$\frac{3}{2}$-Generation of Finite Groups

Scott Harper

University of Bristol

Groups St Andrews

7th August 2017

Generating Finite Simple Groups

Generating Finite Simple Groups

Theorem (Steinberg, 1962)

Every finite simple group is generated by two elements.

Generating Finite Simple Groups

Theorem (Steinberg, 1962)

Every finite simple group is generated by two elements.

Let $P(G)$ be the probability that a pair of elements of G generate G.

Generating Finite Simple Groups

Theorem (Steinberg, 1962)

Every finite simple group is generated by two elements.

Let $P(G)$ be the probability that a pair of elements of G generate G.

Netto's Conjecture (1882) $P(A_n) \to 1$ as $n \to \infty$

Generating Finite Simple Groups

Theorem (Steinberg, 1962)

Every finite simple group is generated by two elements.

Let $P(G)$ be the probability that a pair of elements of G generate G.

Netto's Conjecture (1882) $P(A_n) \to 1$ as $n \to \infty$

Theorem (Liebeck & Shalev, 1995)

If G is a finite simple group, then $P(G) \to 1$ as $|G| \to \infty$

Generating Finite Simple Groups

Theorem (Steinberg, 1962)

Every finite simple group is generated by two elements.

Let $P(G)$ be the probability that a pair of elements of G generate G.

Netto's Conjecture (1882) $P(A_n) \to 1$ as $n \to \infty$

Theorem (Liebeck & Shalev, 1995)

If G is a finite simple group, then $P(G) \to 1$ as $|G| \to \infty$

Summary: Finite simple groups have many generating pairs.

Generating Finite Simple Groups

Theorem (Steinberg, 1962)

Every finite simple group is generated by two elements.

Let $P(G)$ be the probability that a pair of elements of G generate G.

Netto's Conjecture (1882) $P(A_n) \to 1$ as $n \to \infty$

Theorem (Liebeck & Shalev, 1995)

If G is a finite simple group, then $P(G) \to 1$ as $|G| \to \infty$

Summary: Finite simple groups have many generating pairs.

Question: How are these generating pairs distributed across the group?

$\frac{3}{2}$-Generation

A group G is **$\frac{3}{2}$-generated** if every non-identity element of G is contained in a generating pair.

$\frac{3}{2}$-Generation

A group G is **$\frac{3}{2}$-generated** if every non-identity element of G is contained in a generating pair.

Theorem (Guralnick & Kantor, 2000)

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

$\frac{3}{2}$-Generation

A group G is **$\frac{3}{2}$-generated** if every non-identity element of G is contained in a generating pair.

Theorem (Guralnick & Kantor, 2000)

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

Main Question

Which finite groups are $\frac{3}{2}$-generated?

$\frac{3}{2}$-Generation

A group G is **$\frac{3}{2}$-generated** if every non-identity element of G is contained in a generating pair.

Theorem (Guralnick & Kantor, 2000)

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

Main Question

Which finite groups are $\frac{3}{2}$-generated?

Simple groups: Groups such that all proper quotients are **trivial**.

$\frac{3}{2}$-Generation

A group G is **$\frac{3}{2}$-generated** if every non-identity element of G is contained in a generating pair.

Theorem (Guralnick & Kantor, 2000)

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

Main Question

Which finite groups are $\frac{3}{2}$-generated?

Simple groups: Groups such that all proper quotients are **trivial**.

Any more? Groups such that all proper quotients are **cyclic**?

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$.

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since G is $\frac{3}{2}$-generated, there exists $x \in G$ such that $\langle x, n \rangle = G$.

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since G is $\frac{3}{2}$-generated, there exists $x \in G$ such that $\langle x, n \rangle = G$.

In particular, $\langle xN, nN \rangle = G/N$.

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since G is $\frac{3}{2}$-generated, there exists $x \in G$ such that $\langle x, n \rangle = G$.

In particular, $\langle xN, nN \rangle = G/N$. Since nN is trivial in G/N, in fact, $G/N = \langle xN \rangle$.

