Simple groups, generation and probabilistic methods

Tim Burness

Groups St Andrews
University of Birmingham

August 6th 2017

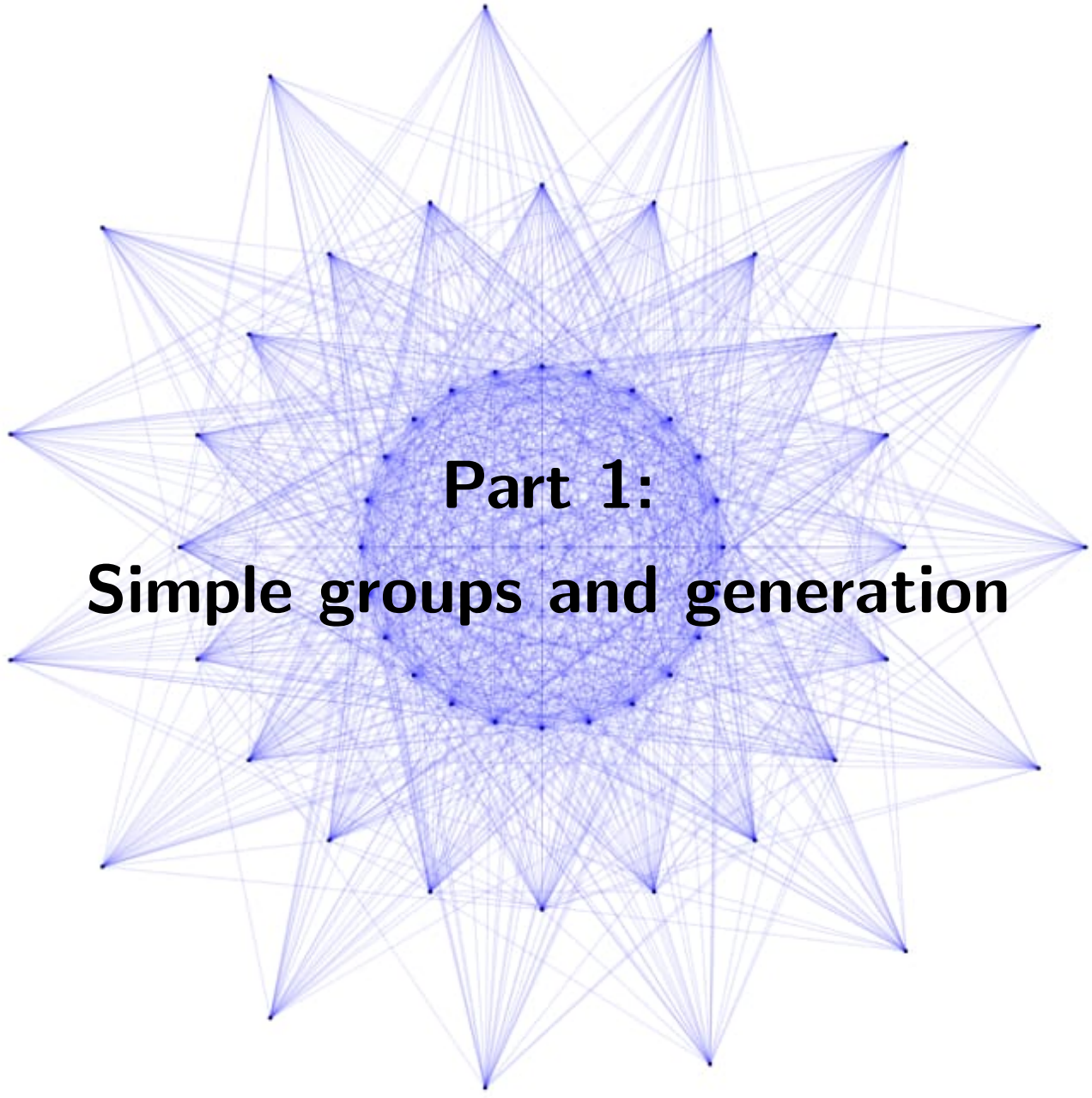
Overview

1: Introduction: Simple groups and generation

2: Generating subgroups of simple groups

3: $\frac{3}{2}$-generation, spread and probabilistic methods

4: The generating graph of a finite group



Part 1:
Simple groups and generation

Let G be a finite group and define

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

Let G be a finite group and define

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

Note. Subgroups may need many more generators!

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

Let G be a finite group and define

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

Note. Subgroups may need many more generators!

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

Example. Let $p \geqslant 3$ be a prime and consider

$$G = (Z_2)^{p+1} \rtimes Z_p \text{ and } H = (Z_2)^{p+1}$$

Then $H < G$ is maximal, $d(G) = 2$ and $d(H) = p + 1 = [G : H] + 1$.

Let G be a finite group and define

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

Note. Subgroups may need many more generators!

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

Example. Let $p \geqslant 3$ be a prime and consider

$$G = (Z_2)^{p+1} \rtimes Z_p \text{ and } H = (Z_2)^{p+1}$$

Then $H < G$ is maximal, $d(G) = 2$ and $d(H) = p + 1 = [G : H] + 1$.

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

Theorem (Steinberg, 1962). *Finite simple groups are 2-generated.*

Example. $A_n = \langle (1,2,3), (k, k+1, \ldots, n) \rangle$ with $k = 1$ or 2.

Example. If $q \geqslant 4$ then

$$\mathsf{SL}_2(q) = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

where $\mathbb{F}_q^\times = \langle \alpha \rangle$.

Theorem (Steinberg, 1962). *Finite simple groups are* 2*-generated.*

Example. $A_n = \langle (1,2,3), (k, k+1, \ldots, n) \rangle$ with $k = 1$ or 2.

Example. If $q \geqslant 4$ then

$$\mathsf{SL}_2(q) = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

where $\mathbb{F}_q^\times = \langle \alpha \rangle$.

