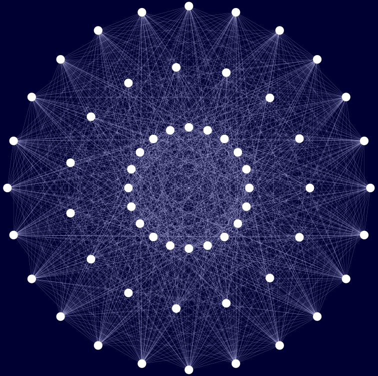
$\frac{3}{2}$-Generation of Finite Groups



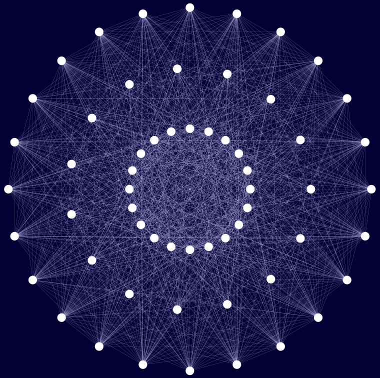
Scott Harper

(University of Bristol)

Postgraduate Group Theory Conference

30th June 2016

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



Scott Harper

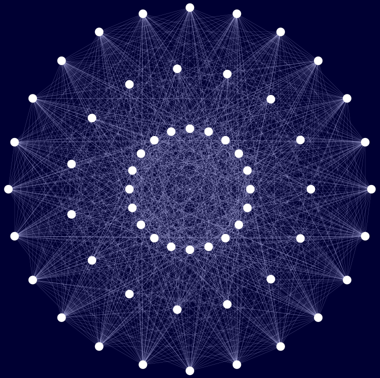
(University of Bristol)

Postgraduate Group Theory Conference

30th June 2016

.

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



Scott Harper

(University of Bristol)

Postgraduate Group Theory Conference

30th June 2016

Generating Finite Groups

Generating Finite Groups

A finite group G is d-generated if G has a generating set of size d.

Generating Finite Groups

A finite group G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

Generating Finite Groups

A finite group G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

Dihedral groups are 2-generated: $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

Generating Finite Groups

A finite group G is *d-generated* if G has a generating set of size d.

Cyclic groups are 1-generated

Dihedral groups are 2-generated: $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric groups are 2-generated: $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Generating Finite Groups

A finite group G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

Dihedral groups are 2-generated: $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric groups are 2-generated: $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Alternating groups are 2-generated:

– if n is odd $A_n = \langle (1\,2\,3), (1\,2\,\ldots\,n) \rangle$

– if n is even $A_n = \langle (1\,2\,3), (2\,3\,\ldots\,n) \rangle$

Generating Finite Groups

A finite group G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

Dihedral groups are 2-generated: $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric groups are 2-generated: $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Alternating groups are 2-generated:
– if n is odd $A_n = \langle (1\,2\,3), (1\,2\,\ldots\,n) \rangle$
– if n is even $A_n = \langle (1\,2\,3), (2\,3\,\ldots\,n) \rangle$

Theorem (Steinberg 1962; Aschbacher & Guralnick 1984)

Every finite simple group is 2-generated.

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

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

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

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

Theorem (Stein 1998; 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 belongs to a generating pair.

Theorem (Stein 1998; 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 belongs to a generating pair.

Theorem (Stein 1998; 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 belongs to a generating pair.

Theorem (Stein 1998; 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?

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

Proposition

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

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

Proposition

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

Proof

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

Proposition

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

Proof

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

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

Proposition

If G is $\frac{3}{2}$-generated then 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 $\langle x, n \rangle = G$.

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

Proposition

If G is $\frac{3}{2}$-generated then 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, $\langle xN, nN \rangle = G/N$.

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

Proposition

If G is $\frac{3}{2}$-generated then 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, $G/N = \langle xN \rangle$.

