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

Scott Harper

(University of Bristol)

Cambridge Junior Algebra Seminar

4th March 2016

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

Scott Harper

(University of Bristol)

Cambridge Junior Algebra Seminar

4th March 2016

Generating Finite Groups

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

Write $d(G)$ for the least d such that G is d-generated.

Generating Finite Groups

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

Write $d(G)$ for the least d such that G is d-generated.

Examples

Cyclic groups $d(G) = 1$ if and only if G is cyclic

Generating Finite Groups

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

Write $d(G)$ for the least d such that G is d-generated.

Examples

Cyclic groups $d(G) = 1$ if and only if G is cyclic

Dihedral group $d(D_{2n}) = 2$ since $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = \mathrm{id}, \sigma\rho\sigma = \rho^{-1} \rangle$

Generating Finite Groups

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

Write $d(G)$ for the least d such that G is d-generated.

Examples

Cyclic groups $d(G) = 1$ if and only if G is cyclic

Dihedral group $d(D_{2n}) = 2$ since $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = \mathrm{id}, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric group $d(S_n) \leq 2$ since $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Generating Finite Groups

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

Write $d(G)$ for the least d such that G is d-generated.

Examples

Cyclic groups $d(G) = 1$ if and only if G is cyclic

Dihedral group $d(D_{2n}) = 2$ since $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = \mathrm{id}, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric group $d(S_n) \leq 2$ since $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Alternating groups $d(A_n) \leq 2$ since

– 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.

Write $d(G)$ for the least d such that G is d-generated.

Examples

Cyclic groups $d(G) = 1$ if and only if G is cyclic

Dihedral group $d(D_{2n}) = 2$ since $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = \mathrm{id}, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric group $d(S_n) \leq 2$ since $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Alternating groups $d(A_n) \leq 2$ since

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

Elementary abelian $d(C_2^n) = n$

Generating Finite Groups

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

Write $d(G)$ for the least d such that G is d-generated.

Examples

Cyclic groups $d(G) = 1$ if and only if G is cyclic

Dihedral group $d(D_{2n}) = 2$ since $D_{2n} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = \mathrm{id}, \sigma\rho\sigma = \rho^{-1} \rangle$

Symmetric group $d(S_n) \leq 2$ since $S_n = \langle (1\,2), (1\,2\,\ldots\,n) \rangle$

Alternating groups $d(A_n) \leq 2$ since

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

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

Elementary abelian $d(C_2^n) = n$

Are other important classes of groups 2-generated?

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups

Alternating groups

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups

Alternating groups

Groups of Lie type

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups

Alternating groups

Groups of Lie type

Sporadic groups

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups — Cyclic groups are 1-generated.

Alternating groups

Groups of Lie type

Sporadic groups

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups: Cyclic groups are 1-generated.

Alternating groups: If n is odd then $A_n = \langle (1\,2\,3), (1\,2\,\ldots\,n) \rangle$.
If n is even then $A_n = \langle (1\,2\,3), (2\,3\,\ldots\,n) \rangle$.

Groups of Lie type

Sporadic groups

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups	Cyclic groups are 1-generated.
Alternating groups	If n is odd then $A_n = \langle (1\,2\,3), (1\,2\,\ldots\,n) \rangle$. If n is even then $A_n = \langle (1\,2\,3), (2\,3\,\ldots\,n) \rangle$.
Groups of Lie type	Steinberg, 1962
Sporadic groups	

Generating Finite Simple Groups

Theorem

Every finite simple group is 2-generated.

Proof

By the CFSG we can consider the following cases.

Cyclic groups	Cyclic groups are 1-generated.
Alternating groups	If n is odd then $A_n = \langle (1\,2\,3), (1\,2\,\ldots\,n) \rangle$. If n is even then $A_n = \langle (1\,2\,3), (2\,3\,\ldots\,n) \rangle$.
Groups of Lie type	Steinberg, 1962
Sporadic groups	Aschbacher & Guralnick, 1984

∎

Netto's Conjecture

If we arbitrarily select two or more substitutions of n elements, it is to be regarded as extremely probable that the group of lowest order which contains these is the symmetric group, or at least the alternating group. In the case of two substitutions the probability in favor of the symmetric group may be taken as about $\frac{3}{4}$, and in favor of the alternating, but not symmetric, group as about $\frac{1}{4}$. In order that any given substitutions may generate a group which is only a part of the $n!$ possible substitutions, very special relations are necessary, and it is highly improbable that arbitrarily chosen substitutions $s_i = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix}$ should satisfy these conditions. The exception most likely to occur would be that all the given substitutions were severally equivalent to an even number of transpositions and would consequently generate the alternating group.

