Generation and random generation of simple groups

Tim Burness

University of Bristol

Algebra & Combinatorics Seminar
University of Auckland
June 12th 2015

Introduction

Let $n \in \mathbb{N}$. A group G is ***n*-generated** if it can be generated by n elements.

Set $d(G) = \min\{n \in \mathbb{N} : G \text{ is } n\text{-generated}\}$.

Examples

- $d(G) = 1 \iff G$ is cyclic
- If $G = (Z_2)^n = Z_2 \times Z_2 \times \cdots \times Z_2$ (n factors) then $d(G) = n$
- D_{2n} and S_n are 2-generated, e.g.

$$S_n = \langle (1, 2, \ldots, n), (1, 2) \rangle$$

- If $N \leqslant G$ is a normal subgroup, then

$$d(G/N) \leqslant d(G) \leqslant d(G/N) + d(N)$$

- Subgroups may require many more generators, e.g. $(Z_2)^n < S_{2n}$

If $H \leqslant G$ is a finite-index subgroup, then

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

Example: Let p be a prime and take

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

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

Simple groups

By **CFSG**, the nonabelian finite simple groups are as follows:

- Alternating groups A_n, $n \geqslant 5$
- Groups of Lie type (classical and exceptional)
- 26 sporadic groups

Theorem

Every finite simple group is 2-generated

Alternating groups: $A_n = \begin{cases} \langle (1,2,3), (1,2,\ldots,n) \rangle & n \text{ odd} \\ \langle (1,2,3), (2,3,\ldots,n) \rangle & n \text{ even} \end{cases}$

Groups of Lie type: Steinberg, 1962

Sporadic groups: Aschbacher & Guralnick, 1984

Random generation

$$\mathbb{P}(G,k) = \frac{|\{(x_1,\dots,x_k) \in G^k \,:\, G = \langle x_1,\dots,x_k\rangle\}|}{|G|^k}$$

is the probability that k randomly chosen elements generate G.

Netto's conjecture (1882): $\mathbb{P}(A_n, 2) \to 1$ as $n \to \infty$

Theorem (Dixon, 1969)

Netto's conjecture is true

Dixon's conjecture (1969): If (G_n) is any sequence of finite simple groups such that $|G_n| \to \infty$, then $\mathbb{P}(G_n, 2) \to 1$.

Theorem (Kantor & Lubotzky, 1990; Liebeck & Shalev, 1995)

Dixon's conjecture is true

Dixon's conjecture

The proof of Dixon's conjecture is based on an easy observation:

Let $\mathcal{M}$ be the set of maximal subgroups of G and let $x, y \in G$ be randomly chosen elements.

If $G \neq \langle x, y \rangle$ then $x, y \in H$ for some $H \in \mathcal{M}$.

The probability of this event is $[G : H]^{-2}$, so

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

By analysing $\mathcal{M}$, one shows that $Q(G) \to 0$ as $|G| \to \infty$.

Theorem (Menezes, Quick & Roney-Dougal, 2013)

$\mathbb{P}(G, 2) \geqslant 53/90$ *for every finite simple group* G*, with equality iff* $G = A_6$.

Spread

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

- For $x \in G$ and $C = y^G = \{g^{-1}yg \,:\, g \in G\}$, set
$$\mathbb{P}(x, C) = \frac{|\{z \in C \,:\, G = \langle x, z \rangle\}|}{|C|}$$
- If $\mathbb{P}(x, C) > 0$ for all $x \in G \setminus \{1\}$, then G is $\frac{3}{2}$-generated.
- We have
$$1 - \mathbb{P}(x, C) \leqslant \sum_{H \in \mathcal{M}(y)} \frac{|x^G \cap H|}{|x^G|}$$
where $\mathcal{M}(y)$ is the set of maximal subgroups of G containing y.

Spread

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

Let $k \in \mathbb{N}$. Then 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.

Theorem (Breuer, Guralnick & Kantor, 2008)

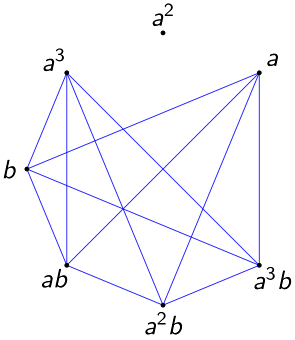
- *Every finite simple group has spread 2*
- *Moreover, every finite simple group has spread 3, except for*

$$A_5,\ A_6,\ \Omega_8^+(2),\ \mathrm{Sp}_{2m}(2)\,(m \geqslant 3)$$

Generating graphs

Let $\Gamma(G)$ be the **generating graph** of G: vertices $G \setminus \{1\}$, with x, y adjacent iff $G = \langle x, y \rangle$.

Example. The generating graph of D_8:



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

Generating graphs of simple groups

Let $\Gamma(G)$ be the **generating graph** of G: vertices $G \setminus \{1\}$, with x, y adjacent iff $G = \langle x, y \rangle$.

