Transitive permutation groups: Minimal, invariable and random generation

Gareth Tracey

University of Warwick

Bielefeld, January 12th, 2017

A motivational question

How many subgroups does the symmetric group S_n have?

A motivational question

How many subgroups does the symmetric group S_n have?

For a finite group G, let $Sub(G)$ denote the set of subgroups of G.

Suppose that every subgroup of S_n can be generated by $f(n)$ elements..

A motivational question

How many subgroups does the symmetric group S_n have?

For a finite group G, let $Sub(G)$ denote the set of subgroups of G.

Suppose that every subgroup of S_n can be generated by $f(n)$ elements..

Then

$$|Sub(S_n)| \leq n!^{f(n)}$$

A motivational question

How many subgroups does the symmetric group S_n have?

For a finite group G, let $Sub(G)$ denote the set of subgroups of G.

Suppose that every subgroup of S_n can be generated by $f(n)$ elements..

Then

$$|Sub(S_n)| \leq n!^{f(n)}$$

Similarly, if X is a group-theoretical property, and $Sub_X(S_n)$ denotes the set of X-subgroups of S_n, and every X-subgroup of S_n can be generated by $f_X(n)$ elements, we have

$$|Sub_X(S_n)| \leq n!^{f_X(n)}$$

$d(G)$ for subgroups of S_n

Therefore, the question now is: For a fixed property X, what is $f_X(n)$?

$d(G)$ for subgroups of S_n

Therefore, the question now is: For a fixed property X, what is $f_X(n)$?

For a group G, let $d(G)$ denote the minimal number of elements required to generate G.

$d(G)$ for subgroups of S_n

Therefore, the question now is: For a fixed property X, what is $f_X(n)$?

For a group G, let $d(G)$ denote the minimal number of elements required to generate G.

Take $G \leq S_n$. Then

$d(G)$ for subgroups of S_n

Therefore, the question now is: For a fixed property X, what is $f_X(n)$?

For a group G, let $d(G)$ denote the minimal number of elements required to generate G.

Take $G \leq S_n$. Then

$d(G) \leq n - 1$

$d(G)$ for subgroups of S_n

Therefore, the question now is: For a fixed property X, what is $f_X(n)$?

For a group G, let $d(G)$ denote the minimal number of elements required to generate G.

Take $G \leq S_n$. Then

$d(G) \leq n - \#(\text{Orbits of } G) \leq n - 1$

The general case: G is an arbitrary subgroup of S_n

..So we have $d(G) \leq n-1$ for $G \leq S_n$.. Can we do any better than linear in n?

The general case: G is an arbitrary subgroup of S_n

..So we have $d(G) \leq n-1$ for $G \leq S_n$.. Can we do any better than linear in n?

Example:

Take n to be even, and let $G = \langle (1,2),(3,4),\dots,(n-1,n) \rangle$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^{n/2}$, so $d(G) = n/2$.

The general case: G is an arbitrary subgroup of S_n

..So we have $d(G) \leq n-1$ for $G \leq S_n$.. Can we do any better than linear in n?

Example:

Take n to be even, and let $G = \langle (1,2), (3,4), \ldots, (n-1, n) \rangle$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^{n/2}$, so $d(G) = n/2$.

Theorem (McIver; Neumann, 1989 (CFSG))

Let G be a permutation group of degree $n \geq 2$, with $(G, n) \neq (S_3, 3)$. Then

(i) $d(G) \leq n/2$.

The general case: G is an arbitrary subgroup of S_n

..So we have $d(G) \leq n-1$ for $G \leq S_n$.. Can we do any better than linear in n?

Example:

Take n to be even, and let $G = \langle (1,2),(3,4),\ldots,(n-1,n)\rangle$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^{n/2}$, so $d(G) = n/2$.

Theorem (McIver; Neumann, 1989 (CFSG))

Let G be a permutation group of degree n, with $(G,n) \neq (S_3,3)$. Then

(i) $d(G) \leq n/2$, *and;*

(ii) *If G is transitive and $n > 4$, $(G,n) \neq (D_8 \circ D_8, 8)$, then $d(G) < n/2$.*

Transitive permutation groups

Many believed that a bound of the form $d(G) \leq (\log_2 n)^c$ should hold..