E. Netto, *The theory of substitutions and its application to algebra*,
Trans. F. N. Cole, Ann Arbor, Michigan, (1892)

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write

$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write
$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write
$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Netto, 1882 Conjecture: $P(A_n)$ is "about" 1

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write

$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Netto, 1882	Conjecture: $P(A_n)$ is "about" 1
Dixon, 1969	Confirmed that $P(A_n) \to 1$ as $n \to \infty$

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write

$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x, y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Netto, 1882	Conjecture: $P(A_n)$ is "about" 1
Dixon, 1969	Confirmed that $P(A_n) \to 1$ as $n \to \infty$ Conjecture: $P(G) \to 1$ as $\lvert G\rvert \to \infty$

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write
$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Netto, 1882	Conjecture: $P(A_n)$ is "about" 1
Dixon, 1969	Confirmed that $P(A_n) \to 1$ as $n \to \infty$ Conjecture: $P(G) \to 1$ as $\lvert G\rvert \to \infty$
Kantor & Lubotzky, 1990	Dixon's conjecture confirmed for G classical

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write

$$P(G) = \frac{|\{(x, y) \in G \times G \mid \langle x, y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Netto, 1882	Conjecture: $P(A_n)$ is "about" 1
Dixon, 1969	Confirmed that $P(A_n) \to 1$ as $n \to \infty$ Conjecture: $P(G) \to 1$ as $|G| \to \infty$
Kantor & Lubotzky, 1990	Dixon's conjecture confirmed for G classical
Liebeck & Shalev, 1995	Dixon's conjecture extended to G exceptional

Simple Groups: It is possible; is it probable?

Let G be a finite simple group.

Write

$$P(G) = \frac{|\{(x,y) \in G \times G \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Asymptotic Results

Netto, 1882	Conjecture: $P(A_n)$ is "about" 1
Dixon, 1969	Confirmed that $P(A_n) \to 1$ as $n \to \infty$ Conjecture: $P(G) \to 1$ as $\lvert G\rvert \to \infty$
Kantor & Lubotzky, 1990	Dixon's conjecture confirmed for G classical
Liebeck & Shalev, 1995	Dixon's conjecture extended to G exceptional

Lower Bound

Menezes, Quick & Roney-Dougal, 2013

$P(G) \geq \frac{53}{90}$ with equality if and only if $G = A_6$.

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

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

Conjecture (Steinberg, 1962)

Every non-identity element of a finite simple group is in a generating pair.

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

Conjecture (Steinberg, 1962)

Every non-identity element of a finite simple group is in a generating pair.

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

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

Conjecture (Steinberg, 1962)

Every non-identity element of a finite simple group is in a generating pair.

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

Conjecture (Steinberg, 1962)

Every non-identity element of a finite simple group is in a generating pair.

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.

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

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

Conjecture (Steinberg, 1962)

Every non-identity element of a finite simple group is in a generating pair.

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.

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.

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

Conjecture (Steinberg, 1962)

Every non-identity element of a finite simple group is in a generating pair.

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.

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.

Theorem (Breuer, Guralnick & Kantor, 2008)

For a finite simple group G, $s(G) \geq 2$.

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

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

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

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

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

Groups such that all proper quotients are cyclic?

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

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

Groups such that all proper quotients are cyclic?

Proposition

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

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

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

Groups such that all proper quotients are cyclic?

Proposition

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

Proof

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

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

Groups such that all proper quotients are cyclic?

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 $1 \neq n \in N$.

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

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

Groups such that all proper quotients are cyclic?

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 $\langle x, n \rangle = G$.

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

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

Groups such that all proper quotients are cyclic?

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

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

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

Groups such that all proper quotients are cyclic?

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, $G/N = \langle xN \rangle$.

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

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

Groups such that all proper quotients are cyclic?

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. ∎

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

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

Groups such that all proper quotients are cyclic?

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 $\langle g, h \rangle = G$.

