Simple groups, generation and probabilistic methods

Tim Burness

Groups, Geometry and Representations
Segal-Shalev Birthday Conference

University of Oxford

September 4th 2018

University of Bristol

Overview

1. Spread and uniform spread
2. The uniform domination number
3. Main tools: Base sizes and probabilistic methods
4. Main results

This is joint work with **Scott Harper**

Part 1:

Spread and uniform spread

Let $G = \langle x, y \rangle$ be a finite group.

How are the generating pairs $\{x, y\}$ distributed across the group?

More precisely:

- Can we impose conditions on the orders of x and y, or their conjugacy classes?
- What is the probability that two random elements generate G?
- Does G have the $\frac{3}{2}$**-generation** property?

  That is, does every nontrivial element belong to a generating pair?

Theorem (Steinberg, 1962). Every simple group is 2-generated.

Let us assume $G = \langle x, y \rangle$ is non-cyclic. Set $G^\# = G \setminus \{1\}$.

We say that G has **spread** k if for any $x_1, \ldots, x_k \in G^\#$ 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.

- **Piccard, 1939:** $\begin{cases} s(S_n) \geqslant 1 \text{ if } n \neq 4 \\ s(A_n) \geqslant 1 \end{cases}$

- **Binder, 1970:** $s(S_n) = \begin{cases} 0 & \text{if } n = 4 \\ 2 & \text{if } n \text{ even, } n \neq 4 \\ 3 & \text{if } n \text{ odd} \end{cases}$

- **Brenner & Wiegold, 1975:** $s(A_n) = \begin{cases} 2 & \text{if } n = 6 \\ 4 & \text{if } n \text{ even, } n \neq 6 \\ ? & \text{if } n \text{ odd} \end{cases}$

Example. $6\,098\,892\,799 \leqslant s(A_{19}) \leqslant 6\,098\,892\,803$

G has **uniform spread** k if there exists $C = y^G$ such that for any $x_1, \dots, x_k \in G^\#$ there exists $z \in C$ with $G = \langle x_i, z \rangle$ for all i.

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

Let G be a (non-abelian) simple group.

- **Guralnick & Kantor, 2000:** $u(G) \geqslant 1$
- **Breuer, Guralnick & Kantor, 2008:**
  $u(G) \geqslant 2$, with equality iff $G = A_5$, A_6, $\Omega_8^+(2)$ or $\Omega_{2r+1}(2)$ with $r \geqslant 3$
- **Guralnick & Shalev, 2003:**
  Let (G_n) be a sequence of simple groups with $|G_n| \to \infty$. Then either $u(G_n) \to \infty$, or there is an infinite subsequence consisting of
  - odd-dimensional orthogonal groups over a field of fixed size; or
  - alternating groups of degree all divisible by a fixed prime.

Notation. For $x, y \in G$ and $H \leqslant G$ we define

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

$$\mathcal{M}(y) = \{H \,:\, H < G \text{ is maximal and } y \in H\}$$

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

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 $x \in G^\#$.

Then $Q(x,y) < \frac{1}{k}$ for all $x \in G^\#$ and thus $u(G) \geqslant k$.

Example. Let $G = E_8(q)$ and choose $y \in G$ of order

$$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1.$$

- $\mathcal{M}(y) = \{H\}$, with $H = N_G(\langle y \rangle) = \langle y \rangle{:}C_{30}$
- $|x^G| > q^{58}$ for all $x \in G^\#$

Hence

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|} < \frac{|H|}{q^{58}} < \frac{1}{q^{44}}$$

for all $x \in G^\#$, so $u(G) \geqslant q^{44}$.

Example. $G = A_{19}, |y| = 19 \implies \mathcal{M}(y) = \{H\},\ H = C_{19}{:}C_9$. Then

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x, G/H) \leqslant \frac{1}{6098892800} \implies u(G) \geqslant 6098892799$$

The **generating graph** $\Gamma(G)$ has vertices $G^{\#}$, with x, y adjacent if and only if $G = \langle x, y \rangle$. In this setting,

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

Note. Suppose $1 \neq N \trianglelefteqslant G$ and G/N is non-cyclic. Then no element in N belongs to a generating pair, so $s(G) = 0$ (e.g. $s(S_4) = 0$).

Conjecture.

The following are equivalent, for any finite non-cyclic group G:

(a) $s(G) \geqslant 1$.

(b) $s(G) \geqslant 2$.

(c) $\Gamma(G)$ contains a Hamiltonian cycle.

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

Part 2:

The uniform domination number

A **total dominating set** (TDS) of a graph Γ is a set S of vertices such that every vertex of Γ is adjacent to a vertex in S.