Transitive permutation groups

Many believed that a bound of the form $d(G) \leq (\log_2 n)^c$ should hold..

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n$$

as $m \to \infty$.

Transitive permutation groups

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n$$

as $m \to \infty$.

Theorem (Kovács; Newman, 1989)

Let $G \leq S_n$ be transitive and nilpotent. Then

$$d(G) = O\left(\frac{n}{\sqrt{\log_2 n}}\right)$$

Transitive permutation groups

Theorem (Bryant; Kovács; Robinson, 1995)

Let $G \leq S_n$ be transitive and soluble. Then

$$d(G) = O\left(\frac{n}{\sqrt{\log_2 n}}\right)$$

Transitive permutation groups

Theorem (Bryant; Kovács; Robinson, 1995)

Let $G \leq S_n$ be transitive and soluble. Then

$$d(G) = O\left(\frac{n}{\sqrt{\log_2 n}}\right)$$

Theorem (Lucchini; Menegazzo; Morigi, 2000 (CFSG))

Let $G \leq S_n$ be transitive. Then

$$d(G) = O\left(\frac{n}{\sqrt{\log_2 n}}\right)$$

Transitive permutation groups

Theorem (Bryant; Kovács; Robinson, 1995)

Let $G \leq S_n$ be transitive and soluble. Then

$$d(G) = O\left(\frac{n}{\sqrt{\log_2 n}}\right)$$

Theorem (Lucchini; Menegazzo; Morigi, 2000 (CFSG))

Let $G \leq S_n$ be transitive. Then

$$d(G) = O\left(\frac{n}{\sqrt{\log_2 n}}\right)$$

..But what about the constants involved?..

Transitive permutation groups

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n \text{ as } m \to \infty.$$

Transitive permutation groups

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n \text{ as } m \to \infty.$$

Lemma (T., 2015)

$b = \sqrt{2/\pi} = 0.79\ldots.$

Transitive permutation groups

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n \text{ as } m \to \infty.$$

Lemma (T., 2015)

$b = \sqrt{2/\pi} = 0.79\ldots.$

Conjecture

Let G be a transitive permutation group of degree $n \geq 2$. Then

$$d(G) \leq \frac{(b + o(1))n}{\sqrt{\log_2 n}}.$$

Transitive permutation groups

Lemma (T., 2015)

$b = \sqrt{2/\pi} = 0.79\ldots.$

Conjecture

Let G be a transitive permutation group of degree $n \geq 2$. Then

$$d(G) \leq \frac{(b + o(1))n}{\sqrt{\log_2 n}}.$$

Theorem (T., 2015 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then

$$d(G) \leq \frac{cn}{\sqrt{\log_2 n}}$$

where $c := \sqrt{3}/2 = 0.86\ldots.$

Transitive permutation groups

Theorem (T., 2015 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then

$$d(G) \leq \frac{cn}{\sqrt{\log_2 n}}$$

where $c := \sqrt{3}/2 = 0.86\ldots$.

Remark

$c = \sqrt{3}/2$ is the optimal value when $n = 8$ and $G \cong D_8 \circ D_8$.

So how many transitive subgroups in S_n?

We can deduce that

$$|Sub_{transitive}(S_n)| \leq n!^{\frac{cn}{\sqrt{\log_2 n}}}$$

So how many transitive subgroups in S_n?

We can deduce that

$$|Sub_{transitive}(S_n)| \leq n!^{\frac{cn}{\sqrt{\log_2 n}}}$$

Theorem (Lucchini; Menegazzo; Morigi, 2000 (CFSG))

There exists an absolute constant $\overline{c}$ such that

$$|Sub_{transitive}(S_n)| \leq 2^{\frac{\overline{c}n^2}{\sqrt{\log_2 n}}}$$

Back to our original question..

From the McIver-Neumann “Half n” bound, we can also deduce that

$$|Sub(S_n)| \leq n!^{\frac{n}{2}}$$

Back to our original question..

From the McIver-Neumann "Half n" bound, we can also deduce that

$$|Sub(S_n)| \leq n!^{\frac{n}{2}}$$

Theorem (Pyber, 1993)

Let $Sub(S_n)$ denote the number of subgroups of S_n. Then

$$|Sub(S_n)| \leq 24^{(\frac{1}{6}+o(1))n^2}$$

Back to our original question..