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

Proposition

If G is $\frac{3}{2}$-generated then 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. ∎

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

Proposition

If G is $\frac{3}{2}$-generated then 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)

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

Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;

Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

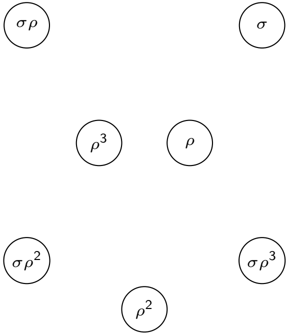
Dihedral group D_8

Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8

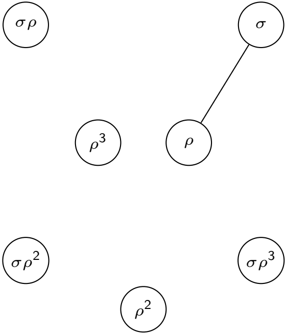


Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8

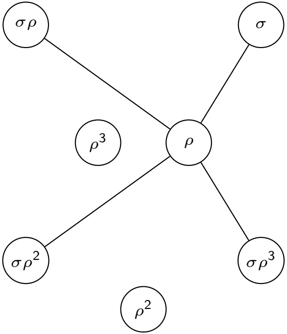


Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8

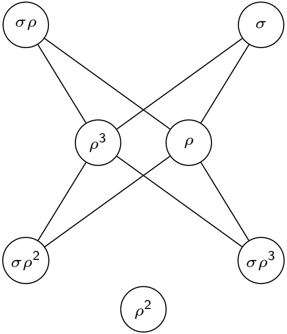


Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h\rangle = G$.

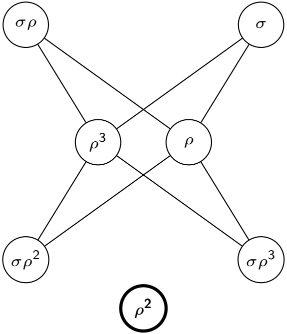
Dihedral group D_8



The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8

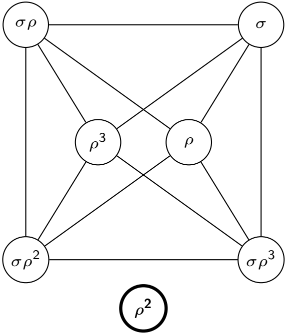


Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8

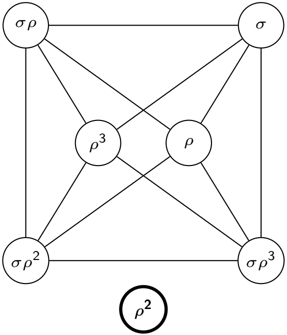


Generating Graphs

The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8



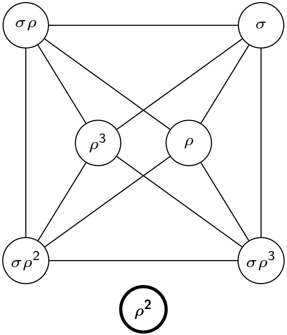
Alternating group A_4

Generating Graphs

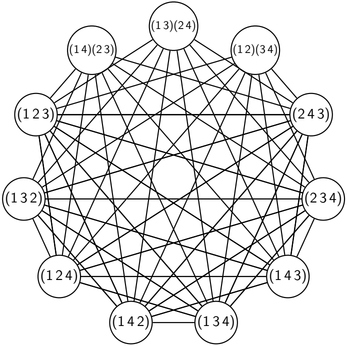
The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h\rangle = G$.

Dihedral group D_8



Alternating group A_4

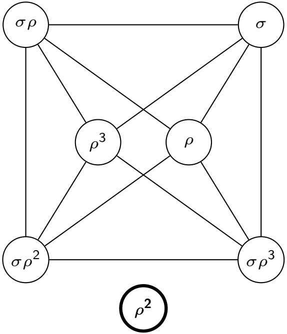


Generating Graphs

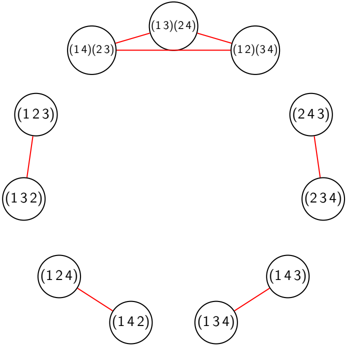
The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8



