_i)}{\mathrm{Iso}^*(G_i)} \to 1 \text{ as } i \to \infty.$$

2. Let $\mathrm{Iso}^*(n)$ [respectively $\mathrm{Iso}^*_{\mathcal{P}}(n)$] be the number of isomorphism classes of finite groups [resp. finite $\mathcal{P}$-groups] of order at most n. We say that a random finite group has property $\mathcal{P}$ if

$$\frac{\mathrm{Iso}^*{}_{\mathcal{P}}(G_i)}{\mathrm{Iso}^*(G_i)} \to 1 \text{ as } i \to \infty.$$

For example, classical conjectures of Erdős and Pyber state:

Conjecture (Erdős, 1968)

Let n, x be positive integers with $n \leq 2^x$. Then

$$\mathrm{Iso}(n) \leq \mathrm{Iso}(2^x).$$

Conjecture (Pyber, 1990)

A random finite group is nilpotent.

Sticking to our theme of symmetric groups, we have the following conjecture of Kantor:

Conjecture (Kantor, 1993)

A random subgroup of the symmetric groups $(S_n)_n$ *is nilpotent.*

Sticking to our theme of symmetric groups, we have the following conjecture of Kantor:

Conjecture (Kantor, 1993)

A random subgroup of the symmetric groups $(S_n)_n$ is nilpotent.

Theorem (T., 2023)

There exists absolute constants C and C_0 such that a random subgroup G of the symmetric groups $(S_n)_n$ has the property that at most $C_0\sqrt{n}$ points from $\{1, \ldots, n\}$ lie in a G-orbit of size greater than C.

Sticking to our theme of symmetric groups, we have the following conjecture of Kantor:

Conjecture (Kantor, 1993)

A random subgroup of the symmetric groups $(S_n)_n$ is nilpotent.

Theorem (T., 2023)

There exists absolute constants C and C_0 such that a random subgroup G of the symmetric groups $(S_n)_n$ has the property that at most $C_0\sqrt{n}$ points from $\{1, \ldots, n\}$ lie in a G-orbit of size greater than C.

Corollary

A random subgroup of the symmetric groups $(S_n)_n$ has at least $O(n)$ orbits.

Sticking to our theme of symmetric groups, we have the following conjecture of Kantor:

Conjecture (Kantor, 1993)

A random subgroup of the symmetric groups $(S_n)_n$ is nilpotent.

Theorem (T., 2023)

There exists absolute constants C and C_0 such that a random subgroup G of the symmetric groups $(S_n)_n$ has the property that at most $C_0\sqrt{n}$ points from $\{1, \dots, n\}$ lie in a G-orbit of size greater than C.

Corollary

A random subgroup of the symmetric groups $(S_n)_n$ has at least $O(n)$ orbits.

Theorem (Lucchini, 1998)

A random subgroup of the symmetric groups $(S_n)_n$ is intransitive.