The **total domination number** $\gamma_t(\Gamma)$ of Γ is the minimal size of a TDS.

Let G be a finite group with $s(G) \geqslant 1$ and generating graph $\Gamma(G)$.
Then $\gamma_t(\Gamma(G))$ is the total domination number of G, denoted $\gamma_t(G)$, i.e.

$$\gamma_t(G) = \min \left\{ |S| \ : \ \begin{array}{l} S \subseteq G^{\#} \text{ such that for all } x \in G^{\#}, \\ \text{there exists } y \in S \text{ with } G = \langle x, y \rangle \end{array} \right\}$$

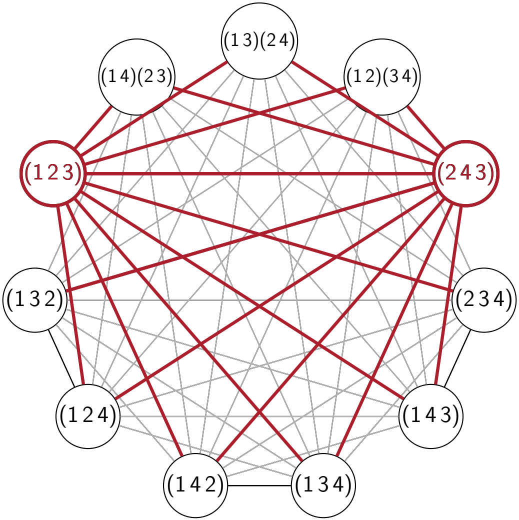
Similarly, if $u(G) \geqslant 1$ then the **uniform domination number** $\gamma_u(G)$ is the minimal size of a TDS for $\Gamma(G)$ consisting of **conjugate** elements.

Note that

$$2 \leqslant \gamma_t(G) \leqslant \gamma_u(G) \leqslant |C|$$

for some conjugacy class C of G.

An example: $G = A_4$



Conclusion. $\{(1, 2, 3), (2, 4, 3)\}$ is a TDS for G, hence $\gamma_u(G) = 2$

Uniform domination for simple groups

Recall: G simple $\implies u(G) \geqslant 1$ [Guralnick & Kantor, 2000]

Therefore, we can study $\gamma_u(G)$ for **simple groups**:

- Can we determine "good" bounds on $\gamma_u(G)$?
- Are there any examples with $\gamma_u(G) = 2$? Can we classify them?
- Suppose $\gamma_u(G) = 2$ and $y \in G$.

  What is the probability, denoted $P(G, y)$, that $\{y, y^g\}$ is a TDS for a randomly chosen conjugate y^g?
- What are the asymptotic properties of

$$P(G) = \max\{P(G, y) \,:\, y \in G\}$$

  for sequences of simple groups G with $\gamma_u(G) = 2$?

Part 3:

Main tools

The base size connection

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group on a finite set Ω.

A subset B of Ω is a **base** for G if $\bigcap_{b \in B} G_b = 1$.

The **base size** of G, denoted $b(G, \Omega)$, is the minimal size of a base for G.

Note that if G is transitive, say $\Omega = G/H$, then

$$b(G, \Omega) = \min\{|S| \,:\, S \subseteq G \text{ and } \bigcap_{g \in S} H^g = 1\}$$

Lemma. Suppose $y \in G$ and $\mathcal{M}(y) = \{H\}$ with H core-free. Then $\{y^{g_1}, \dots, y^{g_c}\}$ is a TDS if and only if $\bigcap_{i=1}^{c} H^{g_i} = 1$, so

$$\gamma_u(G) \leqslant b(G, G/H)$$

Theorem (B. et al., 2011). Let $G \leqslant \mathrm{Sym}(\Omega)$ be primitive and simple of "non-standard" type. Then $b(G, \Omega) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ and $|\Omega| = 24$.

Example. Let G be an exceptional simple group of Lie type and assume

$$G \notin \{F_4(2^f), G_2(3^f), {}^2F_4(2)'\}.$$

By [Weigel, 1992], there exists $y \in G$ with $\mathcal{M}(y) = \{H\}$, so

$$\gamma_u(G) \leqslant b(G, G/H) \leqslant 6.$$

Example. Take $G = E_8(q)$ and $y \in G$ with

$$|y| = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1.$$

Then $\mathcal{M}(y) = \{H\}$, with $H = \langle y \rangle{:}C_{30}$, and

$$\gamma_u(G) = b(G, G/H) = 2.$$

Lemma. Suppose that for all $y \in G^{\#}$ there exists $H \in \mathcal{M}(y)$ with H core-free and $b(G, G/H) \geqslant c$. Then $\gamma_u(G) \geqslant c$.

