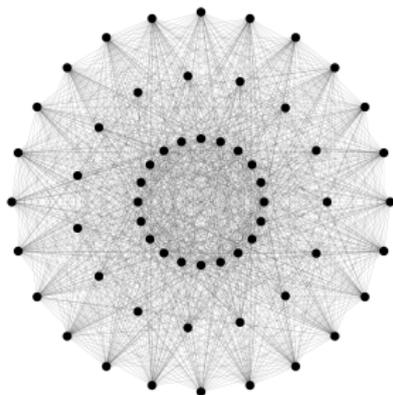


$\frac{3}{2}$ -Generation of Finite Groups

Scott Harper



Pure Postgraduate Seminar

10th March 2017

The Generation Game

Let G be a finite group.

The Generation Game

Let G be a finite group.

A subset $X \subseteq G$ is a **generating set** of G if $G = \langle X \rangle$.

The Generation Game

Let G be a finite group.

A subset $X \subseteq G$ is a **generating set** of G if $G = \langle X \rangle$.

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

The Generation Game

Let G be a finite group.

A subset $X \subseteq G$ is a **generating set** of G if $G = \langle X \rangle$.

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

Cyclic groups are 1-generated

The Generation Game

Let G be a finite group.

A subset $X \subseteq G$ is a **generating set** of G if $G = \langle X \rangle$.

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: $D_{n\text{-gon}} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

The Generation Game

Let G be a finite group.

A subset $X \subseteq G$ is a **generating set** of G if $G = \langle X \rangle$.

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: $D_{n\text{-gon}} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

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

The Generation Game

Let G be a finite group.

A subset $X \subseteq G$ is a **generating set** of G if $G = \langle X \rangle$.

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: $D_{n\text{-gon}} = \langle \sigma, \rho \mid \sigma^2 = \rho^n = 1, \sigma\rho\sigma = \rho^{-1} \rangle$

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 $A_n = \langle (123), (23 \dots n) \rangle$

It's simple . . .

It's simple . . .

How do you factorise a number a ?

It's simple . . .

How do you factorise a number a ?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \dots, \quad n_{k-1}/n_k = q_k,$$

and do this so that q_1, \dots, q_k and n_k are all prime.

It's simple . . .

How do you factorise a number a ?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \dots, \quad n_{k-1}/n_k = q_k,$$

and do this so that q_1, \dots, q_k and n_k are all prime.

(A number p is **prime** if p has exactly two divisors: 1 and p .)

It's simple . . .

How do you factorise a number a ?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \dots, \quad n_{k-1}/n_k = q_k,$$

and do this so that q_1, \dots, q_k and n_k are all prime.

(A number p is **prime** if p has exactly two divisors: 1 and p .)

How do you factorise a finite group G ?

It's simple . . .

How do you factorise a number a ?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \dots, \quad n_{k-1}/n_k = q_k,$$

and do this so that q_1, \dots, q_k and n_k are all prime.

(A number p is **prime** if p has exactly two divisors: 1 and p .)

How do you factorise a finite group G ?

Repeatedly divide by big normal subgroups:

$$G/N_1 = Q_1, \quad N_1/N_2 = Q_2, \quad \dots, \quad N_{k-1}/N_k = Q_k,$$

and do this so that Q_1, \dots, Q_k and N_k are all simple.

It's simple . . .

How do you factorise a number a ?

Repeatedly divide by big divisors

$$a/n_1 = q_1, \quad n_1/n_2 = q_2, \quad \dots, \quad n_{k-1}/n_k = q_k,$$

and do this so that q_1, \dots, q_k and n_k are all prime.

(A number p is **prime** if p has exactly two divisors: 1 and p .)

How do you factorise a finite group G ?

Repeatedly divide by big normal subgroups:

$$G/N_1 = Q_1, \quad N_1/N_2 = Q_2, \quad \dots, \quad N_{k-1}/N_k = Q_k,$$

and do this so that Q_1, \dots, Q_k and N_k are all simple.

(A group S is **simple** if S has exactly two normal subgroups: 1 and S .)