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.*

Let $P_k(G)$ be the probability that k random elements generate G.

Let $P_k(G)$ be the probability that k random elements generate G.

Theorem. *For a non-abelian simple group G:*

(a) $P_2(G) \geqslant 53/90$ [Menezes, Quick & Roney-Dougal, 2013]

Let $P_k(G)$ be the probability that k random elements generate G.

Theorem. *For a non-abelian simple group G:*

(a) $P_2(G) \geqslant 53/90$ [Menezes, Quick & Roney-Dougal, 2013]

(b) $P_2(G) \to 1$ *as* $|G| \to \infty$ [Liebeck & Shalev, 1995]

Let $P_k(G)$ be the probability that k random elements generate G.

Theorem. *For a non-abelian simple group G:*

(a) $P_2(G) \geqslant 53/90$ [Menezes, Quick & Roney-Dougal, 2013]

(b) $P_2(G) \to 1$ *as* $|G| \to \infty$ [Liebeck & Shalev, 1995]

Main idea. Let $\mathcal{M}$ be the set of maximal subgroups of G and suppose $x, y \in G$ are randomly chosen.

If $G \neq \langle x, y \rangle$ then $x, y \in H$ for some $H \in \mathcal{M}$, and the probability of this event is $|H|^2/|G|^2 = [G : H]^{-2}$.

Let $P_k(G)$ be the probability that k random elements generate G.

Theorem. *For a non-abelian simple group G:*

(a) $P_2(G) \geqslant 53/90$ [Menezes, Quick & Roney-Dougal, 2013]

(b) $P_2(G) \to 1$ *as* $|G| \to \infty$ [Liebeck & Shalev, 1995]

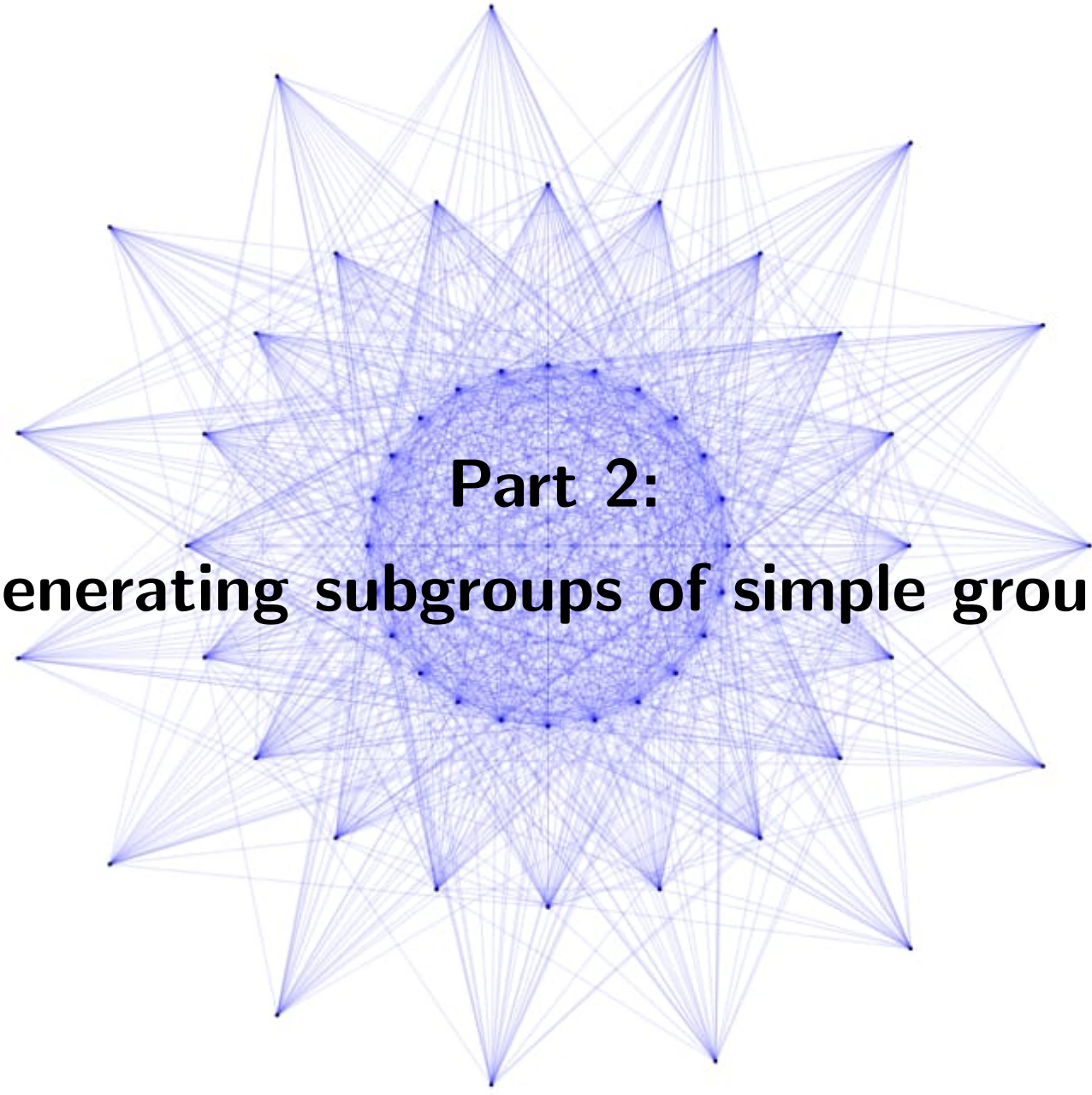
Main idea. Let $\mathcal{M}$ be the set of maximal subgroups of G and suppose $x, y \in G$ are randomly chosen.

If $G \neq \langle x, y \rangle$ then $x, y \in H$ for some $H \in \mathcal{M}$, and the probability of this event is $|H|^2/|G|^2 = [G : H]^{-2}$.