Example. Let $G = A_n$ with $n \geqslant 8$ even, so each $y \in G^{\#}$ is contained in a maximal intransitive subgroup H of G.

- By [Halasi, 2012],

$$b(G, G/H) \geqslant \lceil \log_2 n \rceil - 1$$

  and thus $\gamma_u(G) \geqslant \lceil \log_2 n \rceil - 1$ by the lemma.

- Set $d = (2, \frac{n}{2} - 1)$, $k = \frac{n}{2} - d$ and $y = (1, \dots, k)(k+1, \dots, n) \in G$.

  Then $\mathcal{M}(y) = \{H\}$ with $H = (S_k \times S_{n-k}) \cap G$ and

$$\gamma_u(G) \leqslant b(G, G/H) \leqslant \left\lceil \log_{\lceil \frac{2n}{n-2d} \rceil} n \right\rceil \cdot \left\lceil \frac{n+2d}{n-2d} \right\rceil \leqslant 2\lceil \log_2 n \rceil.$$

Probabilistic methods

For $y \in G$, $c \in \mathbb{N}$ we define

$$Q(G, y, c) = \text{Probability } c \text{ random conjugates of } y \text{ do } \textbf{not} \text{ form a TDS}$$

Note. $Q(G, y, c) < 1 \implies \gamma_u(G) \leqslant c$

Lemma. Let $x_1^G, \dots, x_k^G$ be the conjugacy classes of elements of prime order in G. Then

$$Q(G, y, c) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \left(\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(x_i, G/H) \right)^c$$

Note. If $\mathcal{M}(y) = \{H\}$, this is equivalent to a key lemma of Liebeck & Shalev (1999) for studying $b(G, G/H)$.

An example

Let $G = \mathrm{PSL}_{r+1}(q)$, where $r \geqslant 8$ is even, and set

$$y = \left(\begin{array}{c|c} y_1 & \\ \hline & y_2 \end{array}\right) \in G, \ \text{with } y_1 \in \mathrm{GL}_{\frac{r}{2}}(q),\ y_2 \in \mathrm{GL}_{\frac{r}{2}+1}(q) \text{ irreducible.}$$

- $\mathcal{M}(y) = \{H_1, H_2\}$ by [Guralnick, Penttila, Praeger & Saxl, 1999]
- $\mathrm{fpr}(x, G/H_i) < 2q^{-\frac{r}{2}}$ for all $x \in G^{\#}$ by [Guralnick & Kantor, 2000]

Let $c = 2r + 26$. Then

$$Q(G, y, c) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \left(\sum_{j=1}^{2} \mathrm{fpr}(x_i, G/H_j) \right)^c < q^{r^2+2r} \left(4q^{-\frac{r}{2}}\right)^c < q^{-4}$$

Conclusion. $\gamma_u(G) \leqslant 2r + 26$

Part 4:

Main results

Theorem (B. & Harper, 2018). Let G be a finite simple group.

- G sporadic: $\gamma_u(G) \leqslant 4$ (e.g. $\gamma_u(\mathrm{M}_{11}) = \gamma_u(\mathrm{M}_{12}) = 4$)
- G alternating, degree n: $\gamma_u(G) \leqslant c \log_2 n$ (e.g. $c = 77$)
- G exceptional: $\gamma_u(G) \leqslant 5$
- G classical, rank r: $\gamma_u(G) \leqslant 7r + 56$

Stronger bounds hold in special cases, e.g.

- $G = A_n$, n even: $\lceil \log_2 n \rceil - 1 \leqslant \gamma_u(G) \leqslant 2\lceil \log_2 n \rceil$
- $G = \Omega_{2r+1}(q)$, $r \geqslant 3$: $r \leqslant \gamma_u(G) \leqslant 7r$

Theorem (B. & Harper, 2018). Let G be a finite simple group.

Then $\gamma_u(G) = 2$ only if G is one of the following:

- $\mathrm{M}_{23}, \mathrm{J}_1, \mathrm{J}_4, \mathrm{Ru}, \mathrm{Ly}, \mathrm{O'N}, \mathrm{Fi}_{23}, \mathrm{Fi}_{24}', \mathrm{Th}, \mathbb{B}, \mathbb{M}$, or $\mathrm{J}_3, \mathrm{He}, \mathrm{Co}_1, \mathrm{HN}$
- A_n, $n \geqslant 13$ prime
- ${}^2B_2(q), {}^2G_2(q), {}^2F_4(q), {}^3D_4(q), {}^2E_6(q), E_6(q), E_7(q), E_8(q)$
- $\mathrm{PSL}_2(q)$, $q \geqslant 11$ odd
- $\mathrm{PSL}_n^{\epsilon}(q), n$ odd, $(n, q, \epsilon) \neq (3, 2, +), (3, 4, +), (3, 3, -), (3, 5, -)$
- $G = \mathrm{PSp}_n(q)$, $n \equiv 2 \pmod 4$, $n \geqslant 10$, q odd
- $G = \mathrm{P}\Omega_n^{-}(q)$, $n \equiv 0 \pmod 4$, $n \geqslant 8$