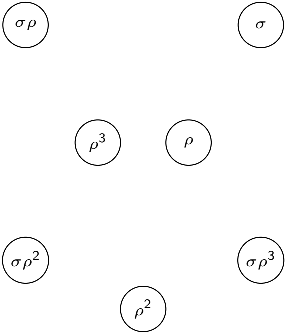
Dihedral group D_8

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

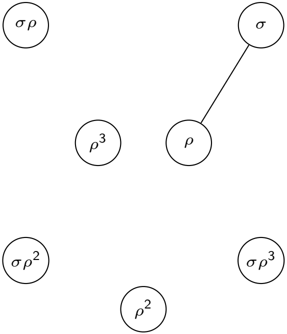


Generating Graphs

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

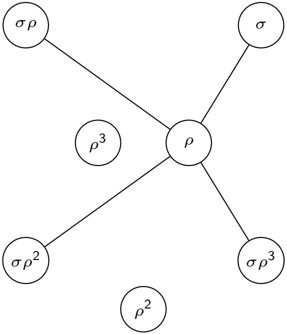


Generating Graphs

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

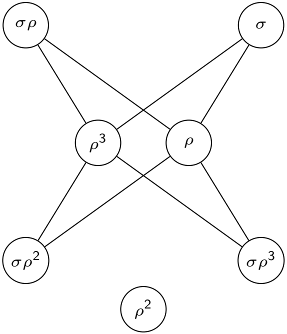


Generating Graphs

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

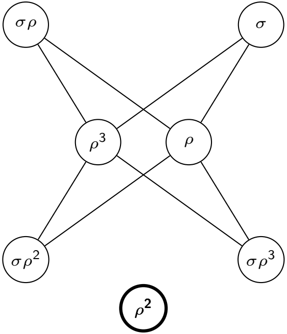


Generating Graphs

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

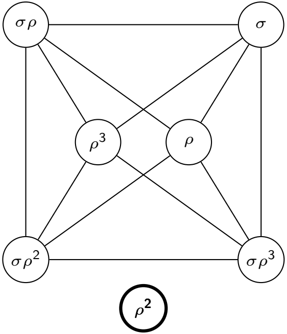


Generating Graphs

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 $\langle g, h \rangle = G$.

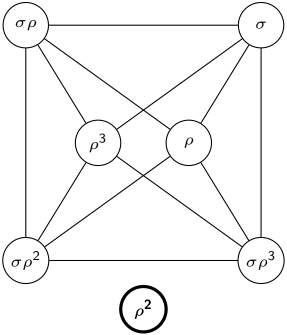
Dihedral group D_8



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

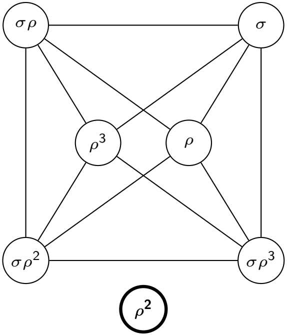


Alternating group A_4

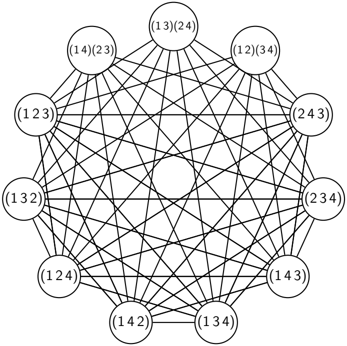
The generating graph of a group G is the graph $\Gamma(G)$ such that

- 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



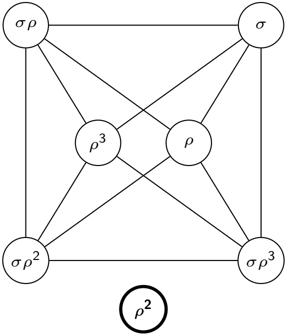
Alternating group A_4



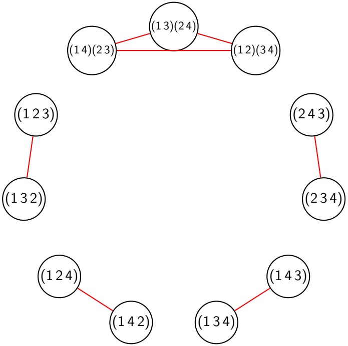
The generating graph of a group G is the graph $\Gamma(G)$ such that