Therefore,

$$1 - P_2(G) \leqslant \sum_{H \in \mathcal{M}} [G : H]^{-2} =: Q(G)$$

Now study $\mathcal{M}$ and show that $Q(G) \to 0$ as $|G| \to \infty$.



Part 2:
Generating subgroups of simple groups

Maximal subgroups

Question. Is there a constant c such that $d(H) \leqslant c$ for every maximal subgroup H of a finite simple group?

Maximal subgroups

Question. Is there a constant c such that $d(H) \leqslant c$ for every maximal subgroup H of a finite simple group?

Theorem (B, Liebeck & Shalev, 2013).

(a) *Every maximal subgroup of a simple group is 4-generated.*

(b) *Given $\epsilon > 0$, there exists $k = k(\epsilon)$ such that $P_k(H) > 1 - \epsilon$ for any maximal subgroup H of any simple group.*

- In (a), infinitely many examples need 4 generators.
- The example $H = S_{n-2} < A_n$ shows that (b) is best possible.

Maximal subgroups

Question. Is there a constant c such that $d(H) \leqslant c$ for every maximal subgroup H of a finite simple group?

Theorem (B, Liebeck & Shalev, 2013).

(a) *Every maximal subgroup of a simple group is 4-generated.*

(b) *Given $\epsilon > 0$, there exists $k = k(\epsilon)$ such that $P_k(H) > 1 - \epsilon$ for any maximal subgroup H of any simple group.*

- In (a), infinitely many examples need 4 generators.
- The example $H = S_{n-2} < A_n$ shows that (b) is best possible.

We get $d(H) \leqslant 6$ for any maximal subgroup of an **almost simple** group.

Question. Is the optimal bound $d(H) \leqslant 4$?

Main ingredients

- The maximal subgroups H of a given simple group are not known in general, but there are **powerful reduction theorems**:
  - Alternating groups: O'Nan-Scott theorem
  - Classical groups: Aschbacher's theorem
  - Exceptional groups: Results of Liebeck, Seitz and others

  In particular, either H is 'known', or H is almost simple

Main ingredients

- The maximal subgroups H of a given simple group are not known in general, but there are **powerful reduction theorems**:
  - Alternating groups: O'Nan-Scott theorem
  - Classical groups: Aschbacher's theorem
  - Exceptional groups: Results of Liebeck, Seitz and others

  In particular, either H is 'known', or H is almost simple

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

- For sporadic groups, we consult the $\mathbb{ATLAS}$.

- For random generation (part (b)), we apply a deep theorem of Jaikin-Zapirain & Pyber (2011).

Example

Let H be a maximal subgroup of S_n or A_n.

Lemma. *We have* $d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$. *In particular,* $d(H) \leqslant 3$ *if* H *is non-diagonal.*

Example

Let H be a maximal subgroup of S_n or A_n.

Lemma. *We have* $d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$. *In particular,* $d(H) \leqslant 3$ *if* H *is non-diagonal.*

Suppose $H = T^k.(\mathrm{Out}(T) \times S_k)$ is diagonal ($k \geqslant 2$, T simple). Then

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

by a theorem of Lucchini & Menegazzo (1997), and we get $d(H) \leqslant 4$.

Example

Let H be a maximal subgroup of S_n or A_n.

Lemma. *We have* $d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$. *In particular,* $d(H) \leqslant 3$ *if* H *is non-diagonal.*

Suppose $H = T^k.(\mathrm{Out}(T) \times S_k)$ is diagonal ($k \geqslant 2$, T simple). Then

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

by a theorem of Lucchini & Menegazzo (1997), and we get $d(H) \leqslant 4$.

Example. Suppose $T = \mathrm{P}\Omega^+_{12}(p^2)$, $p \geqslant 3$ and $k = 2$.

Example

Let H be a maximal subgroup of S_n or A_n.

Lemma. *We have* $d(S_k \times S_{n-k}) = d(\mathrm{AGL}_m(p)) = d(S_k \wr S_t) = 2$. *In particular,* $d(H) \leqslant 3$ *if* H *is non-diagonal.*

Suppose $H = T^k.(\mathrm{Out}(T) \times S_k)$ is diagonal ($k \geqslant 2$, T simple). Then

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

by a theorem of Lucchini & Menegazzo (1997), and we get $d(H) \leqslant 4$.

Example. Suppose $T = \mathrm{P}\Omega^+_{12}(p^2)$, $p \geqslant 3$ and $k = 2$.

Then $H = T^2.(\mathrm{Out}(T) \times S_2) < A_n$ is maximal (with $n = |T|$) and

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

Application: Primitive groups

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

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

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

Application: Primitive groups

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

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

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

Theorem. $d(H) \leqslant d(G) + 4$

Application: Primitive groups

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

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

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

Theorem. $d(H) \leqslant d(G) + 4$

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

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

Question. Is $d(H) \leqslant d(G) + 2$ the optimal bound?

Deeper subgroups

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 if and only if it has depth 1.

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

Deeper subgroups

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 if and only if it has depth 1.

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

Question.

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

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

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

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 $c = 70$).

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 $d(H) = \mathbf{74\,207\,281}$:

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 $d(H) = \mathbf{74\,207\,281}$: Take $q = 2^{74207281}$ and

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 $d(H) = \mathbf{74\,207\,281}$: Take $q = 2^{74207281}$ and

$$G = \mathrm{PSL}_2(q)$$

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 $d(H) = \mathbf{74\,207\,281}$: Take $q = 2^{74207281}$ and

$$G = \mathrm{PSL}_2(q) > (Z_2)^{74207281} \rtimes Z_{q-1}$$

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**: Take $q = 2^{74207281}$ and

$$G = \mathrm{PSL}_2(q) > (Z_2)^{74207281} \rtimes Z_{q-1} > (Z_2)^{74207281} = H$$

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]

- **Remaining cases:** Study the possibilities for H using the **reduction theorems** of O'Nan-Scott, Aschbacher, Liebeck-Seitz and others.