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since G is $\frac{3}{2}$-generated, there exists $x \in G$ such that $\langle x, n \rangle = G$.

In particular, $\langle xN, nN \rangle = G/N$. Since nN is trivial in G/N, in fact, $G/N = \langle xN \rangle$. So G/N is cyclic. ■

Let G be a finite group.

Proposition

G is $\frac{3}{2}$-generated $\implies$ every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since G is $\frac{3}{2}$-generated, there exists $x \in G$ such that $\langle x, n \rangle = G$.

In particular, $\langle xN, nN \rangle = G/N$. Since nN is trivial in G/N, in fact, $G/N = \langle xN \rangle$. So G/N is cyclic. ∎

Conjecture (Breuer, Guralnick & Kantor, 2008)

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Which finite groups are $\frac{3}{2}$-generated?

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Which finite groups are $\frac{3}{2}$-generated?

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Need to show: For all finite groups G,

$$\text{every proper quotient of } G \text{ is cyclic} \implies G \text{ is } \tfrac{3}{2}\text{-generated.}$$

Which finite groups are $\frac{3}{2}$-generated?

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Need to show: For all finite groups G,

every proper quotient of G is cyclic $\implies$ G is $\frac{3}{2}$-generated.

It suffices to show: For all finite **almost simple** groups G,

every proper quotient of G is cyclic $\implies$ G is $\frac{3}{2}$-generated.

Which finite groups are $\frac{3}{2}$-generated?

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Need to show: For all finite groups G,

$$\text{every proper quotient of } G \text{ is cyclic} \implies G \text{ is } \tfrac{3}{2}\text{-generated.}$$

It suffices to show: For all finite **almost simple** groups G,

$$\text{every proper quotient of } G \text{ is cyclic} \implies G \text{ is } \tfrac{3}{2}\text{-generated.}$$

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

Which finite groups are $\frac{3}{2}$-generated?

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Need to show: For all finite groups G,

$$\text{every proper quotient of } G \text{ is cyclic} \implies G \text{ is } \tfrac{3}{2}\text{-generated.}$$

It suffices to show: For all finite **almost simple** groups G,

$$\text{every proper quotient of } G \text{ is cyclic} \implies G \text{ is } \tfrac{3}{2}\text{-generated.}$$

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

Examples $G = S_n$ (with $T = A_n$); $G = \mathrm{PGL}_n(q)$ (with $T = \mathrm{PSL}_n(q)$).

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating

Classical

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating

Classical

Exceptional

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating

Classical

Exceptional

Sporadic

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

Exceptional

Sporadic

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

Exceptional

Sporadic Breuer, Guralnick & Kantor, 2008

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

Linear

Exceptional

Sporadic Breuer, Guralnick & Kantor, 2008

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

Linear

Symplectic

Exceptional

Sporadic Breuer, Guralnick & Kantor, 2008

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

Linear

Symplectic   Orthogonal

Exceptional

Sporadic Breuer, Guralnick & Kantor, 2008

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

Linear

Symplectic Orthogonal Unitary

Exceptional

Sporadic Breuer, Guralnick & Kantor, 2008

Conjecture

G is $\frac{3}{2}$-generated $\iff$ every proper quotient of G is cyclic.

Aim: For simple T and $g \in \mathrm{Aut}(T)$, show that $G = \langle T, g \rangle$ is $\frac{3}{2}$-generated.

Alternating Piccard, 1939

Classical

- **Linear** Burness & Guest, 2013
- **Symplectic** **Orthogonal** **Unitary**

Exceptional

Sporadic Breuer, Guralnick & Kantor, 2008

$\frac{3}{2}$-Generation and Spread

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $\langle T, g \rangle$ is $\frac{3}{2}$-generated.

$\frac{3}{2}$-Generation and Spread

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $\langle T, g \rangle$ is $\frac{3}{2}$-generated.

A group G has **spread** k if for any distinct $x_1, \dots, x_k \in G \setminus 1$ there exists an element $z \in G$ such that $\langle x_1, g \rangle = \cdots = \langle x_k, z \rangle = G$.