Alternating group A_4

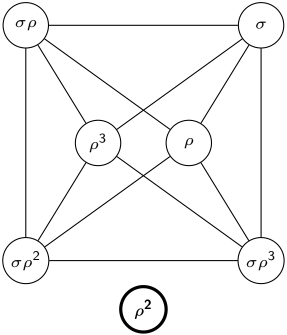


Generating Graphs

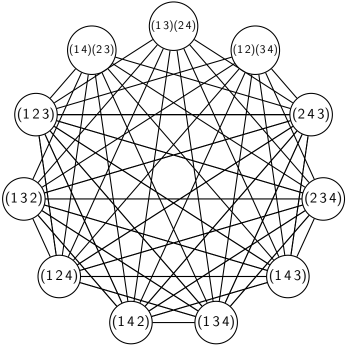
The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8



Alternating group A_4

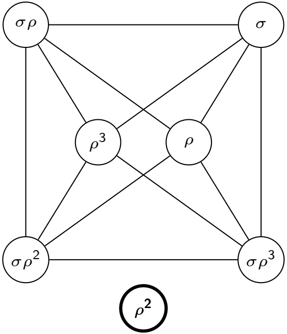


Generating Graphs

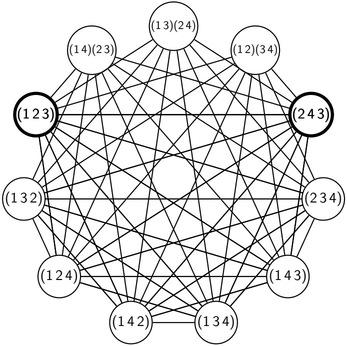
The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$.

Dihedral group D_8



Alternating group A_4

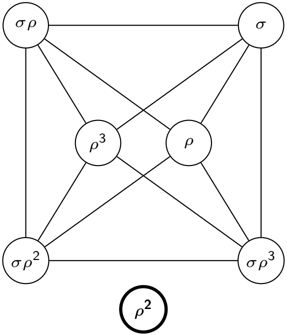


Generating Graphs

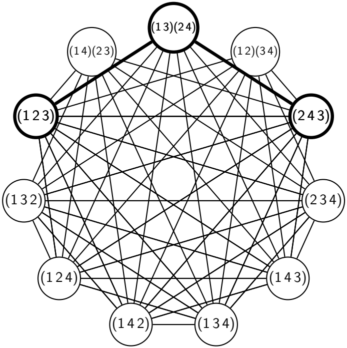
The generating graph of a group G is the graph $\Gamma(G)$ such that

- the vertices are the non-identity elements of G;
- two vertices g and h are adjacent if and only if $\langle g, h\rangle = G$.

Dihedral group D_8



Alternating group A_4



Spread and Uniform Spread

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

Spread and Uniform Spread

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 $\langle x_1, z \rangle = \cdots = \langle x_k, z \rangle = G$.

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

Spread and Uniform Spread

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

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

Theorem (Breuer, Guralnick & Kantor, 2008)

Every finite simple group G has spread two.

Spread and Uniform Spread

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

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

Theorem (Breuer, Guralnick & Kantor, 2008)

Every finite simple group G has uniform spread two.

Spread and Uniform Spread

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 $\langle x_1, z \rangle = \cdots = \langle x_k, z \rangle = G$.

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

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

Theorem (Breuer, Guralnick & Kantor, 2008)

Every finite simple group G has uniform spread two.

Spread and Uniform Spread

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 $\langle x_1, z \rangle = \cdots = \langle x_k, z \rangle = G$.

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

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

Write $u(G)$ for the greatest integer k such that G has uniform spread k.

Theorem (Breuer, Guralnick & Kantor, 2008)

Every finite simple group G has uniform spread two.

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

Main Conjecture

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

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

Main Conjecture

A finite group is $\frac{3}{2}$-generated iff every proper quotient 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 groups are $\frac{3}{2}$-generated?