Special primes

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

Theorem. *This is equivalent to the following open problem:*

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

Special primes

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

Theorem. *This is equivalent to the following open problem:*

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

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

Note. The answer is **no** if there are infinitely many Mersenne primes.

Third maximals

Lemma. *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

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

Proof. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$.

Third maximals

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

Proof. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$. Then

$$G = S_{2(p+1)} > S_2 \wr S_{p+1}$$

Third maximals

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

Proof. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$. Then

$$G = S_{2(p+1)} > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p)$$

Third maximals

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

Proof. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$. Then

$$G = S_{2(p+1)} > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p) > (S_2)^{p+1}.S_4 = H$$

Third maximals

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

Proof. Let $p \geqslant 5$ be a prime such that $p \equiv \pm 3 \pmod 8$. Then

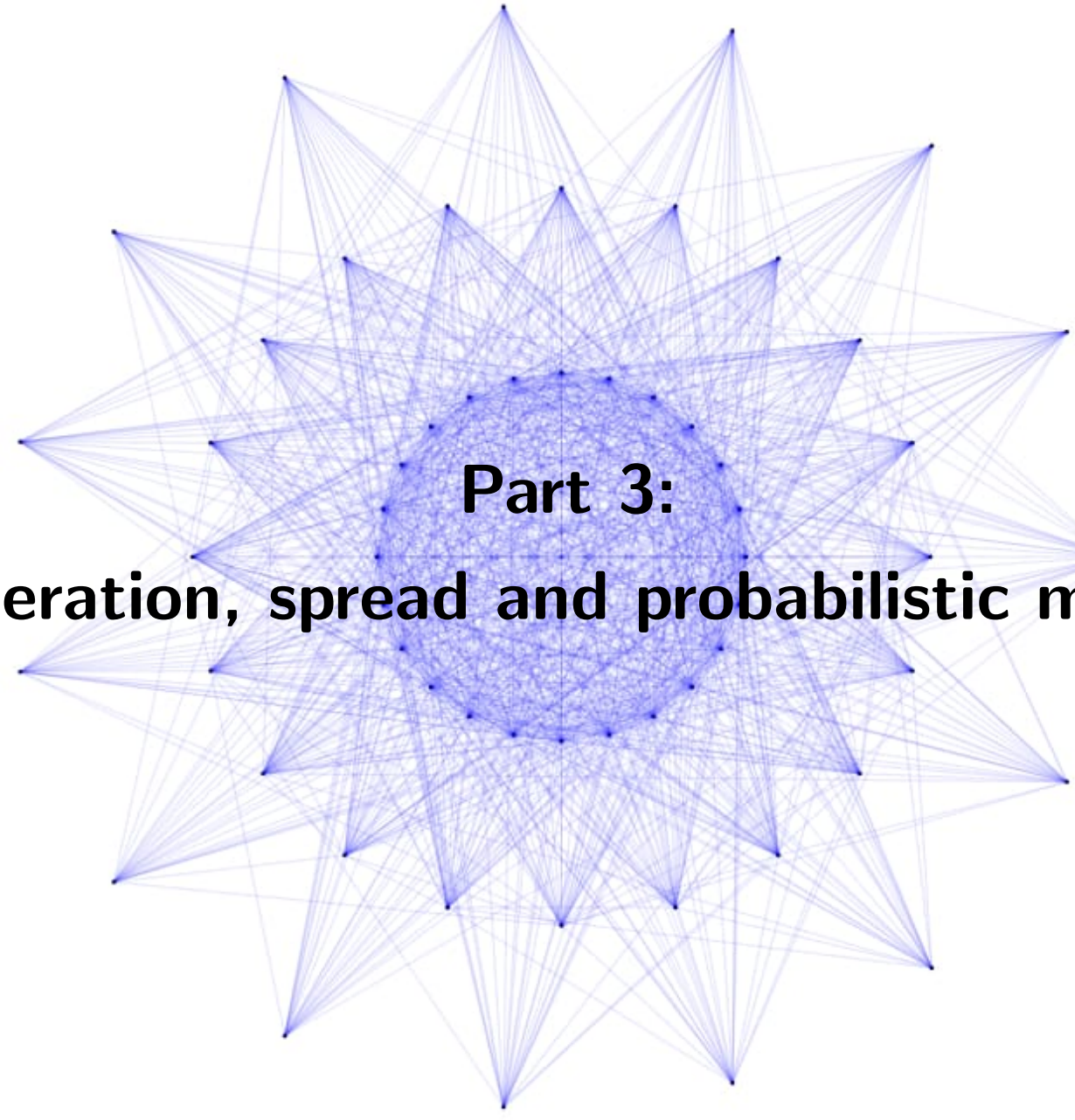
$$G = S_{2(p+1)} > S_2 \wr S_{p+1} > (S_2)^{p+1}.\mathrm{PGL}_2(p) > (S_2)^{p+1}.S_4 = H$$

is a third maximal subgroup and

$$p + 1 = d((S_2)^{p+1}) \leqslant [H : (S_2)^{p+1}] \cdot (d(H) - 1) + 1,$$

so

$$d(H) \geqslant \frac{p}{24} + 1$$



Part 3:

$\frac{3}{2}$-generation, spread and probabilistic methods

G is $\frac{3}{2}$-**generated** if for any $x \in G \setminus \{1\}$ there exists $y \in G$ s.t. $G = \langle x, y \rangle$.

G is $\frac{3}{2}$-**generated** if for any $x \in G \setminus \{1\}$ there exists $y \in G$ s.t. $G = \langle x, y \rangle$.

Theorem (Guralnick & Kantor, 2000).

Every finite simple group is $\frac{3}{2}$-generated.