From the McIver-Neumann "Half n" bound, we can also deduce that

$$|Sub(S_n)| \leq n!^{\frac{n}{2}}$$

Theorem (Pyber, 1993)

Let $Sub(S_n)$ denote the number of subgroups of S_n. Then

$$|Sub(S_n)| \leq 24^{(\frac{1}{6}+o(1))n^2}$$

S_n contains an elementary abelian subgroup $G := \langle (1,2),(3,4),\ldots \rangle$ of order $2^{\lfloor \frac{n}{2} \rfloor}$.

Back to our original question..

From the McIver-Neumann “Half n” bound, we can also deduce that

$$|Sub(S_n)| \leq n!^{\frac{n}{2}}$$

Theorem (Pyber, 1993)

Let $Sub(S_n)$ denote the number of subgroups of S_n. Then

$$|Sub(S_n)| \leq 24^{(\frac{1}{6}+o(1))n^2}$$

S_n contains an elementary abelian subgroup $G := \langle (1,2),(3,4),\dots\rangle$ of order $2^{\lfloor \frac{n}{2} \rfloor}$.

An easy counting argument shows that

$$|Sub(G)| = 2^{(\frac{1}{16}+o(1))n^2}$$

Back to our original question..

Theorem (Pyber, 1993)

Let $Sub(S_n)$ denote the number of subgroups of S_n. Then

$$2^{(\frac{1}{16}+o(1))n^2} \leq |Sub(S_n)| \leq 24^{(\frac{1}{6}+o(1))n^2}.$$

Back to our original question..

Theorem (Pyber, 1993)

Let $Sub(S_n)$ denote the number of subgroups of S_n. Then

$$2^{(\frac{1}{16}+o(1))n^2} \leq |Sub(S_n)| \leq 24^{(\frac{1}{6}+o(1))n^2}.$$

Thus, the order of magnitude is

$$|Sub(S_n)| = 2^{(\alpha+o(1))n^2}$$

for some constant α.

Back to our original question..

Theorem (Pyber, 1993)

Let $Sub(S_n)$ denote the number of subgroups of S_n. Then

$$2^{(\frac{1}{16}+o(1))n^2} \leq |Sub(S_n)| \leq 24^{(\frac{1}{6}+o(1))n^2}.$$

Thus, the order of magnitude is

$$|Sub(S_n)| = 2^{(\alpha+o(1))n^2}$$

for some constant α.

Conjecture (Pyber, 1993)

$|Sub(S_n)| = 2^{(\frac{1}{16}+o(1))n^2}$.

A reduction theorem

Conjecture (Pyber, 1993)

$|Sub(S_n)| = 2^{(\frac{1}{16}+o(1))n^2}$.

For a constant $k \geq 1$, let $Sub_k(S_n)$ denote the set of subgroups of S_n all of whose orbits have length at most k.. Jan-Christoph Schlage-Puchta proved the following reduction:

A reduction theorem

Conjecture (Pyber, 1993)

$|Sub(S_n)| = 2^{(\frac{1}{16}+o(1))n^2}$.

For a constant $k \geq 1$, let $Sub_k(S_n)$ denote the set of subgroups of S_n all of whose orbits have length at most k.. Jan-Christoph Schlage-Puchta proved the following reduction:

Theorem (Schlage-Puchta, 2016)

Assume that

$$\max\left\{\frac{d(G)\log_2|G|}{n^2} : G \leq S_n \textit{ transitive}\right\} \to 0 \textit{ as } n \to \infty \ (*)$$

Then $|Sub(S_n)| = |Sub_k(S_n)|2^{o(n^2)}$, *for some absolute constant* k.

A reduction theorem

Conjecture (Pyber, 1993)

$|Sub(S_n)| = 2^{(\frac{1}{16}+o(1))n^2}$.

Theorem (Schlage-Puchta, 2016)

Assume that

$$\max\left\{\frac{d(G)\log_2|G|}{n^2} : G \leq S_n \textit{ transitive}\right\} \to 0 \textit{ as } n \to \infty \ (*)$$

Then $|Sub(S_n)| = |Sub_k(S_n)|2^{o(n^2)}$, *for some absolute constant* k.