Example: The symmetry group of a triangle D_{Δ}

Example: The symmetry group of a triangle D_{Δ}

The subgroup of rotational symmetries C_3 is normal in D_{Δ} .

Example: The symmetry group of a triangle D_Δ

The subgroup of rotational symmetries C_3 is normal in D_Δ .

Then $D_\Delta/C_3 = C_2$. So the simple factors of D_Δ are C_3 and C_2 .

Example: The symmetry group of a triangle D_Δ

The subgroup of rotational symmetries C_3 is normal in D_Δ .

Then $D_\Delta/C_3 = C_2$. So the simple factors of D_Δ are C_3 and C_2 .

Theorem For a prime p , the cyclic group C_p is simple.

Example: The symmetry group of a triangle D_Δ

The subgroup of rotational symmetries C_3 is normal in D_Δ .

Then $D_\Delta/C_3 = C_2$. So the simple factors of D_Δ are C_3 and C_2 .

Theorem For a prime p , the cyclic group C_p is simple.

Example: The symmetric group S_n for $n \geq 5$

Example: The symmetry group of a triangle D_Δ

The subgroup of rotational symmetries C_3 is normal in D_Δ .

Then $D_\Delta/C_3 = C_2$. So the simple factors of D_Δ are C_3 and C_2 .

Theorem For a prime p , the cyclic group C_p is simple.

Example: The symmetric group S_n for $n \geq 5$

The subgroup of even permutations A_n is normal in S_n .

Example: The symmetry group of a triangle D_Δ

The subgroup of rotational symmetries C_3 is normal in D_Δ .

Then $D_\Delta/C_3 = C_2$. So the simple factors of D_Δ are C_3 and C_2 .

Theorem For a prime p , the cyclic group C_p is simple.

Example: The symmetric group S_n for $n \geq 5$

The subgroup of even permutations A_n is normal in S_n .

Then $S_n/A_n = C_2$. So the simple factors of S_n are A_n and C_2 .

Example: The symmetry group of a triangle D_Δ

The subgroup of rotational symmetries C_3 is normal in D_Δ .

Then $D_\Delta/C_3 = C_2$. So the simple factors of D_Δ are C_3 and C_2 .

Theorem For a prime p , the cyclic group C_p is simple.

Example: The symmetric group S_n for $n \geq 5$

The subgroup of even permutations A_n is normal in S_n .

Then $S_n/A_n = C_2$. So the simple factors of S_n are A_n and C_2 .

Theorem For $n \geq 5$, the alternating group A_n is simple.

Theorem (The Classification of Finite Simple Groups)

Every finite simple group is isomorphic to one of the following 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)

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

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 group of Lie type

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 group of Lie type (e.g. $\text{PSL}_n(q)$)

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 group of Lie type (e.g. $\text{PSL}_n(q)$)
- one of the 26 sporadic simple groups.