- 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

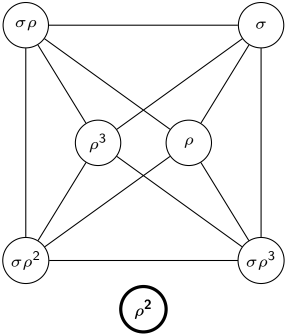


Generating Graphs

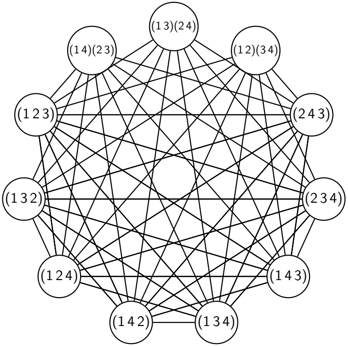
The generating graph of a group G is the graph $\Gamma(G)$ such that

- 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

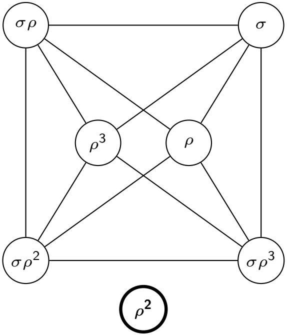


Generating Graphs

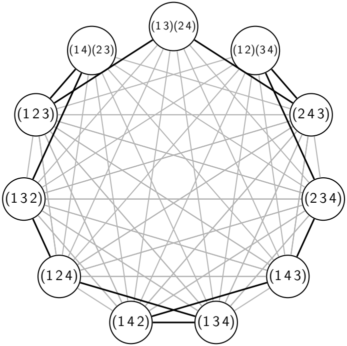
The generating graph of a group G is the graph $\Gamma(G)$ such that

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

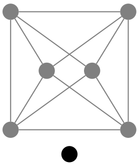
Dihedral group D_8



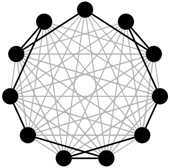
Alternating group A_4



Generating Graphs

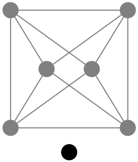


- $\Gamma(G)$ is disconnected and, moreover, has isolated vertices (i.e. $s(G) = 0$).

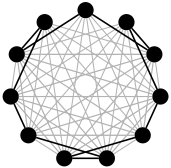


- $\Gamma(G)$ is connected and has diameter 2 (i.e $s(G) \geq 2$).
- $\Gamma(G)$ has a Hamiltonian cycle.

Generating Graphs

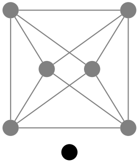


- $\Gamma(G)$ is disconnected and, moreover, has isolated vertices (i.e. $s(G) = 0$).

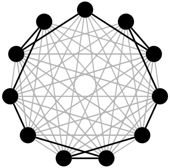


- $\Gamma(G)$ is connected and has diameter 2 (i.e $s(G) \geq 2$).
- $\Gamma(G)$ has a Hamiltonian cycle.

Other questions about $\Gamma(G)$:



- $\Gamma(G)$ is disconnected and, moreover, has isolated vertices (i.e. $s(G) = 0$).

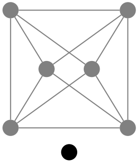


- $\Gamma(G)$ is connected and has diameter 2 (i.e $s(G) \geq 2$).
- $\Gamma(G)$ has a Hamiltonian cycle.

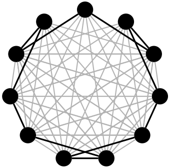
Other questions about $\Gamma(G)$:

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

Generating Graphs



- $\Gamma(G)$ is disconnected and, moreover, has isolated vertices (i.e. $s(G) = 0$).

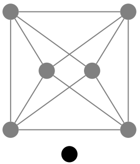


- $\Gamma(G)$ is connected and has diameter 2 (i.e $s(G) \geq 2$).
- $\Gamma(G)$ has a Hamiltonian cycle.

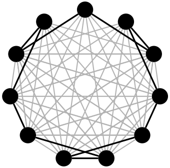
Other questions about $\Gamma(G)$:

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

Generating Graphs



- $\Gamma(G)$ is disconnected and, moreover, has isolated vertices (i.e. $s(G) = 0$).



- $\Gamma(G)$ is connected and has diameter 2 (i.e $s(G) \geq 2$).
- $\Gamma(G)$ has a Hamiltonian cycle.