G is $\frac{3}{2}$-**generated** if for any $x \in G \setminus \{1\}$ there exists $y \in G$ s.t. $G = \langle x, y \rangle$.

Theorem (Guralnick & Kantor, 2000).

Every finite simple group is $\frac{3}{2}$-generated.

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

Let $s(G) \geqslant 0$ be the **exact spread** of G.

G is $\frac{3}{2}$-**generated** if for any $x \in G \setminus \{1\}$ there exists $y \in G$ s.t. $G = \langle x, y \rangle$.

Theorem (Guralnick & Kantor, 2000).

Every finite simple group is $\frac{3}{2}$-generated.

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

Let $s(G) \geqslant 0$ be the **exact spread** of G.

Theorem (Brenner & Wiegold, 1975).

- *For $n \geqslant 4$, $s(A_{2n}) = 4$*

G is $\frac{3}{2}$-**generated** if for any $x \in G \setminus \{1\}$ there exists $y \in G$ s.t. $G = \langle x, y \rangle$.

Theorem (Guralnick & Kantor, 2000).

Every finite simple group is $\frac{3}{2}$*-generated.*

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

Let $s(G) \geqslant 0$ be the **exact spread** of G.

Theorem (Brenner & Wiegold, 1975).

- *For* $n \geqslant 4$, $s(A_{2n}) = 4$
- $6\,098\,892\,799 \leqslant s(A_{19}) \leqslant 6\,098\,892\,803$
- *For* $q \geqslant 4$ *even*, $s(\mathrm{PSL}_2(q)) = q - 2$

Spread for simple groups

Theorem (Guralnick & Shalev, 2003).

Let (G_n) be a sequence of simple groups with $|G_n| \to \infty$. Then either

- $s(G_n) \to \infty$*; or*
- (G_n) *has a subsequence of alternating groups of degree divisible by a fixed prime, or odd-dimensional orthogonal groups over a field of fixed size.*

Spread for simple groups

Theorem (Guralnick & Shalev, 2003).

Let (G_n) be a sequence of simple groups with $|G_n| \to \infty$. Then either

- $s(G_n) \to \infty$*; or*
- (G_n) *has a subsequence of alternating groups of degree divisible by a fixed prime, or odd-dimensional orthogonal groups over a field of fixed size.*

Theorem (Breuer, Guralnick & Kantor, 2008).

$s(G) \geqslant 2$ for every simple group G, with equality iff

$$G = A_5,\ A_6,\ \Omega_8^+(2) \text{ or } \Omega_{2m+1}(2) \text{ with } m \geqslant 3$$

For $x, y \in G$, let

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

be the probability that x and a random conjugate of y do **not** generate G.

For $x, y \in G$, let

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

be the probability that x and a random conjugate of y do **not** generate G.

Lemma. *Suppose there exists $y \in G$ and $k \in \mathbb{N}$ s.t. $Q(x,y) < 1/k$ for all non-trivial $x \in G$. Then $s(G) \geqslant k$.*

For $x, y \in G$, let

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

be the probability that x and a random conjugate of y do **not** generate G.

Lemma. *Suppose there exists $y \in G$ and $k \in \mathbb{N}$ s.t. $Q(x,y) < 1/k$ for all non-trivial $x \in G$. Then $s(G) \geqslant k$.*

Proof. For $x_1, \ldots, x_k \in G \setminus \{1\}$, let E_i be the event that $G = \langle x_i, z\rangle$ for a random conjugate $z \in y^G$. Set $E = E_1 \cap \cdots \cap E_k$.

For $x, y \in G$, let

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

be the probability that x and a random conjugate of y do **not** generate G.

> **Lemma.** *Suppose there exists $y \in G$ and $k \in \mathbb{N}$ s.t. $Q(x,y) < 1/k$ for all non-trivial $x \in G$. Then $s(G) \geqslant k$.*

Proof. For $x_1, \ldots, x_k \in G \setminus \{1\}$, let E_i be the event that $G = \langle x_i, z\rangle$ for a random conjugate $z \in y^G$. Set $E = E_1 \cap \cdots \cap E_k$. Then

$$\mathbb{P}(E) = 1 - \mathbb{P}(\bar{E}_1 \cup \cdots \cup \bar{E}_k) \geqslant 1 - \sum_{i=1}^{k} \mathbb{P}(\bar{E}_i) = 1 - \sum_{i=1}^{k} Q(x_i, y)$$

and thus $\mathbb{P}(E) > 1 - k \cdot \frac{1}{k} = 0$.

For $H < G$ and $x \in G$, let

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

be the **fixed point ratio** of x w.r.t the action of G on G/H.

For $y \in G$, let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y.

For $H < G$ and $x \in G$, let

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

be the **fixed point ratio** of x w.r.t the action of G on G/H.

For $y \in G$, let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y.

Key Lemma. *Suppose there exists $y \in G$ and $k \in \mathbb{N}$ such that*

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

for all $x \in G$ of prime order. Then $s(G) \geqslant k$.

For $H < G$ and $x \in G$, let

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

be the **fixed point ratio** of x w.r.t the action of G on G/H.

For $y \in G$, let $\mathcal{M}(y)$ be the set of maximal subgroups of G containing y.

Key Lemma. *Suppose there exists $y \in G$ and $k \in \mathbb{N}$ such that*

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

for all $x \in G$ of prime order. Then $s(G) \geqslant k$.

Example. $G = A_{19}, |y| = 19 \implies \mathcal{M}(y) = \{H\}$, $H = \mathrm{AGL}_1(19) \cap G$.

$$\text{Then } \max_{1 \neq x \in G} \mathrm{fpr}(x, G/H) = \frac{1}{6098892800} \implies s(G) \geqslant 6098892799$$

Example

Claim. *If $G = A_n$ and $n \geqslant 8$ is even, then $s(G) \geqslant 3$.*

Set $t = n/2 - \gcd(2, n/2 - 1)$ and $y = (1, \ldots, t)(t+1, \ldots, n) \in G$.