The Periodic Table Of Finite Simple Groups

$0, C_2, Z_3$	Dynkin Diagrams of Simple Lie Algebras														C_2				
1															2				
$A_1(4), A_1(5)$	$A_2(2)$													$G_2(2)'$	C_3				
A_5	$A_1(7)$													${}^3A_3(4)$	2				
168	168													$B_2(3)$	$C_3(3)$	$D_4(2)$	${}^2D_4(2^2)$	${}^2A_2(9)$	C_3
60	360													25920	436800000	174182400	197406720	6048	3
$A_1(9), A_1(2)'$	${}^3G_2(3)'$													$B_2(4)$	$C_3(5)$	$D_4(3)$	${}^2D_4(3^2)$	${}^2A_2(16)$	C_5
A_6	$A_1(8)$													979200	226944	4021790400	3115236841920	82400	5
360	504													46784750	454489800	2349929548800	25101579358400	126000	C_7
A_7	$A_1(11)$	$E_6(2)$	$E_7(2)$	$E_8(2)$	$F_4(2)$	$G_2(3)$	${}^3D_4(2^3)$	${}^2E_6(2^2)$	${}^2B_2(2^3)$	${}^2F_4(2)'$	${}^2G_2(3^3)$	$B_3(2)$	$C_4(3)$	$D_5(2)$	${}^2D_5(2^2)$	${}^2A_2(25)$	C_7		
2520	660	21844187032	49537529488	3311128	3311128	4245496	211341312	79552479803	29120	17971200	1087544472	1451520	46784750	454489800	2349929548800	25101579358400	126000	7	
A_8	$A_1(13)$	$E_6(3)$	$E_7(3)$	$E_8(3)$	$F_4(3)$	$G_2(4)$	${}^3D_4(3^3)$	${}^2E_6(3^2)$	${}^2B_2(2^5)$	${}^2F_4(2^3)$	${}^2G_2(3^5)$	$B_2(5)$	$C_3(7)$	$D_4(5)$	${}^2D_4(4^2)$	${}^2A_3(9)$	C_{11}		
20160	1092	1497000000000	1271000000000	573448790816	573448790816	251596800	20560831156492	4444444444444	32337600	264905352499	63936052	4680000	273457216	5411539000	67536471	29240000	3265920	11	
A_9	$A_1(17)$	$E_6(4)$	$E_7(4)$	$E_8(4)$	$F_4(4)$	$G_2(5)$	${}^3D_4(4^3)$	${}^2E_6(4^2)$	${}^2B_2(2^7)$	${}^2F_4(2^5)$	${}^2G_2(3^7)$	$B_2(7)$	$C_3(9)$	$D_5(3)$	${}^2D_4(5^2)$	${}^2A_2(64)$	C_{13}		
181440	2448	1028797000000	1222000000000	393694057280000	393694057280000	509000000	47862350	44279400	34093303480	10000000	239189938264	138297600	5422571482	1209132799	1780030328	80000000	5515776	13	
A_n	$A_n(q)$	$E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$	${}^3D_4(q^3)$	${}^2E_6(q^2)$	${}^2B_2(2^{2n+1})$	${}^2F_4(2^{2n+1})$	${}^2G_2(3^{2n+1})$	$O_{2n+1}(q)$	$PSU_n(q)$	$O_{2n}^-(q)$	${}^2D_n(q^2)$	${}^2A_n(q^2)$	Z_p		
of $\frac{1}{2}$	$\prod_{i=1}^n (q^i - 1)$	$\frac{q^6 - q^2}{(q^2 - 1)(q^3 - 1)(q^4 - 1)}$	$\frac{q^7 - 1}{(q - 1)(q^2 - 1)(q^3 - 1)(q^4 - 1)(q^5 - 1)}$	$\frac{q^8 - 1}{(q - 1)(q^2 - 1)(q^3 - 1)(q^4 - 1)(q^5 - 1)(q^6 - 1)}$	$\frac{q^4 - 1}{(q - 1)(q^2 - 1)(q^3 - 1)}$	$\frac{q^2 - 1}{(q - 1)(q^2 - 1)}$	$\frac{q^3 - 1}{(q - 1)(q^2 - 1)}$	$\frac{q^2 - 1}{(q - 1)(q^2 - 1)}$	$\frac{q^{2n+1} - 1}{(q - 1)(q^{2n+1} - 1)}$	$\frac{q^n - 1}{(q - 1)(q^n - 1)}$	$\frac{q^n - 1}{(q - 1)(q^n - 1)}$	$\frac{q^{2n} - 1}{(q^2 - 1)(q^{2n} - 1)}$	$\frac{q^{2n} - 1}{(q^2 - 1)(q^{2n} - 1)}$	$\frac{q^{2n} - 1}{(q^2 - 1)(q^{2n} - 1)}$	p				

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Ree Groups and Tits Group*
- Sporadic Groups
- Cyclic Groups

Alternates*
Symbol
Order†

M_{11}	M_{12}	M_{22}	M_{23}	M_{24}	$J(1), J(11)$	HJ	HJM	J_4	HS	McL	He	Ru
7920	95040	463520	10220160	244823040	175560	604800	50232960	86775571840	44352000	898128000	4030307200	14519414400

*The Tits group ${}^2F_4(2)'$ is not a group of Lie type, but is the center of a non-split subgroup of ${}^2F_4(2)$. It is usually given the name Tits group.

