Generating simple groups and their subgroups

Tim Burness

Permutation Groups Workshop
Banff International Research Station
November 16th 2016

University of BRISTOL

Introduction

Let G be a finite group and define

$$d(G) = \min\{|S| \,:\, G = \langle S \rangle\}$$

Introduction

Let G be a finite group and define

$$d(G) = \min\{|S| \, : \, G = \langle S \rangle\}$$

Note that subgroups may need many more generators, e.g.

$$(Z_2)^n \cong \langle (1,2), (3,4), \ldots, (2n-1, 2n) \rangle < S_{2n}$$

Lemma. If $H \leqslant G$ then $d(H) \leqslant [G:H] \cdot (d(G)-1)+1$

Introduction

Let G be a finite group and define

$$d(G) = \min\{|S| \, : \, G = \langle S \rangle\}$$

Note that subgroups may need many more generators, e.g.

$$(Z_2)^n \cong \langle (1,2), (3,4), \ldots, (2n-1, 2n) \rangle < S_{2n}$$

Lemma. If $H \leqslant G$ then $d(H) \leqslant [G : H] \cdot (d(G) - 1) + 1$

Example. Let p be a prime, $n \geqslant 2$ and consider

$$G = Z_n \wr Z_p = (Z_n)^p \rtimes Z_p \qquad H = (Z_n)^p$$

Then $H < G$ is maximal, $d(G) = 2$ and $d(H) = p = [G : H]$.

Simple groups

Theorem (Steinberg, 1962)

Every finite simple group is 2-generated.

Example. If $n \geqslant 2$ and $q > 3$ then $\mathrm{SL}_n(q) = \langle x, y \rangle$, where

$$x = \left(\begin{array}{cc|c} \mu & & \\ & \mu^{-1} & \\ \hline & & I_{n-2} \end{array}\right), \quad y = \left(\begin{array}{cc|c} 1 & 1 & \\ 0 & 1 & \\ \hline & & I_{n-2} \end{array}\right) \left(\begin{array}{c|c} & 1 \\ \hline -I_{n-1} & \end{array}\right)$$

and $\mathbb{F}_q^\times = \langle \mu \rangle$.

Simple groups

Theorem (Steinberg, 1962)

Every finite simple group is 2-generated.

Example. If $n \geqslant 2$ and $q > 3$ then $\mathrm{SL}_n(q) = \langle x, y \rangle$, where

$$x = \left(\begin{array}{cc|c} \mu & & \\ & \mu^{-1} & \\ \hline & & I_{n-2} \end{array}\right), \quad y = \left(\begin{array}{cc|c} 1 & 1 & \\ 0 & 1 & \\ \hline & & I_{n-2} \end{array}\right) \left(\begin{array}{c|c} & 1 \\ \hline -I_{n-1} & \end{array}\right)$$

and $\mathbb{F}_q^\times = \langle \mu \rangle$.

G is **almost simple** if $T \leqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple T.

Theorem (Dalla Volta & Lucchini, 1995)

Every almost simple group is 3-generated.

Maximal subgroups

Question. Is there a constant c such that $d(H) \leqslant c$ for all maximal subgroups H of finite simple groups?

Maximal subgroups

Question. Is there a constant c such that $d(H) \leqslant c$ for all maximal subgroups H of finite simple groups?

Theorem (B, Liebeck & Shalev, 2013)

Every maximal subgroup of a finite simple group is 4-generated.

- This is best possible – there are infinitely many examples for which 4 generators are needed.
- Maximal subgroups of **almost simple** groups are 6-generated.

Maximal subgroups

Question. Is there a constant c such that $d(H) \leqslant c$ for all maximal subgroups H of finite simple groups?

Theorem (B, Liebeck & Shalev, 2013)

Every maximal subgroup of a finite simple group is 4-generated.

- This is best possible – there are infinitely many examples for which 4 generators are needed.
- Maximal subgroups of **almost simple** groups are 6-generated.
- The maximal subgroups H of a given simple group are not known in general. More precisely, either H is 'known', or H is almost simple.

  For H almost simple, $d(H) \leqslant 3$ by Dalla Volta & Lucchini.