Example

Claim. *If $G = A_n$ and $n \geqslant 8$ is even, then $s(G) \geqslant 3$.*

Set $t = n/2 - \gcd(2, n/2 - 1)$ and $y = (1, \ldots, t)(t+1, \ldots, n) \in G$.

- $\mathcal{M}(y) = \{L\}$ with $L = (S_t \times S_{n-t}) \cap G$:
  - Let $H \in \mathcal{M}(y)$. Then H intransitive $\implies$ $H = L$
  - H imprimitive ruled out by cycle-shape of y
  - H primitive ruled out by Marggraff's Theorem (1889) since $\langle y \rangle$ contains a t-cycle and $t < n/2$

Example

Claim. *If $G = A_n$ and $n \geqslant 8$ is even, then $s(G) \geqslant 3$.*

Set $t = n/2 - \gcd(2, n/2 - 1)$ and $y = (1, \ldots, t)(t+1, \ldots, n) \in G$.

- $\mathcal{M}(y) = \{L\}$ with $L = (S_t \times S_{n-t}) \cap G$:
  - Let $H \in \mathcal{M}(y)$. Then H intransitive $\implies$ $H = L$
  - H imprimitive ruled out by cycle-shape of y
  - H primitive ruled out by Marggraff's Theorem (1889) since $\langle y \rangle$ contains a t-cycle and $t < n/2$
- Easy combinatorial argument with t-sets $\implies$ $\mathrm{fpr}(x, G/L) < 1/3$ for all $x \in G$ of prime order
- Now apply the Key Lemma

Conjecture (Breuer, Guralnick & Kantor, 2008).

A finite group G is $\frac{3}{2}$-generated iff G/N is cyclic for every non-trivial normal subgroup N of G.

Note. G/N non-cyclic $\implies$ no element in N belongs to a generating pair

Conjecture (Breuer, Guralnick & Kantor, 2008).

A finite group G is $\frac{3}{2}$-generated iff G/N is cyclic for every non-trivial normal subgroup N of G.

Note. G/N non-cyclic $\implies$ no element in N belongs to a generating pair

- G soluble: Brenner & Wiegold, 1975
- G simple: Guralnick & Kantor, 2000

Conjecture (Breuer, Guralnick & Kantor, 2008).

A finite group G is $\frac{3}{2}$-generated iff G/N is cyclic for every non-trivial normal subgroup N of G.

Note. G/N non-cyclic $\implies$ no element in N belongs to a generating pair

- G soluble: Brenner & Wiegold, 1975
- G simple: Guralnick & Kantor, 2000
- **Guralnick:** A reduction to **almost simple** groups.

  Let $G = \langle T, x \rangle$ be an almost simple group with socle T:

Conjecture (Breuer, Guralnick & Kantor, 2008).

A finite group G is $\frac{3}{2}$-generated iff G/N is cyclic for every non-trivial normal subgroup N of G.

Note. G/N non-cyclic $\implies$ no element in N belongs to a generating pair

- G soluble: Brenner & Wiegold, 1975
- G simple: Guralnick & Kantor, 2000
- **Guralnick:** A reduction to **almost simple** groups.

  Let $G = \langle T, x \rangle$ be an almost simple group with socle T:

  - T alternating or sporadic: Breuer et al., 2008
  - $T = \mathrm{PSL}_n(q)$: B & Guest, 2013
  - $T = \mathrm{PSp}_n(q)$ or $\Omega_n(q)$: Harper, 2017