†The specific groups and families, alternate names in the upper left and other names in which they may be known. For specific non-split groups, their order is given in parentheses. All such non-split groups appear on the table except the family ${}^2F_4(2)'$.

Sz	$O'N, O-S$	3	2	1	C_{01}	F_4, D	HN	LyS	Ly	F_4, E	Th	$M(22)$	$M(23)$	$F_{4,1}, M(24)'$	F_2	F_4, M_4
Suz	$O'N$	C_{03}	C_{02}	C_{01}										$F_{2,2}^2$	B	M
448344897600	840181585920	49576436480	4236510331200	4197776300	543360000	91200000	273000	51761376	90728163	86787002	445417545440	4689451675	1255305189184	441721202400		

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 group of Lie type (e.g $\text{PSL}_n(q)$)
- one of the 26 sporadic simple groups.

Caveat mathematicae

There are many ways of putting simple groups together.

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 group of Lie type (e.g $\text{PSL}_n(q)$)
- one of the 26 sporadic simple groups.

Caveat mathematicae

There are many ways of putting simple groups together.

- Both $C_2 \times C_2$ and C_4 decompose into two copies of C_2 .

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 group of Lie type (e.g $\text{PSL}_n(q)$)
- one of the 26 sporadic simple groups.

Caveat mathematicae

There are many ways of putting simple groups together.

- Both $C_2 \times C_2$ and C_4 decompose into two copies of C_2 .
- All 49,487,365,422 groups of order 1024 decompose into ten C_2 .

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 group of Lie type (e.g $\text{PSL}_n(q)$)
- one of the 26 sporadic simple groups.

Caveat mathematicae

There are many ways of putting simple groups together.

- Both $C_2 \times C_2$ and C_4 decompose into two copies of C_2 .
- All 49,487,365,422 groups of order 1024 decompose into ten C_2 .

Theorem (Steinberg, 1962)

Every finite simple group is 2-generated.

What are the chances?

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 $s_i = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{i_1} & x_{i_2} & \dots & x_{i_n} \end{pmatrix}$ 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)

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

Let $P(G)$ be the probability that two random elements generate G .

That is,

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

Let $P(G)$ be the probability that two random elements generate G .

That is,

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

Now we can formalise Netto's idea.

Netto's Conjecture $P(A_n) \rightarrow 1$ as $n \rightarrow \infty$.

Let $P(G)$ be the probability that two random elements generate G .

That is,

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

Now we can formalise Netto's idea.

Netto's Conjecture $P(A_n) \rightarrow 1$ as $n \rightarrow \infty$.

Numerical evidence

n	5	6	7	8	9	10
$P(A_n)$	0.633	0.588	0.726	0.738	0.848	0.875

GAP computations by N. Menezes, M. Quick and C. M. Roney-Dougal

Cyclic groups of prime order

Let p be prime. Then

$$P(C_p) = \frac{p^2 - 1}{p^2}$$

and so $P(C_p) \rightarrow 1$ as $p \rightarrow \infty$.

Cyclic groups of prime order

Let p be prime. Then

$$P(C_p) = \frac{p^2 - 1}{p^2}$$

and so $P(C_p) \rightarrow 1$ as $p \rightarrow \infty$.

Eighty years later . . .

Cyclic groups of prime order

Let p be prime. Then

$$P(C_p) = \frac{p^2 - 1}{p^2}$$

and so $P(C_p) \rightarrow 1$ as $p \rightarrow \infty$.

Eighty years later . . .

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of **probabilistic group theory**.

Cyclic groups of prime order

Let p be prime. Then

$$P(C_p) = \frac{p^2 - 1}{p^2}$$

and so $P(C_p) \rightarrow 1$ as $p \rightarrow \infty$.

Eighty years later ...