Other questions about $\Gamma(G)$:

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

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

Main Conjecture

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

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

Main Conjecture

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

Main Conjecture

A finite group 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,

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

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

Main Conjecture

A finite group 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,

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

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 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,

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

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

Progress so far

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

Progress so far

Alternating groups	Symmetric groups: Brenner & Wiegold, 1975 & 1980
	Extensions of A_6: Computation

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

Progress so far

Alternating groups	Symmetric groups: Brenner & Wiegold, 1975 & 1980
	Extensions of A_6: Computation
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 that $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Progress so far

Alternating groups	Symmetric groups: Brenner & Wiegold, 1975 & 1980
	Extensions of A_6: Computation
Sporadic groups	Breuer, Guralnick & Kantor, 2008
Classical 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 that $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Progress so far

Alternating groups	Symmetric groups: Brenner & Wiegold, 1975 & 1980
	Extensions of A_6: Computation
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 that $\langle T, g \rangle$ is $\frac{3}{2}$-generated for T simple and $g \in \mathrm{Aut}(T)$.

Progress so far

Alternating groups	Symmetric groups: Brenner & Wiegold, 1975 & 1980
	Extensions of A_6: Computation
Sporadic groups	Breuer, Guralnick & Kantor, 2008
Classical groups	Linear groups: Burness & Guest, 2013

Problem

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

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.

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

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.

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.

A group G has uniform spread k if there exists a conjugacy class C such that for any distinct $x_1, \ldots, x_k \in G \setminus 1$ 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.

Many of the earlier results on spread, in fact, established uniform spread.

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.

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

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

Lemma 2

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

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1. Choose $s \in A_5$ by studying maximal subgroups

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1. Choose $s \in A_5$ by studying maximal subgroups

Maximal subgroups of A_5:

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1. Choose $s \in A_5$ by studying maximal subgroups

Maximal subgroups of A_5:

- 10 isomorphic to S_3 (Example: $\langle (1\,2\,3), (1\,2)(4\,5) \rangle$);

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1 Choose $s \in A_5$ by studying maximal subgroups

Maximal subgroups of A_5:

- 10 isomorphic to S_3 (Example: $\langle (1\,2\,3), (1\,2)(4\,5) \rangle$);
- 5 isomorphic to A_4 (Example: $\langle (1\,2\,3), (2\,3\,4) \rangle$);

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1. Choose $s \in A_5$ by studying maximal subgroups

Maximal subgroups of A_5:

- 10 isomorphic to S_3 (Example: $\langle (1\,2\,3), (1\,2)(4\,5) \rangle$);
- 5 isomorphic to A_4 (Example: $\langle (1\,2\,3), (2\,3\,4) \rangle$);
- 6 isomorphic to D_{10} (Example: $\langle (1\,2\,3\,4\,5), (2\,5)(3\,4) \rangle$).

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1. Choose $s \in A_5$ by studying maximal subgroups

Maximal subgroups of A_5:

- 10 isomorphic to S_3 (Example: $\langle(1\,2\,3),(1\,2)(4\,5)\rangle$);
- 5 isomorphic to A_4 (Example: $\langle(1\,2\,3),(2\,3\,4)\rangle$);
- 6 isomorphic to D_{10} (Example: $\langle(1\,2\,3\,4\,5),(2\,5)(3\,4)\rangle$).

Choose $s = (1\,2\,3\,4\,5)$.

Example: Alternating Group A_5

Proposition

The alternating group A_5 has uniform spread (at least) two.

Proof

1. Choose $s \in A_5$ by studying maximal subgroups

Maximal subgroups of A_5:

- 10 isomorphic to S_3 (Example: $\langle (1\,2\,3), (1\,2)(4\,5) \rangle$);
- 5 isomorphic to A_4 (Example: $\langle (1\,2\,3), (2\,3\,4) \rangle$);
- 6 isomorphic to D_{10} (Example: $\langle (1\,2\,3\,4\,5), (2\,5)(3\,4) \rangle$).

Choose $s = (1\,2\,3\,4\,5)$.

Then $\mathcal{M}(A_5, s) = \{H\}$ where $H \cong D_{10}$.