Theorem

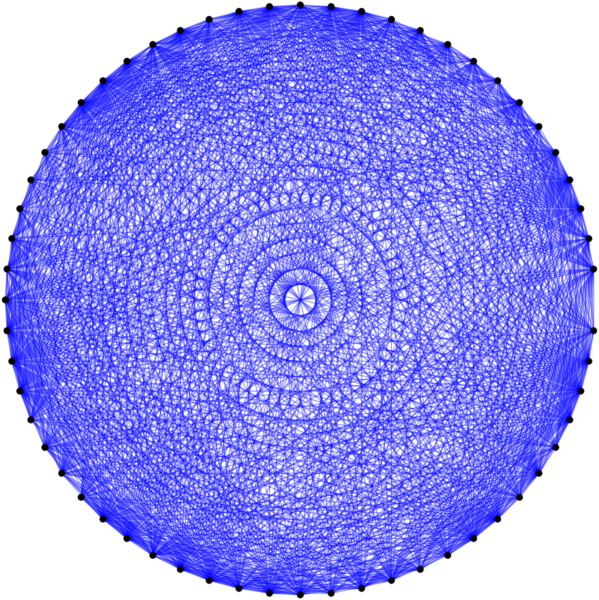
Let G be a nonabelian finite simple group.

- $\Gamma(G)$ *has no isolated vertices*
- $\Gamma(G)$ *is connected and has diameter* 2
- $\Gamma(G)$ *contains a Hamiltonian cycle if* $|G|$ *is sufficiently large*

Questions. What is the (co)-clique number of $\Gamma(G)$? What is its chromatic number? etc.

For $G = A_5$: Clique number $= 8$
Coclique number $= 15$ (note: $|\{x \in G \,:\, |x| = 2\}| = 15$)
Chromatic number $= 9$

The generating graph of A_5



Generating subgroups of simple groups

Joint work with Martin Liebeck (Imperial College London)
and Aner Shalev (Hebrew University of Jerusalem)

The main problem

Question: To what extent can certain generation properties of simple groups be extended to their maximal subgroups?

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

Theorem (B, Liebeck & Shalev, 2013)

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

- This is best possible – there are infinitely many maximal subgroups of simple groups that require 4 generators.
- We establish stronger results for alternating and sporadic groups.
- The maximal subgroups H of a given simple group are not completely known, in general:

  More precisely, either H is 'known', or H is **almost simple**, so

  $$S \leqslant H \leqslant \mathrm{Aut}(S)$$

  for some nonabelian simple group S.
- **Key Observation:** By a theorem of Dalla Volta & Lucchini (1995), every almost simple group is 3-generated.

Alternating groups

Let $G = S_n$ or A_n, and let H be a maximal subgroup of G.

Theorem (O'Nan & Scott, 1979)

One of the following holds:

- $H = (S_k \times S_{n-k}) \cap G$, $1 \leqslant k < n/2$ **[Intransitive]**
- $H = \mathrm{AGL}_d(p) \cap G$, $n = p^d$, p *prime* **[Affine]**
- $H = (S_k \wr S_t) \cap G$, $n = kt$ *or* k^t **[Imprimitive or product type]**
- $H = (T^k.(\mathrm{Out}(T) \times S_k)) \cap G$, T *nonabelian simple*, $n = |T|^{k-1}$ **[Diagonal type]**
- H *is* **almost simple**

Alternating groups

Proposition

We have
$$d(S_k \times S_{n-k}) = d(\mathrm{AGL}_d(p)) = d(S_k \wr S_t) = 2$$
so $d(H) \leqslant 3$ if H is non-diagonal.

Let $H = T^k.(\mathrm{Out}(T) \times S_k)$ be a diagonal-type subgroup.

Here T^k is the unique minimal normal subgroup of H, so by a theorem of Lucchini & Menegazzo (1997) we have

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

Proposition

If H is a maximal subgroup of S_n or A_n, then $d(H) \leqslant 4$, with equality only if H is of diagonal-type.

An example

Let $H = T^2.(\mathrm{Out}(T) \times S_2)$, where $T = \mathrm{P}\Omega^+_{2m}(p^{2f})$ with $m \geqslant 6$ even and p an odd prime. Then

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

Now $L = D_8 \times Z_{2f} \times Z_2$ has a normal subgroup N such that

$$L/N \cong Z_2 \times Z_2 \times Z_2 \times Z_2,$$

so $d(H) = d(L) \geqslant d(L/N) = 4$ and thus $d(H) = 4$.

Further, if $m = 6$ then H is a maximal subgroup of $G = A_{|T|}$ for all possible p and f.

Conclusion. There are infinitely many pairs (G, H), where G is simple, $H < G$ is maximal and $d(H) = 4$.

Groups of Lie type

For groups of Lie type we use powerful reduction theorems of Aschbacher and Liebeck & Seitz on the subgroup structure of these groups.

Parabolic subgroups require special attention:

Let G be a simple group of Lie type over $\mathbb{F}_q$ and let $H = QL$ be a maximal parabolic subgroup of G.