Application: Primitive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabiliser G_α, so

$$d(G) - 1 \leqslant d(G_\alpha) \leqslant [G : G_\alpha] \cdot (d(G) - 1) + 1$$

Question. Is there a constant c such that $d(G_\alpha) \leqslant d(G) + c$?

Application: Primitive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabiliser G_α, so

$$d(G) - 1 \leqslant d(G_\alpha) \leqslant [G : G_\alpha] \cdot (d(G) - 1) + 1$$

Question. Is there a constant c such that $d(G_\alpha) \leqslant d(G) + c$?

Theorem. $d(G_\alpha) \leqslant d(G) + 4$

Application: Primitive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabiliser G_α, so

$$d(G) - 1 \leqslant d(G_\alpha) \leqslant [G : G_\alpha] \cdot (d(G) - 1) + 1$$

Question. Is there a constant c such that $d(G_\alpha) \leqslant d(G) + c$?

Theorem. $d(G_\alpha) \leqslant d(G) + 4$

Example. If G has a regular normal subgroup N then $G/N \cong G_\alpha$ and thus $d(G_\alpha) = d(G/N) \leqslant d(G)$.

Example. If G is almost simple then $d(G_\alpha) \leqslant 6 \leqslant d(G) + 4$.

Example: Alternating groups

Let H be a maximal subgroup of S_n or A_n.

Lemma. We have

$$d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$$

so $d(H) \leqslant 3$ if H is not a diagonal-type subgroup.

Example: Alternating groups

Let H be a maximal subgroup of S_n or A_n.

Lemma. We have

$$d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$$

so $d(H) \leqslant 3$ if H is not a diagonal-type subgroup.

Suppose $H = T^k.(\mathrm{Out}(T) \times S_k)$ is diagonal (T simple). Then

$$d(H) = \max\{2, d(\mathrm{Out}(T) \times S_k)\} \leqslant 4$$

by a theorem of Lucchini & Menegazzo (1997).

Example: Alternating groups

Let H be a maximal subgroup of S_n or A_n.

Lemma. We have

$$d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$$

so $d(H) \leqslant 3$ if H is not a diagonal-type subgroup.

Suppose $H = T^k.(\mathrm{Out}(T) \times S_k)$ is diagonal (T simple). Then

$$d(H) = \max\{2, d(\mathrm{Out}(T) \times S_k)\} \leqslant 4$$

by a theorem of Lucchini & Menegazzo (1997).

Example. If $T = \mathrm{P}\Omega_{12}^{+}(p^{2f})$, $p > 2$, then $H = T^2.(\mathrm{Out}(T) \times S_2) < A_n$ is maximal (with $n = |T|$) and

$$d(H) = \max\{2, d(\mathrm{Out}(T) \times S_2)\} = d(D_8 \times Z_{2f} \times Z_2) = 4.$$

Going deeper in the subgroup lattice

The **depth** of a subgroup $H \leqslant G$ is the maximal length of a chain of subgroups from H to G, e.g. H is maximal iff it has depth 1.

We say H is **second maximal** if it has depth 2, and so on.

Going deeper in the subgroup lattice

The **depth** of a subgroup $H \leqslant G$ is the maximal length of a chain of subgroups from H to G, e.g. H is maximal iff it has depth 1.

We say H is **second maximal** if it has depth 2, and so on.

Theorem (B, Liebeck & Shalev, 2016)

There is a constant c s.t. $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups G with $\mathrm{soc}(G) \notin \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}$.

Going deeper in the subgroup lattice

The **depth** of a subgroup $H \leqslant G$ is the maximal length of a chain of subgroups from H to G, e.g. H is maximal iff it has depth 1.

We say H is **second maximal** if it has depth 2, and so on.

Theorem (B, Liebeck & Shalev, 2016)

There is a constant c s.t. $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups G with $\mathrm{soc}(G) \notin \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}$.

- We can take $c = 12$, unless G is exceptional and H is maximal in a parabolic subgroup of G (here we take $c = 70$).

Going deeper in the subgroup lattice

The **depth** of a subgroup $H \leqslant G$ is the maximal length of a chain of subgroups from H to G, e.g. H is maximal iff it has depth 1.