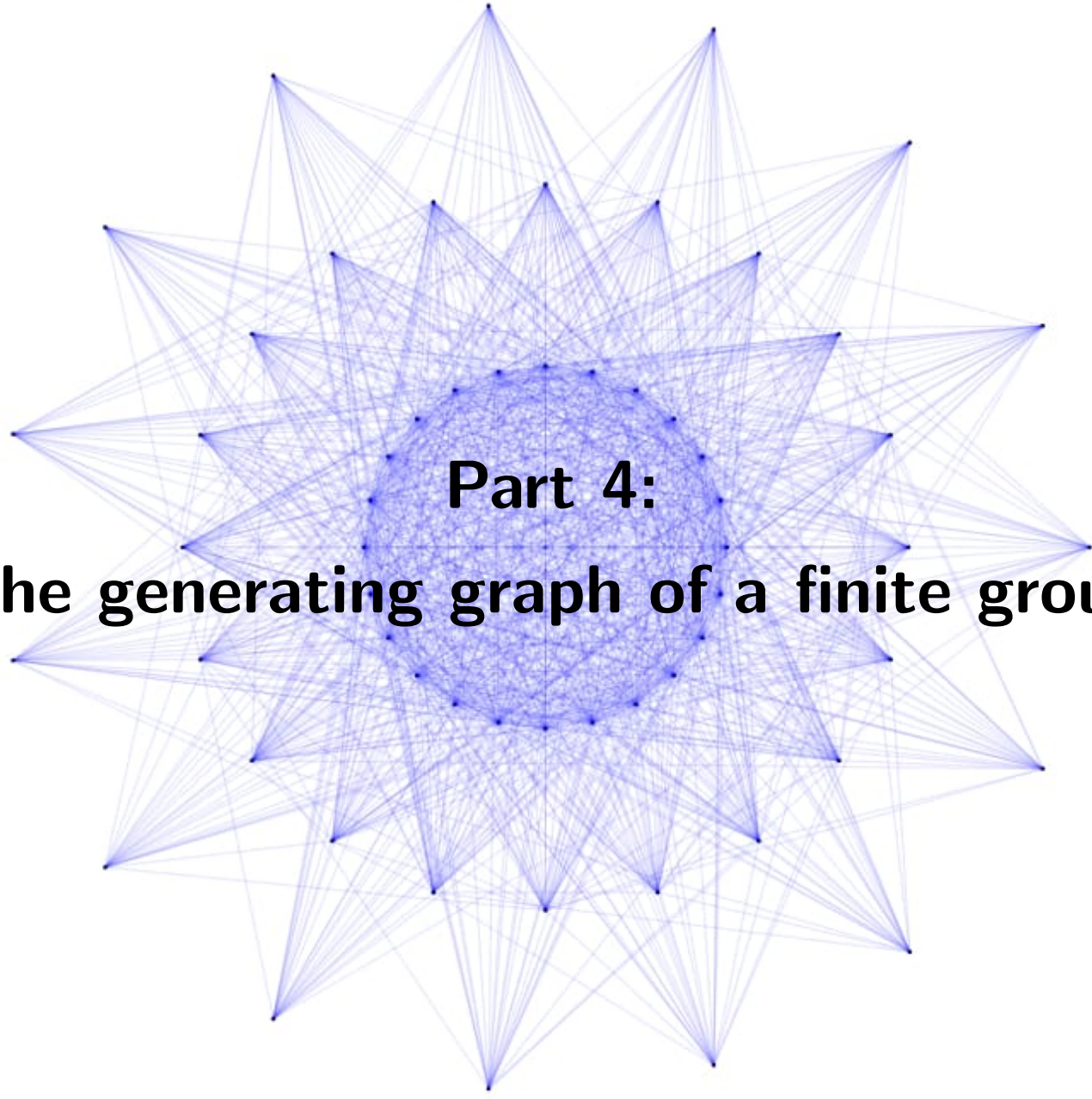
Scott's talk

- **Scott Harper (Bristol)**

  $\frac{3}{2}$-generation of finite groups

- Monday, 14:30–15:00

  Poynting Building, SLT

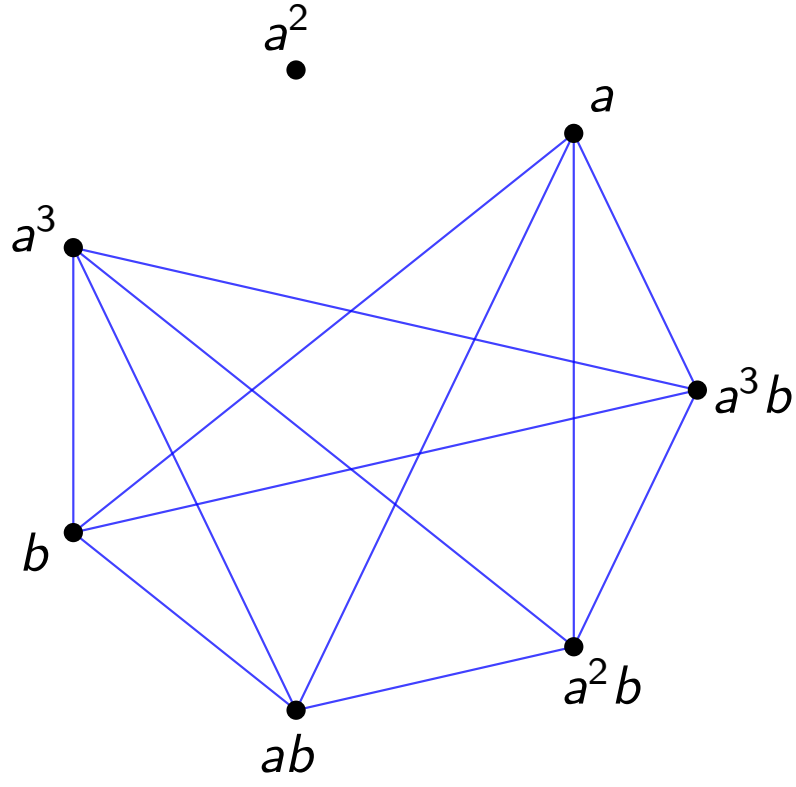


Part 4:
The generating graph of a finite group

Let G be a finite group.

The **generating graph** $\Gamma(G)$ has vertex set $G \setminus \{1\}$ and two vertices x, y are joined by an edge if and only if $G = \langle x, y \rangle$.

Example. $D_8 = \langle a, b \mid a^4 = b^2 = 1,\ ab = ba^{-1} \rangle$:



$\Gamma(G)$ encodes some interesting generation properties of G, e.g.

$$d(G) \leqslant 2 \iff \Gamma(G) \text{ is non-empty}$$
$$s(G) \geqslant 1 \iff \Gamma(G) \text{ has no isolated vertices}$$
$$s(G) \geqslant 2 \implies \Gamma(G) \text{ is connected with diameter at most 2}$$

$\Gamma(G)$ encodes some interesting generation properties of G, e.g.

$$d(G) \leqslant 2 \iff \Gamma(G) \text{ is non-empty}$$
$$s(G) \geqslant 1 \iff \Gamma(G) \text{ has no isolated vertices}$$
$$s(G) \geqslant 2 \implies \Gamma(G) \text{ is connected with diameter at most 2}$$

- What is the **(co)-clique number** of $\Gamma(G)$?
- What is the **chromatic number** of $\Gamma(G)$?
- Does $\Gamma(G)$ contain a **Hamiltonian cycle**? etc. etc.