Main Conjecture

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

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

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

Main Conjecture

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

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

Note: A group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for a simple group T.

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

Main Conjecture

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

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

Note: A group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for a simple group T.

Examples: $G = S_n$ (with $T = A_n$); $G = PGL_n(q)$ (with $T = PSL_n(q)$).

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

Main Conjecture

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

Strategy: Show $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

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

Main Conjecture

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

Strategy: Show $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Alternating groups	Brenner & Wiegold, 1975 & 1980
Sporadic groups	Breuer, Guralnick & Kantor, 2008

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

Main Conjecture

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

Strategy: Show $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Alternating groups	Brenner & Wiegold, 1975 & 1980
Sporadic groups	Breuer, Guralnick & Kantor, 2008

Classical groups	Linear groups: Burness & Guest, 2013

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

Main Conjecture

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

Strategy: Show $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Alternating groups	Brenner & Wiegold, 1975 & 1980
Sporadic groups	Breuer, Guralnick & Kantor, 2008

Classical groups	Linear groups: Burness & Guest, 2013

Classical groups	Symplectic groups, Orthogonal groups, Unitary groups
Exceptional groups	

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

Main Conjecture

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

Strategy: Show $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Alternating groups	Brenner & Wiegold, 1975 & 1980
Sporadic groups	Breuer, Guralnick & Kantor, 2008

Classical groups	Linear groups: Burness & Guest, 2013

Classical groups	Symplectic groups, Orthogonal groups, Unitary groups
Exceptional groups	

Project: Show $\langle T, g \rangle$ has strong spread properties when T is of Lie type.

Symplectic Groups

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Define $Sp_n(q) = \{A \in GL_n(q) \mid f(vA, wA) = f(v, w) \text{ for all } v, w \in V\}$.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Define $Sp_n(q) = \{A \in GL_n(q) \mid f(vA, wA) = f(v, w) \text{ for all } v, w \in V\}$.

What is $\mathrm{Aut}(T)$?

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Define $Sp_n(q) = \{A \in GL_n(q) \mid f(vA, wA) = f(v, w) \text{ for all } v, w \in V\}$.

What is $\mathrm{Aut}(T)$?

Define $\sigma\colon T \to T$ as $(a_{ij})\sigma = (a_{ij}^p)$.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Define $Sp_n(q) = \{A \in GL_n(q) \mid f(vA, wA) = f(v, w) \text{ for all } v, w \in V\}$.

What is $\mathrm{Aut}(T)$?

Define $\sigma\colon T \to T$ as $(a_{ij})\sigma = (a_{ij}^p)$. Define $\delta = [\alpha I_{n/2}, I_{n/2}]$ for $\mathbb{F}_q^\times = \langle \alpha \rangle$.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Define $Sp_n(q) = \{A \in GL_n(q) \mid f(vA, wA) = f(v, w) \text{ for all } v, w \in V\}$.

What is $\mathrm{Aut}(T)$?

Define $\sigma \colon T \to T$ as $(a_{ij})\sigma = (a_{ij}^p)$. Define $\delta = [\alpha I_{n/2}, I_{n/2}]$ for $\mathbb{F}_q^\times = \langle \alpha \rangle$.

If $n \neq 4$, $\mathrm{Aut}(T) = T{:}\langle \sigma \rangle$ for even q and $\mathrm{Aut}(T) = T{:}\langle \delta, \sigma \rangle$ for odd q.

Symplectic Groups

Let $q = p^k$ be a prime power and let $n \geq 4$ be even. Let $V = \mathbb{F}_q^n$.

Write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$.

What is T?

Let f be a non-degenerate alternating bilinear form on V.

Define $Sp_n(q) = \{A \in GL_n(q) \mid f(vA, wA) = f(v, w) \text{ for all } v, w \in V\}$.

What is $\mathrm{Aut}(T)$?

Define $\sigma\colon T \to T$ as $(a_{ij})\sigma = (a_{ij}^p)$. Define $\delta = [\alpha I_{n/2}, I_{n/2}]$ for $\mathbb{F}_q^\times = \langle \alpha \rangle$.