$\frac{3}{2}$-Generation and Spread

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $\langle T, g \rangle$ is $\frac{3}{2}$-generated.

A group G has **spread** k if for any distinct $x_1, \dots, x_k \in G \setminus 1$ there exists an element $z \in G$ such that $\langle x_1, g \rangle = \cdots = \langle x_k, z \rangle = G$.

Write ***s(G)*** for the greatest integer k such that G has spread k.

$\frac{3}{2}$-Generation and Spread

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $\langle T, g \rangle$ is $\frac{3}{2}$-generated.

A group G has **spread** k if for any distinct $x_1, \dots, x_k \in G \setminus 1$ there exists an element $z \in G$ such that $\langle x_1, g \rangle = \cdots = \langle x_k, z \rangle = G$.

Write ***s(G)*** for the greatest integer k such that G has spread k.

Theorem (Breuer, Guralnick & Kantor, 2008)

If G is a finite simple group, then $s(G) \geq 2$.

$\frac{3}{2}$-Generation and Spread

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $\langle T, g \rangle$ is $\frac{3}{2}$-generated.

A group G has **spread** k if for any distinct $x_1, \dots, x_k \in G \setminus 1$ there exists an element $z \in G$ such that $\langle x_1, g \rangle = \cdots = \langle x_k, z \rangle = G$.

Write ***s(G)*** for the greatest integer k such that G has spread k.

Theorem (Breuer, Guralnick & Kantor, 2008)

If G is a finite simple group, then $s(G) \geq 2$.

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $s(\langle T, g \rangle) \geq 2$.

Asymptotic Behaviour of Spread

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Then $s(G_n) \to \infty$

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Then $s(G_n) \to \infty$ if and only if there is no subsequence of (G_n) of

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Then $s(G_n) \to \infty$ if and only if there is no subsequence of (G_n) of

- odd-dimensional orthogonal groups over a field of fixed size, or

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Then $s(G_n) \to \infty$ if and only if there is no subsequence of (G_n) of

- odd-dimensional orthogonal groups over a field of fixed size, or
- symplectic groups in even characteristic over a field of fixed size.

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Then $s(G_n) \to \infty$ if and only if there is no subsequence of (G_n) of

- odd-dimensional orthogonal groups over a field of fixed size, or
- symplectic groups in even characteristic over a field of fixed size.

Theorem (H, 2017)

Let $G_n = \langle T_n, g_n \rangle$ where $T_n \in \{\mathrm{PSp}_{2m}(q), \Omega_{2m+1}(q)\}$ and $g_n \in \mathrm{Aut}(T_n)$.
Assume that $|G_n| \to \infty$.

Asymptotic Behaviour of Spread

Theorem (Guralnick & Shalev, 2003)

Let G_n be a finite simple classical group. Assume that $|G_n| \to \infty$.

Then $s(G_n) \to \infty$ if and only if there is no subsequence of (G_n) of

- odd-dimensional orthogonal groups over a field of fixed size, or
- symplectic groups in even characteristic over a field of fixed size.

Theorem (H, 2017)

Let $G_n = \langle T_n, g_n \rangle$ where $T_n \in \{\mathrm{PSp}_{2m}(q), \Omega_{2m+1}(q)\}$ and $g_n \in \mathrm{Aut}(T_n)$. Assume that $|G_n| \to \infty$. Then $s(G_n) \to \infty$ if and only if (T_n) does not have a sequence as above.

Probabilistic Method

Let $s \in G$. Write

$$P(x, s) = \frac{|\{z \in s^G \mid \langle x, z\rangle \neq G\}|}{|s^G|}$$

Probabilistic Method

Let $s \in G$. Write

$$P(x,s) = \frac{|\{z \in s^G \mid \langle x, z\rangle \neq G\}|}{|s^G|}$$

Lemma 1

If for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$, then $s(G) \geq k$.