Example: Alternating Group A_5

2. Calculate $P(x, s)$ by studying conjugacy classes

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3

Example: Alternating Group A_5

2 Calculate $P(x,s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x,s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x,s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

x has order 5

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $\;|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $\;|x^G \cap H| = 0$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

x has order 5 $\;|x^G| = 12$

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

x has order 5 $|x^G| = 12$ and $|x^G \cap H| = 2$

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

x has order 5 $|x^G| = 12$ and $|x^G \cap H| = 2$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{2}{12} = \frac{1}{6}$.

Example: Alternating Group A_5

2 Calculate $P(x,s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x,s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x,s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$ so $P(x,s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

x has order 5 $|x^G| = 12$ and $|x^G \cap H| = 2$ so $P(x,s) = \frac{|x^G \cap H|}{|x^G|} = \frac{2}{12} = \frac{1}{6}$.

In all cases $P(x,s) < \frac{1}{2}$.

Example: Alternating Group A_5

2 Calculate $P(x, s)$ by studying conjugacy classes

Conjugacy classes of $G = A_5$:

$$\mathrm{id}^G, (1\,2\,3)^G, (1\,2)(3\,4)^G, (1\,2\,3\,4\,5)^G, (1\,3\,5\,2\,4)^G.$$

In this case $P(x, s) \leq \frac{|x^G \cap H|}{|x^G|}$.

x has order 2 $|x^G| = 15$ and $|x^G \cap H| = 5$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{5}{15} = \frac{1}{3}$.

x has order 3 $|x^G \cap H| = 0$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = 0$.

x has order 5 $|x^G| = 12$ and $|x^G \cap H| = 2$ so $P(x, s) = \frac{|x^G \cap H|}{|x^G|} = \frac{2}{12} = \frac{1}{6}$.

In all cases $P(x, s) < \frac{1}{2}$. So $u(A_5) \geq 2$. ■

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

Progress so far

Alternating groups	Symmetric groups: Brenner & Wiegold, 1975 & 1980
	Extensions of A_6: Computation
Sporadic groups	Breuer, Guralnick & Kantor, 2008
Classical groups	Linear groups: Burness & Guest, 2013

Problem

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

Symplectic Groups

Symplectic Groups

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

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Define $T = \{A \in GL_n(q) \mid f(Av, Aw) = f(v, w) \text{ for all } v, w \in V\}$.

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Define $T = \{A \in GL_n(q) \mid f(Av, Aw) = f(v, w) \text{ for all } v, w \in V\}$.

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

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Define $T = \{A \in GL_n(q) \mid f(Av, Aw) = f(v, w) \text{ for all } v, w \in V\}$.

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

Define $\sigma \colon T \to T$ as $A\sigma = (a_{ij}^2)$ for all $A = (a_{ij}) \in T$.

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Define $T = \{A \in GL_n(q) \mid f(Av, Aw) = f(v, w) \text{ for all } v, w \in V\}$.

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

Define $\sigma\colon T \to T$ as $A\sigma = (a_{ij}^2)$ for all $A = (a_{ij}) \in T$.

If $n \neq 4$, $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$.

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Define $T = \{A \in GL_n(q) \mid f(Av, Aw) = f(v, w) \text{ for all } v, w \in V\}$.

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

Define $\sigma\colon T \to T$ as $A\sigma = (a_{ij}^2)$ for all $A = (a_{ij}) \in T$.

If $n \neq 4$, $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$. So $G = T{:}\langle \sigma^i \rangle$.

Symplectic Groups

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

Let $T = Sp_n(q)$ and let $T \leq G \leq \mathrm{Aut}(T)$.

What is T?

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

Define $T = \{A \in GL_n(q) \mid f(Av, Aw) = f(v, w) \text{ for all } v, w \in V\}$.

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

Define $\sigma\colon T \to T$ as $A\sigma = (a_{ij}^2)$ for all $A = (a_{ij}) \in T$.

If $n \neq 4$, $\mathrm{Aut}(T) = \langle T, \sigma \rangle = T{:}\langle \sigma \rangle$. So $G = T{:}\langle \sigma^i \rangle$.

Theorem (H, 2016)

For q even and $n \geq 6$, $Sp_n(q){:}\langle \sigma^i \rangle$ is $\frac{3}{2}$-generated.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

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

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

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

Crucial point: $s \notin Sp_n(q)$

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

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

Crucial point: $s \notin Sp_n(q)$ but $s^e \in Sp_n(q)$.