We remark that $Sub_k(S_n)$ consists of the subgroups of the direct products

$$S_{k_1} \times S_{k_2} \times \ldots \times S_{k_t}$$

where $\sum_i k_i = n$ and each $k_i \leq k$.

Does the hypothesis hold true?

Does the hypothesis hold true?

So is

$$\lim_{n\to\infty} \max\left\{ \frac{d(G)\log_2|G|}{n^2} \;:\; G \leq S_n \text{ transitive} \right\} = 0?$$

Does the hypothesis hold true?

So is

$$\lim_{n\to\infty} \max\left\{\frac{d(G)\log_2|G|}{n^2} : G \leq S_n \text{ transitive}\right\} = 0?$$

Must a “large” transitive group have a “small” number of generators?

Does the hypothesis hold true?

So is

$$\lim_{n\to\infty} \max\left\{\frac{d(G)\log_2|G|}{n^2} \;:\; G \leq S_n \text{ transitive}\right\} = 0?$$

Must a "large" transitive group have a "small" number of generators?

Example:

$d(S_n) = 2$, $d(A_n) = 2$;

Does the hypothesis hold true?

So is

$$\lim_{n\to\infty} \max\left\{\frac{d(G)\log_2|G|}{n^2} \,:\, G \leq S_n \text{ transitive}\right\} = 0?$$

Must a "large" transitive group have a "small" number of generators?

Example:

$d(S_n) = 2$, $d(A_n) = 2$;

Example:

If $G \leq S_n$ is primitive, and is not A_n or S_n then $\log_2|G| = O(n)$ (Praeger; Saxl, 1980; Maróti, 2002), and $d(G) \leq \log_2 n$ (Holt; Roney-Dougal, 2013).

Can a large transitive group have many generators?

So is

$$\lim_{n\to\infty} \max \left\{ \frac{d(G)\log_2 |G|}{n^2} \; : \; G \leq S_n \text{ transitive} \right\} = 0?$$

Example:

The maximal imprimitive transitive subgroups of S_n are the wreath products $S_m \wr S_{\frac{n}{m}}$. All of these are 2-generated..

Can a large transitive group have many generators?

So is

$$\lim_{n\to\infty} \max\left\{\frac{d(G)\log_2|G|}{n^2} : G \leq S_n \text{ transitive}\right\} = 0?$$

Example:

The maximal imprimitive transitive subgroups of S_n are the wreath products $S_m \wr S_{\frac{n}{m}}$. All of these are 2-generated..

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n$$

as $m \to \infty$.

Can a large transitive group have many generators?

So is

$$\lim_{n\to\infty} \max \left\{ \frac{d(G)\log_2|G|}{n^2} : G \leq S_n \text{ transitive} \right\} = 0?$$

Example (Kovács; Newman, 1989)

There exists an absolute constant b, and a sequence of transitive permutation groups G_m of degree $n = 2^{2m}$, such that

$$d(G_m) \to \frac{b2^{2m}}{\sqrt{2m}} + 2m = \frac{bn}{\sqrt{\log_2 n}} + \log_2 n$$

as $m \to \infty$.

The groups G_m have order $\sim 2^{n/4}$. Hence

$$d(G_m)\log_2|G_m| \sim Cn^2/\sqrt{\log_2 n}$$

Can a large transitive group have many generators?

The groups G_m have order $\sim 2^{n/4}$. Hence

$$d(G_m)\log_2|G_m| \sim \frac{Cn^2}{\sqrt{\log_2 n}}$$

for some absolute constant C.

Theorem (T., 2016 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then there exists an absolute constant C such that

$$d(G) \leq \frac{Cn^2}{\log_2|G|\sqrt{\log_2 n}}.$$

Can a large transitive group have many generators?

The groups G_m have order $\sim 2^{n/4}$. Hence

$$d(G_m)\log_2|G_m| \sim \frac{Cn^2}{\sqrt{\log_2 n}}$$

for some absolute constant C.

Theorem (T., 2016 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then there exists an absolute constant C such that

$$d(G) \leq \frac{Cn^2}{\log_2|G|\sqrt{\log_2 n}}.$$

Corollary (Schlage-Puchta, 2016 (CFSG))

$|Sub(S_n)| = |Sub_k(S_n)|2^{o(n^2)}$ *for some absolute constant k.*

Minimally transitive groups

Minimally transitive groups

Definition

A transitive permutation group G is called *minimally transitive* if every proper subgroup of G is intransitive.