Probabilistic Method

Let $s \in G$. Write

$$P(x, s) = \frac{|\{z \in s^G \mid \langle x, z \rangle \neq G\}|}{|s^G|}$$

Lemma 1

If for any element $x \in G$ of prime order $P(x, s) < \frac{1}{k}$, then $s(G) \geq k$.

$$\langle x, s^g \rangle \neq G$$

Probabilistic Method

Let $s \in G$. Write

$$P(x,s) = \frac{|\{z \in s^G \mid \langle x, z\rangle \neq G\}|}{|s^G|}$$

Lemma 1

If for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$, then $s(G) \geq k$.

$$\langle x, s^g\rangle \neq G \implies x \text{ lies in a maximal subgroup of } G \text{ which contains } s^g$$

Probabilistic Method

Let $s \in G$. Write

$$P(x,s) = \frac{|\{z \in s^G \mid \langle x,z\rangle \neq G\}|}{|s^G|}$$

Lemma 1

If for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$, then $s(G) \geq k$.

$$\begin{aligned} \langle x, s^g\rangle \neq G &\implies x \text{ lies in a maximal subgroup of } G \text{ which contains } s^g \\ &\implies x^{g^{-1}} \text{ lies in a maximal subgroup of } G \text{ which contains } s \end{aligned}$$

Probabilistic Method

Let $s \in G$. Write

$$P(x, s) = \frac{|\{z \in s^G \mid \langle x, z \rangle \neq G\}|}{|s^G|}$$

Lemma 1

If for any element $x \in G$ of prime order $P(x, s) < \frac{1}{k}$, then $s(G) \geq k$.

$$\begin{aligned} \langle x, s^g \rangle \neq G &\implies x \text{ lies in a maximal subgroup of } G \text{ which contains } s^g \\ &\implies x^{g^{-1}} \text{ lies in a maximal subgroup of } G \text{ which contains } s \end{aligned}$$

Let $\mathcal{M}(G, s)$ be the set of maximal subgroups of G which contain s.

Probabilistic Method

Let $s \in G$. Write

$$P(x,s) = \frac{|\{z \in s^G \mid \langle x, z\rangle \neq G\}|}{|s^G|}$$

Lemma 1

If for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$, then $s(G) \geq k$.

$$\begin{aligned}\langle x, s^g\rangle \neq G &\implies x \text{ lies in a maximal subgroup of } G \text{ which contains } s^g \\ &\implies x^{g^{-1}} \text{ lies in a maximal subgroup of } G \text{ which contains } s\end{aligned}$$

Let $\mathcal{M}(G,s)$ be the set of maximal subgroups of G which contain s.

Lemma 2

$$P(x,s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}.$$

Proof Idea

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$.

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma\colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

1. Choose an element $s \in G$

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

1. Choose an element $s \in G$

Observation 1: $s \notin \mathrm{Sp}_n(q)$

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma\colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

1. Choose an element $s \in G$

Observation 1: $s \notin \mathrm{Sp}_n(q)$

This is a **significant difference** from the case when G is simple.

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma\colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

1. Choose an element $s \in G$

Observation 1: $s \notin \mathrm{Sp}_n(q)$

This is a **significant difference** from the case when G is simple.

Observation 2: $s^e \in \mathrm{Sp}_n(q)$

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

1. Choose an element $s \in G$

Observation 1: $s \notin \mathrm{Sp}_n(q)$

This is a **significant difference** from the case when G is simple.

Observation 2: $s^e \in \mathrm{Sp}_n(q)$

A **central idea** of the method: choose s such that we understand s^e.

Proof Idea

Let $T = \mathrm{Sp}_n(q)$ where $q = 2^e$ with $e > 1$ and where $n \equiv 2 \pmod 4$.

Then $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$ where $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$.

Let $G = \mathrm{Aut}(T)$.

1. Choose an element $s \in G$

Observation 1: $s \notin \mathrm{Sp}_n(q)$

This is a **significant difference** from the case when G is simple.

Observation 2: $s^e \in \mathrm{Sp}_n(q)$

A **central idea** of the method: choose s such that we understand s^e.