We say H is **second maximal** if it has depth 2, and so on.

Theorem (B, Liebeck & Shalev, 2016)

There is a constant c s.t. $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups G with $\mathrm{soc}(G) \notin \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}$.

- We can take $c = 12$, unless G is exceptional and H is maximal in a parabolic subgroup of G (here we take $c = 70$).
- There is a second maximal subgroup H of a simple group G with $d(H) = 74\,207\,281$.

Going deeper in the subgroup lattice

The **depth** of a subgroup $H \leqslant G$ is the maximal length of a chain of subgroups from H to G, e.g. H is maximal iff it has depth 1.

We say H is **second maximal** if it has depth 2, and so on.

Theorem (B, Liebeck & Shalev, 2016)

There is a constant c s.t. $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups G with $\mathrm{soc}(G) \not\in \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}$.

- We can take $c = 12$, unless G is exceptional and H is maximal in a parabolic subgroup of G (here we take $c = 70$).
- There is a second maximal subgroup H of a simple group G with $d(H) = 74\,207\,281$. Take $q = 2^{74207281}$ and

$$H = (Z_2)^{74207281} < B = (Z_2)^{74207281} \rtimes Z_{q-1} < G = \mathrm{L}_2(q).$$

Second maximals and special primes

Question. Is there a constant c such that $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups?

Second maximals and special primes

Question. Is there a constant c such that $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups?

This turns out to be **equivalent** to the following formidable open problem in Number Theory:

Question. Are there only finitely many primes r for which there is a prime power q such that $(q^r - 1)/(q - 1)$ is prime?

Second maximals and special primes

Question. Is there a constant c such that $d(H) \leqslant c$ for all second maximal subgroups H of almost simple groups?

This turns out to be **equivalent** to the following formidable open problem in Number Theory:

Question. Are there only finitely many primes r for which there is a prime power q such that $(q^r - 1)/(q - 1)$ is prime?

The answer is believed to be **no**, but existing methods in Number Theory are very far from proving this.

e.g. the answer is **no** if there are infinitely many Mersenne primes.

Third maximals

Theorem. For each $c \in \mathbb{N}$, there exists a third maximal subgroup H of an almost simple group such that $d(H) > c$.

Third maximals

Theorem. For each $c \in \mathbb{N}$, there exists a third maximal subgroup H of an almost simple group such that $d(H) > c$.

Example. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$ and set $n = 2(p+1)$.

Third maximals

Theorem. For each $c \in \mathbb{N}$, there exists a third maximal subgroup H of an almost simple group such that $d(H) > c$.

Example. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$ and set $n = 2(p+1)$. Then

$$G = S_n > S_2 \wr S_{p+1}$$

Third maximals

Theorem. For each $c \in \mathbb{N}$, there exists a third maximal subgroup H of an almost simple group such that $d(H) > c$.

Example. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$ and set $n = 2(p+1)$. Then

$$G = S_n > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p)$$

Third maximals

Theorem. For each $c \in \mathbb{N}$, there exists a third maximal subgroup H of an almost simple group such that $d(H) > c$.

Example. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$ and set $n = 2(p+1)$. Then

$$G = S_n > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p) > (S_2)^{p+1}.S_4 = H$$

Third maximals

Theorem. For each $c \in \mathbb{N}$, there exists a third maximal subgroup H of an almost simple group such that $d(H) > c$.

Example. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$ and set $n = 2(p+1)$. Then

$$G = S_n > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p) > (S_2)^{p+1}.S_4 = H$$

is a third maximal subgroup and

$$d(H) > \frac{d((S_2)^{p+1}) - 1}{24} = \frac{p}{24}$$

[The first inequality holds since $[H : (S_2)^{p+1}] = 24$.]

Main ingredients

Let $H < M < G$ be **second maximal** with G almost simple.

- If M is almost simple then $d(H) \leqslant 6$ by [BLS, 2013]

Main ingredients

Let $H < M < G$ be **second maximal** with G almost simple.