Minimally transitive groups

Definition

A transitive permutation group G is called *minimally transitive* if every proper subgroup of G is intransitive.

Example:

Any finite group G is minimally transitive of degree $|G|$ (via the regular action).

Minimally transitive groups

Definition

A transitive permutation group G is called *minimally transitive* if every proper subgroup of G is intransitive.

Example:

Any finite group G is minimally transitive of degree $|G|$ (via the regular action).

Example:

$G := Alt(5)$ in its action on the cosets of $\langle (1,2)(3,4), (1,3)(2,4) \rangle$;

$d(G)$ for minimally transitive groups

$d(G)$ for minimally transitive groups

Question

What is the best possible upper bound of the form

$$d(G) \leq f(n)$$

on the set of minimally transitive groups G of degree n?

$d(G)$ for minimally transitive groups

Question

What is the best possible upper bound of the form

$$d(G) \leq f(n) \quad \left(\leq \frac{cn}{\sqrt{\log_2 n}}\right)$$

on the set of minimally transitive groups G of degree n?

$d(G)$ for minimally transitive groups

Question

What is the best possible upper bound of the form

$$d(G) \leq f(n) \quad (\leq \log_2 n) \quad \text{(Neumann; Vaughan-Lee, 1977)}$$

on the set of minimally transitive groups G of degree n?

Minimally transitive groups: A question of Pyber

Theorem (Pyber, 1991)

Let G be a minimally transitive permutation group of degree n, which is either regular or nilpotent. Then $d(G) \leq \mu(n) + 1$.

Minimally transitive groups: A question of Pyber

Theorem (Pyber, 1991)

Let G be a minimally transitive permutation group of degree n, which is either regular or nilpotent. Then $d(G) \leq \mu(n) + 1$.

Question (Pyber, 1991)

Is it true that $d(G) \leq \mu(n) + 1$ for all minimally transitive permutation groups of degree n?

Minimally transitive groups: A question of Pyber

Theorem (Pyber, 1991)

Let G be a minimally transitive permutation group of degree n, which is either regular or nilpotent. Then $d(G) \leq \mu(n) + 1$.

Question (Pyber, 1991)

Is it true that $d(G) \leq \mu(n) + 1$ for all minimally transitive permutation groups of degree n?

Theorem (Lucchini, 1996)

Let G be a soluble minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n) + 1$.

Minimally transitive groups: A question of Pyber

Theorem (Pyber, 1991)

Let G be a minimally transitive permutation group of degree n, which is either regular or nilpotent. Then $d(G) \leq \mu(n) + 1$.

Question (Pyber, 1991)

Is it true that $d(G) \leq \mu(n) + 1$ for all minimally transitive permutation groups of degree n?

Theorem (Lucchini, 1996)

Let G be a soluble minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n) + 1$.

Theorem (T., 2015 (CFSG))

Let G be a minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n) + 1$.

The proof: first step

The proof: first step

Let G be a counterexample of minimal degree n, and let M be any nontrivial normal subgroup of G.

The proof: first step

Let G be a counterexample of minimal degree n, and let M be any nontrivial normal subgroup of G.

Also, let Ω be the set of orbits of M (so $|\Omega| < n$).

The proof: first step

Let G be a counterexample of minimal degree n, and let M be any nontrivial normal subgroup of G.

Also, let Ω be the set of orbits of M (so $|\Omega| < n$).

Then, since M is normal in G, G acts on Ω, and the following hold:

1. G/K acts minimally transitive on Ω, where K is the kernel of the action of G on Ω;
2. $|\Omega|$ divides n.

The proof: first step

It now follows easily, from the minimality of G as a counterexample, and from the minimal transitivity of G, that

$$d(G/M) \leq \mu(|\Omega|) + 1 \leq \mu(n) + 1$$

The proof: first step

It now follows easily, from the minimality of G as a counterexample, and from the minimal transitivity of G, that

$$d(G/M) \leq \mu(|\Omega|) + 1 \leq \mu(n) + 1 < d(G)$$

The proof: first step

It now follows easily, from the minimality of G as a counterexample, and from the minimal transitivity of G, that

$$d(G/M) \leq \mu(|\Omega|) + 1 \leq \mu(n) + 1 < d(G)$$

So we have proved:

Step 1: G needs more generators than any of its proper quotients.