Question: Which elements in $\mathrm{Sp}_n(q)$ arise as s^e for some $s \notin \mathrm{Sp}_n(q)$?

Let X be a connected linear algebraic group.

Let X be a connected linear algebraic group. Example: $X = \mathsf{Sp}_n(\overline{\mathbb{F}}_2)$

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma : X \to X$ be a Frobenius morphism.

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma\colon X \to X$ be a Frobenius morphism. Example: $\sigma\colon (a_{ij}) \mapsto (a_{ij}^2)$

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma \colon X \to X$ be a Frobenius morphism. Example: $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$

Write X_σ be the subgroup of X fixed by σ.

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma \colon X \to X$ be a Frobenius morphism. Example: $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$

Write X_σ be the subgroup of X fixed by σ. Example: $X_\sigma = \mathrm{Sp}_n(2)$

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma \colon X \to X$ be a Frobenius morphism. Example: $\sigma \colon (a_{ij}) \mapsto (a_{ij}^2)$

Write X_σ be the subgroup of X fixed by σ. Example: $X_\sigma = \mathrm{Sp}_n(2)$

Write X_{σ^e} be the subgroup of X fixed by σ^e.

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma : X \to X$ be a Frobenius morphism. Example: $\sigma : (a_{ij}) \mapsto (a_{ij}^2)$

Write X_σ be the subgroup of X fixed by σ. Example: $X_\sigma = \mathrm{Sp}_n(2)$

Write X_{σ^e} be the subgroup of X fixed by σ^e. Example: $X_{\sigma^e} = \mathrm{Sp}_n(q)$

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma : X \to X$ be a Frobenius morphism. Example: $\sigma : (a_{ij}) \mapsto (a_{ij}^2)$

Write X_σ be the subgroup of X fixed by σ. Example: $X_\sigma = \mathrm{Sp}_n(2)$

Write X_{σ^e} be the subgroup of X fixed by σ^e. Example: $X_{\sigma^e} = \mathrm{Sp}_n(q)$

Shintani Descent

There is a bijection (with other nice properties)

$$f : \quad X_{\sigma^e}\text{-classes of } X_{\sigma^e}\sigma \quad \longrightarrow \quad X_\sigma\text{-classes of } X_\sigma$$

such that $f(g)$ is X-conjugate to g^e.

Let X be a connected linear algebraic group. Example: $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_2)$

Let $\sigma : X \to X$ be a Frobenius morphism. Example: $\sigma : (a_{ij}) \mapsto (a_{ij}^2)$

Write X_σ be the subgroup of X fixed by σ. Example: $X_\sigma = \mathrm{Sp}_n(2)$

Write X_{σ^e} be the subgroup of X fixed by σ^e. Example: $X_{\sigma^e} = \mathrm{Sp}_n(q)$

Shintani Descent

There is a bijection (with other nice properties)

$$f : \quad X_{\sigma^e}\text{-classes of } X_{\sigma^e}\sigma \quad \longrightarrow \quad X_\sigma\text{-classes of } X_\sigma$$

such that $f(g)$ is X-conjugate to g^e.

Application For all $x \in \mathrm{Sp}_n(2) \leq \mathrm{Sp}_n(q)$ there exists $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e is $\mathrm{Sp}_n(\overline{\mathbb{F}}_2)$-conjugate to x.

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

2 Determine the maximal subgroups in $\mathcal{M}(G, s)$

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

2. Determine the maximal subgroups in $\mathcal{M}(G, s)$

Theorem (Aschbacher, 1984)

Let G be a classical almost simple group with socle T. Any maximal subgroup of G which does not contain T belongs to one of:

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

2. Determine the maximal subgroups in $\mathcal{M}(G, s)$

Theorem (Aschbacher, 1984)

Let G be a classical almost simple group with socle T. Any maximal subgroup of G which does not contain T belongs to one of:

- $\mathcal{C}_1, \ldots, \mathcal{C}_8$ (a family of geometric subgroups);

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

2 Determine the maximal subgroups in $\mathcal{M}(G, s)$

Theorem (Aschbacher, 1984)

Let G be a classical almost simple group with socle T. Any maximal subgroup of G which does not contain T belongs to one of:

- $\mathcal{C}_1, \ldots, \mathcal{C}_8$ (a family of geometric subgroups);
- $\mathcal{S}$ (the family of almost simple irreducible subgroups).

