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



Scott Harper (University of Bristol)

Young Researchers in Mathematics 2nd August 2016

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



Scott Harper (University of Bristol)

Young Researchers in Mathematics 2nd August 2016

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



Scott Harper (University of Bristol)

Young Researchers in Mathematics 2nd August 2016

Let G be a finite group.

We say that G is d-generated if G has a generating set of size d.

Let G be a finite group.

We say that G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

Let G be a finite group.

We say that G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

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

Let G be a finite group.

We say that G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

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

Symmetric groups are 2-generated: $S_n = \langle (12), (12 \dots n) \rangle$

Let G be a finite group.

We say that G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

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

Symmetric groups are 2-generated: $S_n = \langle (12), (12 \dots n) \rangle$

Alternating groups are 2-generated: - if *n* is odd $A_n = \langle (123), (12 \dots n) \rangle$ - if *n* is even $A_n = \langle (123), (23 \dots n) \rangle$

Let G be a finite group.

We say that G is d-generated if G has a generating set of size d.

Cyclic groups are 1-generated

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

Symmetric groups are 2-generated: $S_n = \langle (12), (12 \dots n) \rangle$

Alternating groups are 2-generated: - if *n* is odd $A_n = \langle (123), (12 \dots n) \rangle$ - if *n* is even $A_n = \langle (123), (23 \dots n) \rangle$

Are other important families of finite groups 2-generated?

Scott Harper

Finite Simple Groups

Finite Simple Groups

A group is simple if it has no proper non-trivial normal subgroups.

Theorem (The Classification of Finite Simple Groups)

Theorem (The Classification of Finite Simple Groups)

Every finite simple group is isomorphic to one of the following groups:

a cyclic group of prime order;

Theorem (The Classification of Finite Simple Groups)

- a cyclic group of prime order;
- an alternating group of degree at least 5;

Theorem (The Classification of Finite Simple Groups)

- a cyclic group of prime order;
- an alternating group of degree at least 5;
- a classical group of Lie type;

Theorem (The Classification of Finite Simple Groups)

- a cyclic group of prime order;
- an alternating group of degree at least 5;
- a classical group of Lie type;
- an exceptional group of Lie type;

Theorem (The Classification of Finite Simple Groups)

- a cyclic group of prime order;
- an alternating group of degree at least 5;
- a classical group of Lie type;
- an exceptional group of Lie type;
- one of the 26 sporadic simple groups.

Theorem (The Classification of Finite Simple Groups)

Every finite simple group is isomorphic to one of the following groups:

- a cyclic group of prime order;
- an alternating group of degree at least 5;
- a classical group of Lie type;
- an exceptional group of Lie type;
- one of the 26 sporadic simple groups.

Theorem (Steinberg, 1962; Aschbacher & Guralnick, 1984)

Every finite simple group is 2-generated.

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 $s_i = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_i & x_i & \dots & x_n \end{pmatrix}$ 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)

Public Domain: http://www.hathitrust.org/access_use#pd

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 $s_i = \begin{pmatrix} x_1 x_2 \dots x_n \\ x_i x_i \dots x_i \end{pmatrix}$ 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)

Public Domain: http://www.hathitrust.org/access_use#pd

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

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

Theorem (Dixon, 1969)

 $P(A_n)
ightarrow 1$ as $n
ightarrow \infty$.

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

Theorem (Dixon, 1969)

 $P(A_n) \rightarrow 1 \text{ as } n \rightarrow \infty.$

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

If G is simple then $P(G) \rightarrow 1$ as $|G| \rightarrow \infty$.

$$P(G) = rac{|\{(x,y) \in G imes G \mid \langle x,y
angle = G\}|}{|G|^2}.$$

Theorem (Dixon, 1969)

 $P(A_n) \rightarrow 1 \text{ as } n \rightarrow \infty.$

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

If G is simple then $P(G) \rightarrow 1$ as $|G| \rightarrow \infty$.

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

If G is simple then $P(G) \ge \frac{53}{90}$ with equality if and only if $G = A_6$.

Theorem (Stein, 1998; Guralnick & Kantor, 2000)

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

Theorem (Stein, 1998; Guralnick & Kantor, 2000)

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

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

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.

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?



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



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

Proof



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

Proof

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

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

Proof

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

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

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

Proof

Let $1 \neq N \leq G$ 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, $G/N = \langle xN \rangle$.
Proposition

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

Proof

Let $1 \neq N \leq G$ 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.

Proposition

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

Proof

Let $1 \neq N \leq G$ 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.

Main Conjecture

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

Main Conjecture

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

Need to show: For all finite groups G,

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

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

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

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

Main Conjecture

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

Need to show: For all finite groups G,

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

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

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

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

Main Conjecture

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

Need to show: For all finite groups G,

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

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

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

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

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

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

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

Alternating groupsBrenner & Wiegold, 1975 & 1980Sporadic groupsBreuer, Guralnick & Kantor, 2008

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

Alternating groups	Brenner & Wiegold, 1975 & 1980
Sporadic groups	Breuer, Guralnick & Kantor, 2008
Classical groups	Linear groups: Burness & Guest, 2013

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

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

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

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

For a prime power q and even n, the symplectic group $Sp_n(q) \leq GL_n(q)$ is the stabiliser of a non-degenerate alternating form on \mathbb{F}_q^n .

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

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

For a prime power q and even n, the symplectic group $Sp_n(q) \leq GL_n(q)$ is the stabiliser of a non-degenerate alternating form on \mathbb{F}_q^n .

Theorem (H, 2016)

Let $g \in Aut(PSp_n(q))$ then $\langle PSp_n(q), g \rangle$ is $\frac{3}{2}$ -generated.

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

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

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

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

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 D₈

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



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 D₈



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 D₈



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 D₈



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 D₈



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





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 A4



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 A4



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





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

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 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.

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.

Wider Aim: Show that the group $\langle T, g \rangle$ has strong spread properties where T is a finite group of Lie type and $g \in Aut(T)$.

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.

Wider Aim: Show that the group $\langle T, g \rangle$ has strong spread properties where T is a finite group of Lie type and $g \in Aut(T)$.

Theorem (H, 2016)

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

Then $s(G) \ge 2$ and $s(G) \to \infty$ as $q \to \infty$.

Further Questions

Further Questions

Generating Graphs:

If the isolated vertices of Γ(G) are removed then is Γ(G) connected?
Generating Graphs:

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



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



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



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



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



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





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



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





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





Generating Graphs:

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

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



Scott Harper (University of Bristol)

Young Researchers in Mathematics 2nd August 2016