Finite groups which need more generators than any proper quotient

Finite groups which need more generators than any proper quotient

Let L be a finite group, with a unique minimal normal subgroup N. If N is abelian, then assume further that N has a complement in L.

Finite groups which need more generators than any proper quotient

Let L be a finite group, with a unique minimal normal subgroup N. If N is abelian, then assume further that N has a complement in L.

For $k \geq 1$, define the following subgroup of L^k:

$$L_k := \{(x_1, x_2, \ldots, x_k) : Nx_i = Nx_j \text{ for all } i, j\} = diag(L^k)N^k$$

Finite groups which need more generators than any proper quotient

Let L be a finite group, with a unique minimal normal subgroup N. If N is abelian, then assume further that N has a complement in L.

For $k \geq 1$, define the following subgroup of L^k:

$$L_k := \{(x_1, x_2, \ldots, x_k) : Nx_i = Nx_j \text{ for all } i, j\} = diag(L^k)N^k$$

Theorem (Dalla Volta; Lucchini, 1998 (CFSG))

Let G be a finite group which needs more generators than any proper quotient. Then there exists a finite group L with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and a positive integer $k \geq 2$, such that $G \cong L_k$.

The proof of the theorem: continued

The proof of the theorem: continued

Thus

$$G \cong L_k := diag(L^k)N^k$$

for some finite group L with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and some $k \geq 2$.

The proof of the theorem: continued

Thus

$$G \cong L_k := diag(L^k)N^k$$

for some finite group L with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and some $k \geq 2$.

Step 2:

1. If N is abelian, then $k \leq \mu(n)$;
2. If N is nonabelian, then $k \leq f(N)\mu(n) + 1$, where $f(N) := r/2 + 1$ if N is a direct product of copies of $Alt(r)$, and $f(N) := 4$ otherwise.

Indices of proper subgroups in nonabelian simple groups

Lemma ((CFSG))

Let S be a nonabelian finite simple group. Then there exists a set of primes $\Gamma = \Gamma(S)$ such that

1. $|\Gamma| \leq f(S)$, *where* $f(S) = r/2 + 1$ *if* S *is an alternating group of degree* r, *and* $f(S) \leq 4$ *otherwise;*
2. $\pi(|S : H|)$ $(= \{p : p \text{ is a prime divisor of } |S : H|\})$ *intersects* Γ *non-trivially for every proper subgroup* H *of* S.

The proof of the theorem: continued

Thus

$$G \cong L_k := diag(L^k)N^k$$

for some finite group L with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and some $k \geq 2$.

Step 2:

1. If N is abelian, then $k \leq \mu(n)$;
2. If N is nonabelian, then $k \leq f(N)\mu(n) + 1$, where $f(N) := r/2 + 1$ if N is a direct product of copies of $Alt(r)$, and $f(N) := 4$ otherwise.

The proof of the theorem: continued

Thus

$$G \cong L_k := diag(L^k)N^k$$

for some finite group L with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and some $k \geq 2$.

Step 2:

1. If N is abelian, then $k \leq \mu(n)$;
2. If N is nonabelian, then $k \leq f(N)\mu(n) + 1$, where $f(N) := r/2 + 1$ if N is a direct product of copies of $Alt(r)$, and $f(N) := 4$ otherwise.

Using results of Dalla Volta and Lucchini, we can now find upper bounds for $d(L_k) > \mu(n) + 1$ in terms of k and N..

The proof of the theorem: continued

Thus

$$G \cong L_k := diag(L^k)N^k$$

for some finite group L with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and some $k \geq 2$.

Step 2:

1. If N is abelian, then $k \leq \mu(n)$;
2. If N is nonabelian, then $k \leq f(N)\mu(n) + 1$, where $f(N) := r/2 + 1$ if N is a direct product of copies of $Alt(r)$, and $f(N) := 4$ otherwise.

Using results of Dalla Volta and Lucchini, we can now find upper bounds for $d(L_k) > \mu(n) + 1$ in terms of k and N..