- If M is almost simple then $d(H) \leqslant 6$ by [BLS, 2013]

- If $\mathrm{core}_M(H) = \bigcap_{m \in M} H^m = 1$, then M acts faithfully and primitively on the cosets M/H, so

$$d(H) \leqslant d(M) + 4 \leqslant 10$$

by [BLS, 2013]

Main ingredients

Let $H < M < G$ be **second maximal** with G almost simple.

- If M is almost simple then $d(H) \leqslant 6$ by [BLS, 2013]
- If $\mathrm{core}_M(H) = \bigcap_{m \in M} H^m = 1$, then M acts faithfully and primitively on the cosets M/H, so

  $$d(H) \leqslant d(M) + 4 \leqslant 10$$

  by [BLS, 2013]
- **Remaining cases.** Study the possibilities for H using work of Aschbacher, Liebeck, O'Nan, Scott, Seitz and others.

Example

Suppose $H < M < G$, where $G = S_n$ and $M = S_k \wr S_t = N.S_t$ with $N = (S_k)^t$ and $k \geqslant 5$.

1. $N \leqslant H$: Here $H = N.J$ with $J < S_t$ maximal.

   Now $d(J) \leqslant 4$ and J has $\ell \leqslant 2$ orbits on $\{1, \ldots, t\}$, so

$$d(H) \leqslant d((S_k)^{\ell}) + d(J) \leqslant 6$$

Example

Suppose $H < M < G$, where $G = S_n$ and $M = S_k \wr S_t = N.S_t$ with $N = (S_k)^t$ and $k \geqslant 5$.

1. $N \leqslant H$: Here $H = N.J$ with $J < S_t$ maximal.

   Now $d(J) \leqslant 4$ and J has $\ell \leqslant 2$ orbits on $\{1, \dots, t\}$, so

   $$d(H) \leqslant d((S_k)^\ell) + d(J) \leqslant 6$$

2. $N \not\leqslant H$: Here $H = (H \cap N).S_t$.

   We may assume H contains $A = (A_k)^t$, so $H/A < M/A = S_2 \wr S_t$ is maximal. One checks that $d(H/A) \leqslant 6$, so

   $$d(H) \leqslant d(A_k) + 6 = 8$$

Application: Subgroup growth

Let G be a finite group, $k, n \in \mathbb{N}$.

$$\mathcal{M}_1(G) = \{H : H < G \text{ is maximal}\}$$

Application: Subgroup growth

Let G be a finite group, $k, n \in \mathbb{N}$.

$$\begin{aligned} \mathcal{M}_1(G) &= \{H : H < G \text{ is maximal}\} \\ \mathcal{M}_k(G) &= \{H : H < G \text{ has depth } k\} \\ m_{k,n}(G) &= \#\{H \in \mathcal{M}_k(G) : [G : H] = n\} \end{aligned}$$

Application: Subgroup growth

Let G be a finite group, $k, n \in \mathbb{N}$.

$$\mathcal{M}_1(G) = \{H : H < G \text{ is maximal}\}$$

$$\mathcal{M}_k(G) = \{H : H < G \text{ has depth } k\}$$

$$m_{k,n}(G) = \#\{H \in \mathcal{M}_k(G) : [G : H] = n\}$$

Theorem (Lubotzky 2002; Jaikin-Zapirain & Pyber, 2011)

There exists a constant $\alpha \in \mathbb{N}$ such that

$$m_{1,n}(G) \leqslant n^{\alpha d(G) + \delta(G)}$$

for all finite groups G and all $n \in \mathbb{N}$, where $\delta(G) \geqslant 0$ is a parameter defined in terms of the non-abelian chief factors of G.

$$m_{1,n}(G) \leqslant n^{\alpha d(G)+\delta(G)}$$

Corollary. Almost simple groups have polynomial maximal and second maximal subgroup growth.

i.e. for $k = 1, 2$ there is a constant c such that $m_{k,n}(G) \leqslant n^c$ for all almost simple groups G and all n.

$$m_{1,n}(G) \leqslant n^{\alpha d(G)+\delta(G)}$$

Corollary. Almost simple groups have polynomial maximal and second maximal subgroup growth.

i.e. for $k = 1, 2$ there is a constant c such that $m_{k,n}(G) \leqslant n^c$ for all almost simple groups G and all n.