If $n \neq 4$, $\mathrm{Aut}(T) = T{:}\langle \sigma \rangle$ for even q and $\mathrm{Aut}(T) = T{:}\langle \delta, \sigma \rangle$ for odd q.

Theorem (H, 2016)

If $n \neq 4$ then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

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

Suppose that for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$. Then G has uniform spread k with respect to the conjugacy class 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

Suppose that for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$. Then G has uniform spread k with respect to the conjugacy class s^G.

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

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

Suppose that for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$. Then G has uniform spread k with respect to the conjugacy class s^G.

$\langle x, s^g\rangle \neq G \implies x$ lies in a maximal subgroup of G 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

Suppose that for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$. Then G has uniform spread k with respect to the conjugacy class s^G.

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

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

Suppose that for any element $x \in G$ of prime order $P(x, s) < \frac{1}{k}$. Then G has uniform spread k with respect to the conjugacy class s^G.

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

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

Suppose that for any element $x \in G$ of prime order $P(x,s) < \frac{1}{k}$. Then G has uniform spread k with respect to the conjugacy class s^G.

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

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

Lemma 2

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

Probabilistic Method

Summary of the probabilistic method:

Probabilistic Method

Summary of the probabilistic method:

1. Choose an element $s \in G$.

Probabilistic Method

Summary of the probabilistic method:

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

Probabilistic Method

Summary of the probabilistic method:

1. Choose an element $s \in G$.
2. Determine the maximal subgroups $\mathcal{M}(G, s)$.
3. Calculate the probability

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

Probabilistic Method

Summary of the probabilistic method:

1. Choose an element $s \in G$.
2. Determine the maximal subgroups $\mathcal{M}(G, s)$.
3. Calculate the probability

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

Example to demonstrate the method:

Probabilistic Method

Summary of the probabilistic method:

1. Choose an element $s \in G$.
2. Determine the maximal subgroups $\mathcal{M}(G, s)$.
3. Calculate the probability

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

Example to demonstrate the method:

Let $q = 2^k$ and $n \equiv 2 \pmod 4$.

Probabilistic Method

Summary of the probabilistic method:

1. Choose an element $s \in G$.
2. Determine the maximal subgroups $\mathcal{M}(G, s)$.
3. Calculate the probability

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

Example to demonstrate the method:

Let $q = 2^k$ and $n \equiv 2 \pmod 4$. Then $T = Sp_n(q)$ and $\mathrm{Aut}(T) = T{:}\langle \sigma \rangle$.

Probabilistic Method

Summary of the probabilistic method:

1. Choose an element $s \in G$.
2. Determine the maximal subgroups $\mathcal{M}(G, s)$.
3. Calculate the probability

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

Example to demonstrate the method:

Let $q = 2^k$ and $n \equiv 2 \pmod 4$. Then $T = Sp_n(q)$ and $\mathrm{Aut}(T) = T{:}\langle \sigma \rangle$.

So $G = Sp_n(q){:}\langle \sigma^i \rangle$.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

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

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

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

Observation 2: $s^e \in Sp_n(q)$

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

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

Observation 2: $s^e \in Sp_n(q)$

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

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

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

Observation 2: $s^e \in Sp_n(q)$

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

Question: Which elements in $Sp_n(q)$ arise as s^e for some $s \in Sp_n(q)\sigma^i$?

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

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

Observation 2: $s^e \in Sp_n(q)$

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

Question: Which elements in $Sp_n(q)$ arise as s^e for some $s \in Sp_n(q)\sigma^i$?

The Shintani map is a bijection (with other nice properties) between $Sp_n(q)$-classes in $Sp_n(q)\sigma^i$ and $Sp_n(q_0)$-classes in $Sp_n(q_0) < Sp_n(q)$.

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

1. Choose an element $s \in G$.

Let σ^i have order $e > 1$ and write $q = q_0^e$.

Observation 1: $s \notin Sp_n(q)$

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

Observation 2: $s^e \in Sp_n(q)$

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

Question: Which elements in $Sp_n(q)$ arise as s^e for some $s \in Sp_n(q)\sigma^i$?