This leads to lower bounds on k in terms of $\mu(n)$ and N..

Invariable generation

Invariable generation

Definition

(i) A subset $\{x_1, x_2, \ldots, x_t\}$ of a group G is said to *invariably generate* G if $G = \langle x_1^{g_1}, x_2^{g_2}, \ldots, x_t^{g_t} \rangle$ for any t-tuple $(g_1, g_2, \ldots, g_t)$ of elements of G.

(ii) The cardinality of the smallest invariable generating set for a finite group G is denoted by $d_I(G)$.

Invariable generation

Definition

(i) A subset $\{x_1, x_2, \ldots, x_t\}$ of a group G is said to *invariably generate* G if $G = \langle x_1^{g_1}, x_2^{g_2}, \ldots, x_t^{g_t} \rangle$ for any t-tuple $(g_1, g_2, \ldots, g_t)$ of elements of G.

(ii) The cardinality of the smallest invariable generating set for a finite group G is denoted by $d_I(G)$.

Clearly $d(G) \leq d_I(G)$ in general, but the question is:

Invariable generation

Definition

(i) A subset $\{x_1, x_2, \ldots, x_t\}$ of a group G is said to *invariably generate* G if $G = \langle x_1^{g_1}, x_2^{g_2}, \ldots, x_t^{g_t} \rangle$ for any t-tuple $(g_1, g_2, \ldots, g_t)$ of elements of G.

(ii) The cardinality of the smallest invariable generating set for a finite group G is denoted by $d_I(G)$.

Clearly $d(G) \leq d_I(G)$ in general, but the question is:

Question

Pick a result of the form

"Let G be a ________ finite group. Then $d(G) \leq \ldots$"

Does this result hold if we replace $d(G)$ by $d_I(G)$?

Invariable generation

Theorem (Kantor; Lubotzky; Shalev, 2011)

Let G be a finite nilpotent group. Any generating set for G is also an invariable generating set. In particular, $d(G) = d_I(G)$.

Invariable generation

Theorem (Kantor; Lubotzky; Shalev, 2011)

Let G be a finite nilpotent group. Any generating set for G is also an invariable generating set. In particular, $d(G) = d_I(G)$.

Theorem (Kantor; Lubotzky; Shalev, 2011)

For every positive integer n, there exists a finite group G such that $d(G) = 2$ and $d_I(G) \leq n$.

Invariable generation

Theorem (Kantor; Lubotzky; Shalev, 2011)

Let G be a finite nilpotent group. Any generating set for G is also an invariable generating set. In particular, $d(G) = d_I(G)$.

Theorem (Kantor; Lubotzky; Shalev, 2011)

For every positive integer n, there exists a finite group G such that $d(G) = 2$ and $d_I(G) \leq n$.

Also...

Theorem (Guralnick; Malle, 2011 and Kantor; Lubotzky; Shalev, 2011 (CFSG))

Let G be a nonabelian finite simple group. Then $d_I(G) = 2$.

$d_l(G)$ for permutation groups

$d_l(G)$ for permutation groups

Theorem (McIver; Neumann, 1989 (CFSG))

Let G be a permutation group of degree n. Then $d(G) \leq n/2$, except when $n = 3$ and $G \cong S_3$.

$d_I(G)$ for permutation groups

Theorem (McIver; Neumann, 1989 (CFSG))

Let G be a permutation group of degree n. Then $d(G) \leq n/2$, except when $n = 3$ and $G \cong S_3$.

Theorem (Detomi; Lucchini, 2014 (CFSG))

Let G be a permutation group of degree n. Then $d_I(G) \leq n/2$, except when $n = 3$ and $G \cong S_3$.

$d_I(G)$ for permutation groups

Theorem (McIver; Neumann, 1989 (CFSG))

Let G be a permutation group of degree n. Then $d(G) \leq n/2$, except when $n = 3$ and $G \cong S_3$.

Theorem (Detomi; Lucchini, 2014 (CFSG))

Let G be a permutation group of degree n. Then $d_I(G) \leq n/2$, except when $n = 3$ and $G \cong S_3$.

Problem

Let G be a permutation group of degree n. Prove that $d_I(G) \leq n - 1$ (or indeed that $d_I(G) = O(n)$) without using CFSG or the O'Nan Scott Theorem.