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

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

Crucial point: $s \notin Sp_n(q)$ but $s^e \in Sp_n(q)$.

Strategy: Choose s such that s^e lies in few maximal subgroups of G. Then s also lies in few maximal subgroups of G.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even

1. Choose $s \in G$ by studying maximal subgroups

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

Crucial point: $s \notin Sp_n(q)$ but $s^e \in Sp_n(q)$.

Strategy: Choose s such that s^e lies in few maximal subgroups of G. Then s also lies in few maximal subgroups of G.

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

1 Choose $s \in G$ by studying maximal subgroups

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

Crucial point: $s \notin Sp_n(q)$ but $s^e \in Sp_n(q)$.

Strategy: Choose s such that s^e lies in few maximal subgroups of G. Then s also lies in few maximal subgroups of G.

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

Key fact: There 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

1 Choose $s \in G$ by studying maximal subgroups

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

Crucial point: $s \notin Sp_n(q)$ but $s^e \in Sp_n(q)$.

Strategy: Choose s such that s^e lies in few maximal subgroups of G. Then s also lies in few maximal subgroups of G.

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

Key fact: There 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 $Sp_n(q_0) < Sp_n(q)$.

So for all $z \in Sp_n(q_0)$ there exists $s \in Sp_n(q)\sigma^i$ such that $s^e = z$.

Example: $G = Sp_n(q){:}\langle \sigma^i \rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

Choose s such that

$$s^e = \left(\begin{array}{c|c} J_2 & \\ \hline & A \end{array}\right) \in Sp_n(q_0)$$

where A acts irreducibly on a non-degenerate $(n-2)$-space (over $\mathbb{F}_{q_0}$).

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

Choose s such that

$$s^e = \left(\begin{array}{c|c} J_2 & \\ \hline & A \end{array}\right) \in Sp_n(q_0)$$

where A acts irreducibly on a non-degenerate $(n-2)$-space (over $\mathbb{F}_{q_0}$).

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

1 Choose $s \in G$ by studying maximal subgroups

Choose s such that

$$s^e = \left(\begin{array}{c|c} J_2 & \\ \hline & A \end{array} \right) \in Sp_n(q_0)$$

where A acts irreducibly on a non-degenerate $(n-2)$-space (over $\mathbb{F}_{q_0}$).

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).*

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

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even

1 Choose $s \in G$ by studying maximal subgroups

Choose s such that

$$s^e = \left(\begin{array}{c|c} J_2 & \\ \hline & A \end{array}\right) \in Sp_n(q_0)$$

where A acts irreducibly on a non-degenerate $(n-2)$-space (over $\mathbb{F}_{q_0}$).

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).*

- A power of s^e has an $(n-1)$-dimensional 1-eigenspace.
- The order of s^e is divisible by $q_0^{\frac{n-2}{2}} + 1$.

Example: $G = Sp_n(q){:}\langle\sigma^i\rangle$, q even

2 Calculate $P(x, s)$ by studying conjugacy classes

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

2 Calculate $P(x,s)$ by studying conjugacy classes

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

2 Calculate $P(x, s)$ by studying conjugacy classes

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

2 Calculate $P(x,s)$ by studying conjugacy classes

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

Further Directions

Future Work: Extend to all other almost simple groups of Lie type.

Further Directions

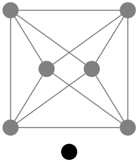
Future Work: Extend to all other almost simple groups of Lie type.

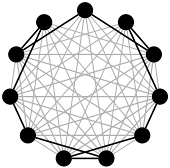
Natural Question: Do any finite groups have spread exactly one?

Further Directions

Future Work: Extend to all other almost simple groups of Lie type.

Natural Question: Do any finite groups have spread exactly one?

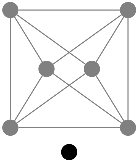


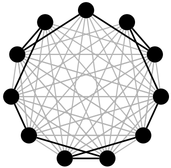


Further Directions

Future Work: Extend to all other almost simple groups of Lie type.

Natural Question: Do any finite groups have spread exactly one?





Conjecture

The following are equivalent.

- Every proper quotient of G is cyclic.
- $\Gamma(G)$ has no isolated vertices (i.e. G has spread one).
- $\Gamma(G)$ has diameter two (i.e. G has spread two).
- $\Gamma(G)$ has a Hamiltonian cycle.