The Shintani map is a bijection (with other nice properties) between $Sp_n(q)$-classes in $Sp_n(q)\sigma^i$ and $Sp_n(q_0)$-classes in $Sp_n(q_0) < Sp_n(q)$.

For each $z \in Sp_n(q_0)$, $z = a^{-1}s^e a$ for some $s \in Sp_n(q)\sigma^i$ and $a \in Sp_n(\overline{\mathbb{F}_q})$.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

Choose s such that

$$s^e = \left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in Sp_n(q_0)$$

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

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

Choose s such that

$$s^e = \left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in Sp_n(q_0)$$

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

Key features: A power of s^e has an $(n-2)$-dimensional 1-eigenspace.
The eigenvalues of s^e are highly restricted.

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

Choose s such that

$$s^e = \left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array}\right) \in Sp_n(q_0)$$

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

Key features: A power of s^e has an $(n-2)$-dimensional 1-eigenspace.
The eigenvalues of s^e are highly restricted.

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

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

Choose s such that

$$s^e = \left(\begin{array}{c|c} A_1 & \\ \hline & A_2 \end{array} \right) \in Sp_n(q_0)$$

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

Key features: A power of s^e has an $(n-2)$-dimensional 1-eigenspace.
The eigenvalues of s^e are highly restricted.

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

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).*

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

3. Calculate the probability $P(x,s)$.

Recall that

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

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

3 Calculate the probability $P(x,s)$.

Recall that

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

Method 1

Directly study G-classes and H-classes, paying close attention to fusing.

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even, $n \equiv 2 \pmod 4$

3 Calculate the probability $P(x,s)$.

Recall that

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

Method 1

Directly study G-classes and H-classes, paying close attention to fusing.

Method 2

Use very general results.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even, $n \equiv 2 \pmod 4$

3 Calculate the probability $P(x,s)$.

Recall that

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

Method 1

Directly study G-classes and H-classes, paying close attention to fusing.

Method 2

Use very general results. For example, by a theorem of Burness (2007),

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

for $\varepsilon \approx \frac{1}{2}$, provided that H is not in $\mathcal{C}_1$.

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ and write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ *and write* $G = \langle T, g \rangle$ *where* $T = PSp_n(q)$ *and* $g \in \mathrm{Aut}(T)$*. Then* $u(G) \geq 2$ *and* $u(G) \to \infty$ *as* $q \to \infty$*.*

Future Work: Prove similar results for all almost simple groups of Lie type.

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ and write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

Future Work: Prove similar results for all almost simple groups of Lie type.

Generating Graphs:

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ and write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

Future Work: Prove similar results for all almost simple groups of Lie type.

Generating Graphs:

- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ *and write* $G = \langle T, g \rangle$ *where* $T = PSp_n(q)$ *and* $g \in \mathrm{Aut}(T)$*. Then* $u(G) \geq 2$ *and* $u(G) \to \infty$ *as* $q \to \infty$*.*

Future Work: Prove similar results for all almost simple groups of Lie type.

Generating Graphs:

- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ and write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

Future Work: Prove similar results for all almost simple groups of Lie type.

Generating Graphs:

- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?
- When does $\Gamma(G)$ have a Hamiltonian cycle?

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ and write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

Future Work: Prove similar results for all almost simple groups of Lie type.

Generating Graphs:

- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?
- When does $\Gamma(G)$ have a Hamiltonian cycle?
- When is $G \ncong H$ but $\Gamma(G) \cong \Gamma(H)$?

Further Directions

Theorem (H, 2016)

Let $n \neq 4$ and write $G = \langle T, g \rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $u(G) \geq 2$ and $u(G) \to \infty$ as $q \to \infty$.

Future Work: Prove similar results for all almost simple groups of Lie type.

Generating Graphs:

- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?
- When does $\Gamma(G)$ have a Hamiltonian cycle?
- When is $G \ncong H$ but $\Gamma(G) \cong \Gamma(H)$?

Question: Is there a finite group with spread exactly one?