Suppose G is simple, $\gamma_u(G) = 2$ and $y \in G$.

$$P(G, y) = \text{Probability that } \{y, y^g\} \text{ is a TDS for a random conjugate } y^g$$
$$P(G) = \max\{P(G, y) \,:\, y \in G\}$$

Theorem (B. & Harper, 2018).
If $G \not\in \{\mathrm{PSp}_{4m+2}(q) \,:\, m \geqslant 2,\, q \text{ odd}\} \cup \{\mathrm{P\Omega}^-_{4m}(q) \,:\, m \geqslant 2\}$ then

$$P(G) \to \begin{cases} \frac{1}{2} & \text{if } G = \mathrm{PSL}_2(q) \\ 1 & \text{otherwise} \end{cases} \quad \text{as } |G| \to \infty$$

Moreover, $P(G) \leqslant \frac{1}{2}$ only if G is one of the following:

- $\mathrm{PSL}_2(q)$ with $q \equiv 3 \pmod 4$, $q \geqslant 11$
- $A_{13}, \mathrm{U}_5(2), \mathrm{Fi}_{23}, \mathrm{J}_3, \mathrm{He}, \mathrm{Co}_1, \mathrm{HN}$

Example. Suppose $G = \mathrm{PSL}_2(q)$ and $q \geqslant 11$ is odd.

Choose $y \in G$ of order $\frac{1}{2}(q+1)$, so $\mathcal{M}(y) = \{H\}$ with $H = D_{q+1}$, and

$$P(G,y) = \frac{|\{y^g \in y^G \,:\, \{y, y^g\} \text{ is a TDS}\}|}{|y^G|}$$
$$= \frac{|\{y^g \in y^G \,:\, H \cap H^g = 1\}|}{|y^G|} = \frac{r|H|^2}{|G|}$$

where r is the number of regular orbits of H on G/H. We compute

$$r = \frac{1}{4}(q - \epsilon)$$

where $q \equiv \epsilon \pmod 4$, $\epsilon \in \{1, 3\}$, and thus

$$P(G,y) = \begin{cases} \frac{1}{2}\left(1 + \frac{1}{q}\right) & \text{if } q \equiv 1 \pmod 4 \\ \frac{1}{2}\left(1 - \frac{q+1}{q(q-1)}\right) & \text{if } q \equiv 3 \pmod 4 \end{cases}$$

Example. Suppose $G = F_4(q)$ and define

$$\mathcal{A} = \{\text{maximal parabolic subgroups of } G\}$$
$$\mathcal{B} = \{\text{maximal rank subgroups of type } B_4(q)\}$$
$$\mathcal{C} = \{\text{maximal rank subgroups of type } {}^3D_4(q)\}$$

By considering the structure of the maximal tori of G, one can show that each $y \in G$ is contained in a maximal subgroup $H \in \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$.

Since $|H|^2 > |G|$, we have $b(G, G/H) \geqslant 3$.

Conclusion. $\gamma_u(G) \geqslant 3$

Example. Suppose $G = \mathrm{P}\Omega_n^-(q)$, $n \equiv 0 \pmod 4$, $n \geqslant 8$. Let $y \in G$.

- *y reducible:* Here y is contained in a maximal reducible subgroup H and $b(G, G/H) \geqslant 3$.

- *y irreducible:* We can assume y is a Singer cycle. By [Bereczky, 2000],

$$\mathcal{M}(y) = \{H_k \, : \, k \text{ is a prime divisor of } n\}$$

  with H_k a field extension subgroup of type $O^-_{n/k}(q^k)$.

  In particular, $\gamma_u(G) \geqslant b(G, G/H_2)$, which is **not known**.

We have $|H_2|^2 < |G|$ and $b(G, G/H_2) \in \{2, 3, 4\}$ by [B., 2007].

For $n = 8$, $\gamma_u(G) = b(G, G/H_2) = 2 + \delta_{2,q}$ for $q \in \{2, 3, 5\}$.

Is $\{P(G) \, : \, G \text{ simple}, \gamma_u(G) = 2\}$ bounded away from zero?