In general, Q/Q' is an irreducible L-module, so if $L = \langle x_1, \dots, x_n \rangle$ and $q \in Q \setminus Q'$, then $H = \langle q, x_1, \dots, x_n \rangle$ (since $Q' \leqslant \Phi(H)$) and thus

$$d(H) \leqslant d(L) + 1.$$

Further generation properties

$$\begin{aligned}
\mathcal{M} &= \{H : H < G \text{ is maximal}\} \\
m_n(G) &= |\{H \in \mathcal{M} : [G : H] = n\}| \\
\mathbb{P}(G,k) &= \text{probability that } k \text{ randomly chosen elements generate } G \\
v(G) &= \min\{k : \mathbb{P}(G,k) \geqslant e^{-1}\}
\end{aligned}$$

The proof of Dixon's conjecture yields the following result:

Theorem

There exists a constant c such that $m_n(G) \leqslant n^c$ and $v(G) \leqslant c$ for any finite simple group G.

Question. Does this extend to maximal subgroups of simple groups?

Theorem (B, Liebeck & Shalev, 2013)

There exists a constant c such that $m_n(H) \leqslant n^c$ and $v(H) \leqslant c$ for any maximal subgroup H of a simple group.

However, Dixon's conjecture does **not** extend to maximal subgroups:

Example. Let $H = S_{n-2} < A_n$. The probability that k randomly chosen elements of H lie in A_{n-2} is 2^{-k}, so $\mathbb{P}(H, k) \leqslant 1 - 2^{-k}$.

Theorem (B, Liebeck & Shalev, 2013)

Given any $\varepsilon > 0$ there exists a constant $c = c(\varepsilon)$ such that $\mathbb{P}(H, c) > 1 - \varepsilon$ for any maximal subgroup H of a simple group.

A key theorem

Recall that $v(G) = \min\{k : \mathbb{P}(G, k) \geqslant e^{-1}\}$.

Theorem (Jaikin-Zapirain & Pyber, 2011)

There exist constants $0 < \alpha < \beta$ such that for any finite group G

$$\alpha(d(G) + \delta(G)) < v(G) < \beta d(G) + \delta(G)$$

where $\delta(G) \in \mathbb{R}^+$ is defined in terms of the chief factors of G.

Let H be a maximal subgroup of a simple group.

- We have $d(H) \leqslant 4$ and $\delta(H) < 1$, so $v(H) < 4\beta + 1 = c$.
- Given $\varepsilon > 0$ choose $k \in \mathbb{N}$ such that $(1 - e^{-1})^k < \varepsilon$. Then

$$1 - \mathbb{P}(H, kc) \leqslant (1 - \mathbb{P}(H, c))^k \leqslant (1 - e^{-1})^k < \varepsilon.$$

Applications and open problems

Application: Second maximal subgroups

A **second maximal** subgroup of G is a maximal subgroup of a maximal subgroup. Let $m_n^2(G)$ be the number of second maximals of index n.

Question. Can we extend our results from maximal to second maximal?

Proposition

There is an absolute constant c s.t. $m_n^2(G) \leqslant n^c$ for any simple group G.

$$\begin{aligned} m_n^2(G) &\leqslant \sum_{a \mid n} m_a(G) \max\{m_{n/a}(H) \mid H \in \mathcal{M}, [G:H] = a\} \\ &\leqslant \sum_{a \mid n} a^{c_1} (n/a)^{c_2} \\ &\leqslant n^{c_1 + c_2 + 1} \end{aligned}$$

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

Example

Suppose $G = \mathrm{PSL}_2(2^k)$ and $2^k - 1 = r$ is a (Mersenne) prime.

Then $H = (Z_2)^k$ has index r in a Borel subgroup of G, so H is a second maximal subgroup and $d(H) = k$.

Answer. No, if there are infinitely many Mersenne primes!

More generally, the answer is no if there are infinitely many integers of the form $p^k - 1$ (p prime) with a prime factor r such that $(p^k - 1)/r = o(k)$.

Application: Permutation groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then

$$G_\alpha = \{x \in G \,:\, x \cdot \alpha = \alpha\}$$

is a maximal subgroup of G, and

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

Question. Is there a constant c such that

$$d(G_\alpha) \leqslant d(G) + c$$

for every primitive permutation group G?

Theorem (B, Liebeck & Shalev, 2013)

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

Some open problems

- **Conjecture:** $d(H) \leqslant 4$ for any maximal subgroup H of an **almost simple** group.

- Is there a constant c such that $d(H) \leqslant c$ for any second maximal subgroup of a simple group, excluding a few known cases (only involving groups of Lie type of rank 1 and 2)?

- Is there a finite group with spread 1 but not spread 2?

- **Conjecture (Breuer, Guralnick & Kantor, 2008):**
A finite group G is $\frac{3}{2}$-generated if and only if G/N is cyclic for every nontrivial normal subgroup N of G.

- **Conjecture (Breuer, Guralnick, Lucchini, Maróti & Nagy, 2010):**
$\Gamma(G)$ contains a Hamiltonian cycle if and only if G/N is cyclic for every nontrivial normal subgroup N of G.