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

2 Determine the maximal subgroups in $\mathcal{M}(G, s)$

Theorem (Aschbacher, 1984)

Let G be a classical almost simple group with socle T. Any maximal subgroup of G which does not contain T belongs to one of:

- $\mathcal{C}_1, \ldots, \mathcal{C}_8$ (a family of geometric subgroups);
- $\mathcal{S}$ (the family of almost simple irreducible subgroups).

Key Features Only two subspaces are stabilised by s^e.

Choose $s \in \mathrm{Sp}_n(q)\sigma$ such that s^e has the form

$$\left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in \mathrm{Sp}_n(2)$$

where A_1 and A_2 act irreducibly on non-degenerate 2- and $(n-2)$-spaces.

2 Determine the maximal subgroups in $\mathcal{M}(G, s)$

Theorem (Aschbacher, 1984)

Let G be a classical almost simple group with socle T. Any maximal subgroup of G which does not contain T belongs to one of:

- $\mathcal{C}_1, \dots, \mathcal{C}_8$ (a family of geometric subgroups);
- $\mathcal{S}$ (the family of almost simple irreducible subgroups).

Key Features Only two subspaces are stabilised by s^e.

A power of s^e has an $(n-2)$-dimensional 1-eigenspace.

3 Calculate $P(x, s)$ for $x \in G$ of prime order

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x, s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x, s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x, s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x,s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to **generation problems**

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x, s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to generation problems, **base sizes**

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x,s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to generation problems, base sizes, **finite geometry**

3 Calculate $P(x, s)$ for $x \in G$ of prime order

Recall that

$$P(x,s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to generation problems, base sizes, finite geometry, **monodromy groups**

3 Calculate $P(x,s)$ for $x \in G$ of prime order

Recall that

$$P(x,s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to generation problems, base sizes, finite geometry, monodromy groups ...

3 Calculate $P(x,s)$ for $x \in G$ of prime order

Recall that

$$P(x,s) \leq \sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|}$$

The quantity $\frac{|x^G \cap H|}{|x^G|}$ is the **fixed point ratio** of the action of G on the G/H.

Fixed point ratios find applications to generation problems, base sizes, finite geometry, monodromy groups ...

Theorem (Burness, 2007)

Let G be an almost simple classical group, let H be a maximal subgroup of G and let $x \in G$ have prime order. Then

$$|x^G \cap H| < |x^G|^{\varepsilon}$$

for $\varepsilon \approx \frac{1}{2}$, provided that H does not stabilise a subspace.

Summary

Conjecture

A finite group is $\frac{3}{2}$-generated iff every proper quotient is cyclic.

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $s(\langle T, g \rangle) \geq 2$.

Summary

Conjecture

A finite group is $\frac{3}{2}$-generated iff every proper quotient is cyclic.

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $s(\langle T, g \rangle) \geq 2$.

Asymptotic Results: We apply a similar probabilistic approach.

Summary

Conjecture

A finite group is $\frac{3}{2}$-generated iff every proper quotient is cyclic.

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $s(\langle T, g \rangle) \geq 2$.

Asymptotic Results: We apply a similar probabilistic approach.

Current work: Prove similar results on the spread of the remaining almost simple groups of Lie type.

Summary

Conjecture

A finite group is $\frac{3}{2}$-generated iff every proper quotient is cyclic.

Theorem (H, 2017)

If $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$ and $g \in \mathrm{Aut}(T)$, then $s(\langle T, g \rangle) \geq 2$.

Asymptotic Results: We apply a similar probabilistic approach.

Current work: Prove similar results on the spread of the remaining almost simple groups of Lie type.

Question: Are there any finite groups with spread one but not two?