Fact. For G almost simple, $\delta(G) \leqslant 1$ and $\delta(M) \leqslant 1$ for all $M \in \mathcal{M}_1(G)$.

Setting $c = 6\alpha + 1$ we get

$$m_{1,n}(G) \leqslant n^{\alpha d(G)+\delta(G)}$$

Corollary. Almost simple groups have polynomial maximal and second maximal subgroup growth.

i.e. for $k = 1, 2$ there is a constant c such that $m_{k,n}(G) \leqslant n^c$ for all almost simple groups G and all n.

Fact. For G almost simple, $\delta(G) \leqslant 1$ and $\delta(M) \leqslant 1$ for all $M \in \mathcal{M}_1(G)$.

Setting $c = 6\alpha + 1$ we get

$$m_{2,n}(G) \leqslant \sum_{a|n} m_{1,a}(G) \max\{m_{1,n/a}(M) \,:\, M \in \mathcal{M}_1(G),\, [G:M] = a\}$$

$$m_{1,n}(G) \leqslant n^{\alpha d(G)+\delta(G)}$$

Corollary. Almost simple groups have polynomial maximal and second maximal subgroup growth.

i.e. for $k = 1, 2$ there is a constant c such that $m_{k,n}(G) \leqslant n^c$ for all almost simple groups G and all n.

Fact. For G almost simple, $\delta(G) \leqslant 1$ and $\delta(M) \leqslant 1$ for all $M \in \mathcal{M}_1(G)$.

Setting $c = 6\alpha + 1$ we get

$$\begin{aligned} m_{2,n}(G) &\leqslant \sum_{a|n} m_{1,a}(G) \max\{m_{1,n/a}(M) \,:\, M \in \mathcal{M}_1(G),\, [G : M] = a\} \\ &\leqslant \sum_{a|n} a^c (n/a)^c \\ &\leqslant n^{c+1} \end{aligned}$$

Third maximals

The result can be extended to **third maximal** subgroups.

Theorem. Almost simple groups have polynomial third maximal subgroup growth.

Third maximals

The result can be extended to **third maximal** subgroups.

Theorem. Almost simple groups have polynomial third maximal subgroup growth.

For example, $\delta(M) \leqslant 1$ for all $M \in \mathcal{M}_2(G)$, so if we assume

$$\mathrm{soc}(G) \notin \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}$$

then

$$m_{3,n}(G) \leqslant n^{c+1}$$

with $c = 70\alpha + 1$.

Third maximals

The result can be extended to **third maximal** subgroups.

Theorem. Almost simple groups have polynomial third maximal subgroup growth.

For example, $\delta(M) \leqslant 1$ for all $M \in \mathcal{M}_2(G)$, so if we assume

$$\mathrm{soc}(G) \notin \{\mathrm{L}_2(q), {}^2B_2(q), {}^2G_2(q)\}$$

then

$$m_{3,n}(G) \leqslant n^{c+1}$$

with $c = 70\alpha + 1$.

Question. For each $t \in \mathbb{N}$, do almost simple groups have polynomial t-maximal subgroup growth?


Workshop on Permutation Groups:
Methods and Applications
Michael Giudici (University of Western Australia)
Thomas Gobet (Nancy-Université)
Martin Liebeck (Imperial College)
Kay Magaard (University of Birmingham)
Gunter Malle (TU Kaiserslautern)
Atilla Maróti (Rényi Institute)
Alice Niemeyer (RWTH Aachen)
Benjamin Nill (University of Magdeburg)
Cheryl Praeger (University of Western Australia)
László Pyber (Rényi Institute)
Colva Roney-Dougal (University of St Andrews)
Aner Shalev (Hebrew University of Jerusalem)
Katrin Tent (University of Münster)
Gareth Tracey (University of Warwick)
January 12th-14th, 2017
Bielefeld University
Kovalevskaya Lecture:
Donna Testerman (EPFL)
On January 14th:
Celebration in honour of the
80th birthday of Bernd Fischer
Organisers: Barbara Baumeister, Tim Burness, Hung Tong-Viet
www.math.uni-bielefeld.de/~baumeist/wop2017
SFB 701
Sonderforschungsbereich 701
Universität Bielefeld