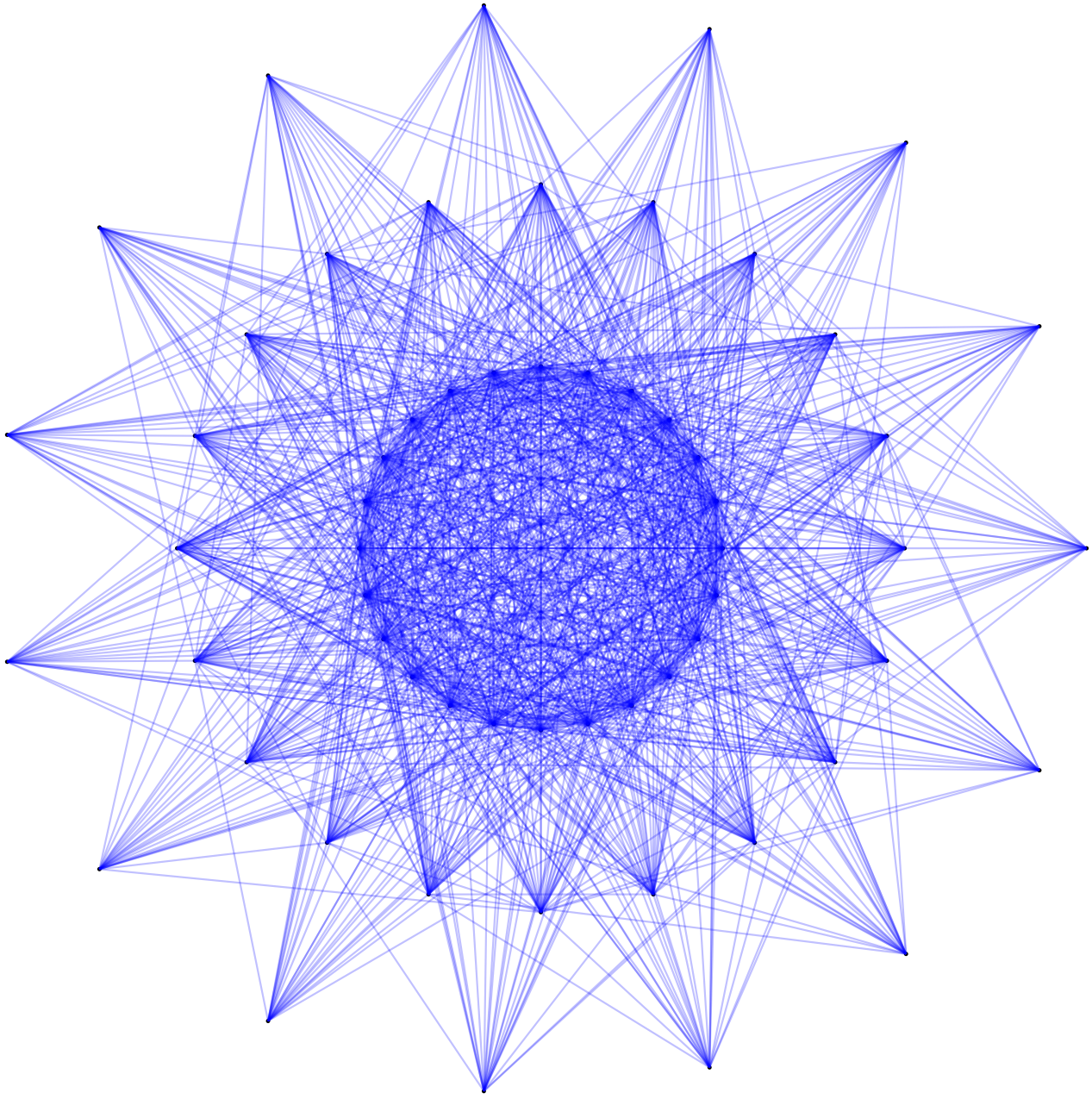
$\Gamma(G)$ encodes some interesting generation properties of G, e.g.

$$d(G) \leqslant 2 \iff \Gamma(G) \text{ is non-empty}$$
$$s(G) \geqslant 1 \iff \Gamma(G) \text{ has no isolated vertices}$$
$$s(G) \geqslant 2 \implies \Gamma(G) \text{ is connected with diameter at most 2}$$

- What is the **(co)-clique number** of $\Gamma(G)$?
- What is the **chromatic number** of $\Gamma(G)$?
- Does $\Gamma(G)$ contain a **Hamiltonian cycle**? etc. etc.

Example. If $G = A_5$ then $\Gamma(G)$ has 59 vertices and 1140 edges.
It has clique number 8, coclique number 15 and chromatic number 9.

The generating graph of A_5



Simple groups

Theorem. *Let G be a non-abelian finite simple group.*

- $\Gamma(G)$ *has no isolated vertices.* [Guralnick & Kantor, 2000]
- $\Gamma(G)$ *is connected and has diameter* 2. [Breuer, Guralnick & Kantor, 2008]
- $\Gamma(G)$ *contains a Hamiltonian cycle if* $|G|$ *is sufficiently large.* [Breuer, Guralnick, Lucchini, Maróti & Nagy, 2010]

Simple groups

Theorem. *Let G be a non-abelian finite simple group.*

- $\Gamma(G)$ *has no isolated vertices.* [Guralnick & Kantor, 2000]
- $\Gamma(G)$ *is connected and has diameter* 2. [Breuer, Guralnick & Kantor, 2008]
- $\Gamma(G)$ *contains a Hamiltonian cycle if* $|G|$ *is sufficiently large.* [Breuer, Guralnick, Lucchini, Maróti & Nagy, 2010]

Conjecture (BGLMN, 2010).

Let G be a finite group with $|G| \geqslant 4$. Then $\Gamma(G)$ is Hamiltonian iff G/N is cyclic for every non-trivial normal subgroup N of G.

Note. Proved in [BGLMN, 2010] for soluble groups.

A generalised conjecture

Conjecture.

The following are equivalent, for any finite group G with $|G| \geqslant 4$:

(a) *G has spread 1.*

(b) *G has spread 2.*

(c) *$\Gamma(G)$ has no isolated vertices.*

(d) *$\Gamma(G)$ is connected.*

(e) *$\Gamma(G)$ is connected with diameter at most 2.*

(f) *$\Gamma(G)$ contains a Hamiltonian cycle.*

(g) *G/N is cyclic for every non-trivial normal subgroup N.*

- This would imply that no finite group has exact spread 1.
- The conjecture is **true** for soluble groups.