$d_l(G)$ for transitive permutation groups

$d_I(G)$ for transitive permutation groups

Theorem (Kovács; Newman, 1989; Bryant; Kovács; Robinson, 1995; Lucchini, 2000 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then $d(G) \leq \frac{cn}{\sqrt{\log_2 n}}$, for some absolute constant c.

$d_I(G)$ for transitive permutation groups

Theorem (Kovács; Newman, 1989; Bryant; Kovács; Robinson, 1995; Lucchini, 2000 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then $d(G) \leq \dfrac{cn}{\sqrt{\log_2 n}}$, for some absolute constant c.

Theorem (T., 2016 (CFSG))

Let G be a transitive permutation group of degree $n \geq 2$. Then $d_I(G) \leq \dfrac{cn}{\sqrt{\log_2 n}}$, where $c := \sqrt{3}/2$.

$d_l(G)$ for minimally transitive permutation groups

Theorem (T., 2015 (CFSG))

Let G be a minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n) + 1$.

$d_I(G)$ for minimally transitive permutation groups

Theorem (T., 2015 (CFSG))

Let G be a minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n) + 1$.

Question

Let G be a minimally transitive permutation group of degree $n \geq 2$. Is $d_I(G) \leq \mu(n) + 1$?

$d_I(G)$ for completely reducible linear groups

Theorem (Kovács; Robinson, 1989 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then $d(G) \leq \frac{3}{2}n$.

$d_l(G)$ for completely reducible linear groups

Theorem (Kovács; Robinson, 1989 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then $d(G) \leq \frac{3}{2}n$.

Theorem (Holt; Roney-Dougal, 2013 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. If $\mathbb{F}$ does not contain a primitive fourth root of unity then $d(G) \leq n$. Furthermore, if $|\mathbb{F}| = 2$ then $d(G) \leq \frac{n}{2}$ (apart from one infinite family of exceptions $B_n \leq GL_2(2)^{\frac{n}{2}}$ where $d(B_n) = \frac{n}{2} + 1$).

$d_I(G)$ for completely reducible linear groups

Theorem (Kovács; Robinson, 1989 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then $d(G) \leq \frac{3}{2}n$.

Theorem (T., 2015 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then

(i) $d_I(G) \leq \frac{3}{2}n$.

$d_I(G)$ for completely reducible linear groups

Theorem (Holt; Roney-Dougal, 2013 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. If $\mathbb{F}$ does not contain a primitive fourth root of unity then $d(G) \leq n$. Furthermore, if $|\mathbb{F}| = 2$ then $d(G) \leq \frac{n}{2}$ (apart from one infinite family of exceptions B_n where $d(B_n) = \frac{n}{2} + 1$).

Theorem (T., 2015 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then

(i) $d_I(G) \leq \frac{3}{2}n$;

(ii) *If $|\mathbb{F}| = 2$ then $d_I(G) \leq \frac{n}{2}$ (apart from one infinite family of exceptions $B_n \leq GL_2(2)^{\frac{n}{2}}$ where $d_I(B_n) = \frac{n}{2} + 1$, and when $G = Sp_4(2) \cong S_6$, where $d_I(G) = 3$).*

$d_I(G)$ for completely reducible linear groups

Theorem (Holt; Roney-Dougal, 2013 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. If $\mathbb{F}$ does not contain a primitive fourth root of unity then $d(G) \leq n$. Furthermore, if $|\mathbb{F}| = 2$ then $d(G) \leq \frac{n}{2}$ (apart from one infinite family of exceptions B_n where $d(B_n) = \frac{n}{2} + 1$).

Theorem (T., 2015 (CFSG))

Let $\mathbb{F}$ be a field, and let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then

(i) $d_I(G) \leq \frac{3}{2}n$;

(ii) *If $|\mathbb{F}| = 2$ then $d_I(G) \leq \frac{n}{2}$ (apart from one infinite family of exceptions $B_n \leq GL_2(2)^{\frac{n}{2}}$ where $d_I(B_n) = \frac{n}{2} + 1$, and when $G = Sp_4(2) \cong S_6$, where $d_I(G) = 3$), and;*

(iii) *If $|\mathbb{F}| = 3$ then $d_I(G) \leq n$.*