Between 1965 and 1968, Paul Erdős and Pál Turán published several papers on random permutations and this was the birth of the field of **probabilistic group theory**.

Using the work of Erdős and Turán, Dixon proved Netto's conjecture.

Theorem (Dixon, 1969)

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

Dixon replaced one conjecture with another even bolder one.

Dixon replaced one conjecture with another even bolder one.

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

Dixon replaced one conjecture with another even bolder one.

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

As a result of the Classification, the following have been proved.

Dixon replaced one conjecture with another even bolder one.

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

As a result of the Classification, the following have been proved.

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

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

Dixon replaced one conjecture with another even bolder one.

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

As a result of the Classification, the following have been proved.

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

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

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

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

Dixon replaced one conjecture with another even bolder one.

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

As a result of the Classification, the following have been proved.

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

Summary: It's easy to generate a finite simple group with two elements.

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

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

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

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

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

Theorem (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 is contained in 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 is contained in 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 is contained in 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**?

Proposition

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

Proposition

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

Proof

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 $1 \neq n \in N$.

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

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

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

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. ■

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

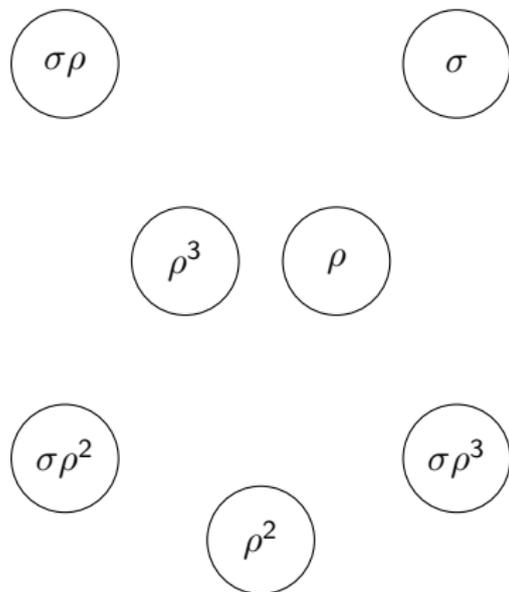
Dihedral group D_n

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_4

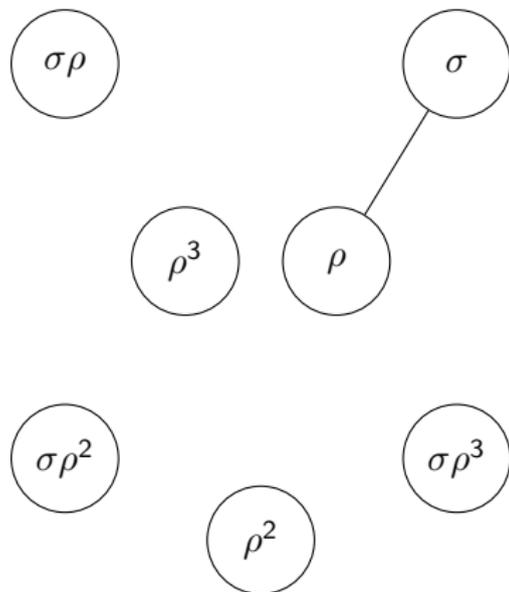


Generating Graphs

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_4

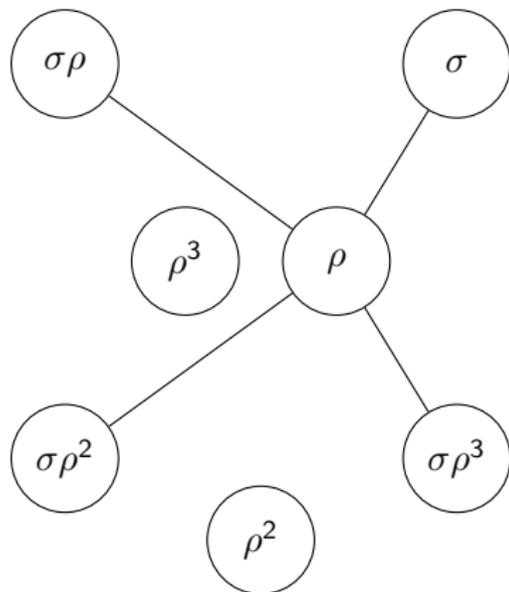


Generating Graphs

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_4

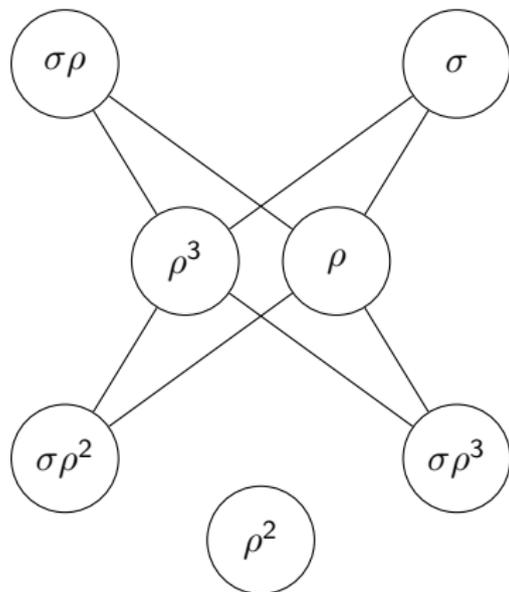


Generating Graphs

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_4

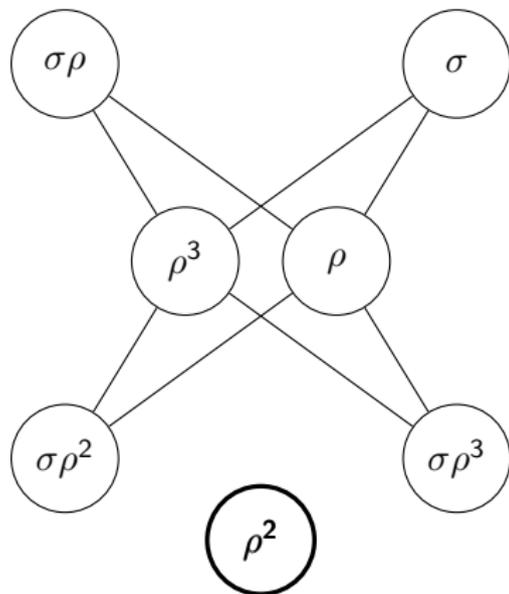


Generating Graphs

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_4

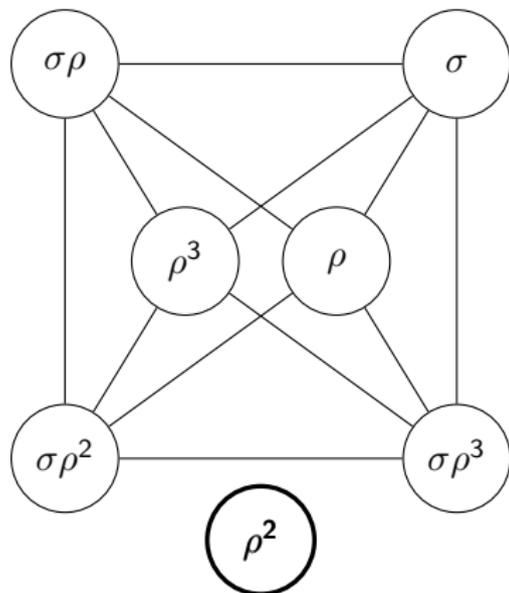


Generating Graphs

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_4

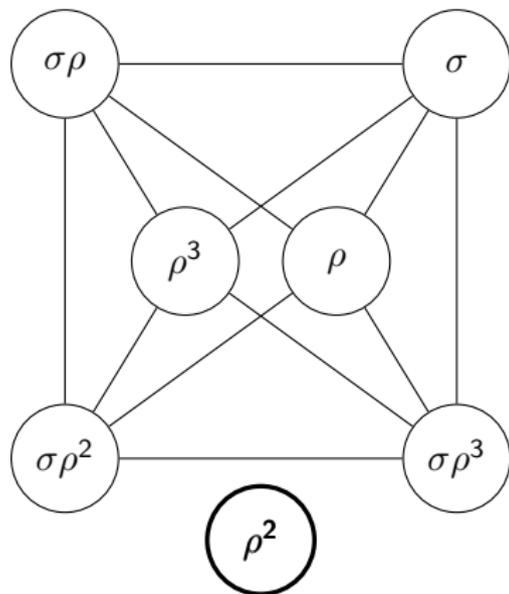


Generating Graphs

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_4



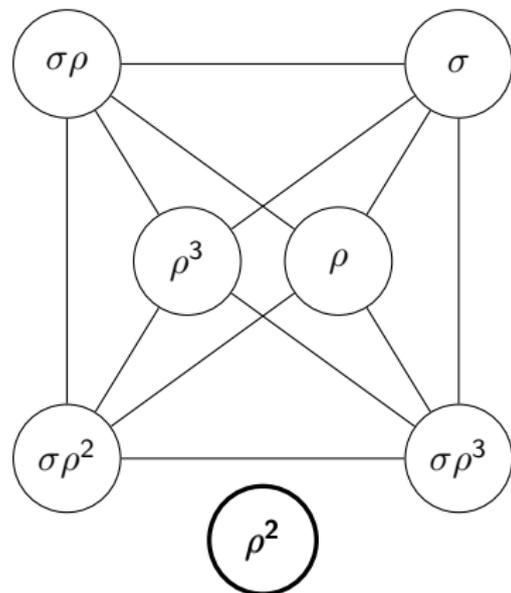
Alternating group A_4

Generating Graphs

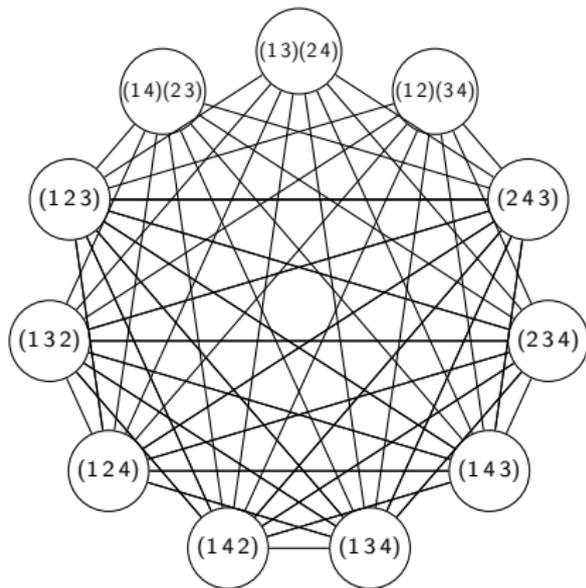
The **generating graph** of a group G is the graph $\Gamma(G)$ such that

- 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_{\square}



Alternating group A_4

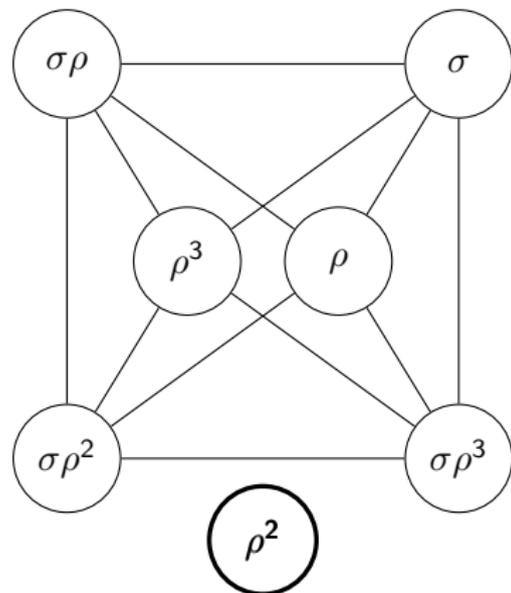


Generating Graphs

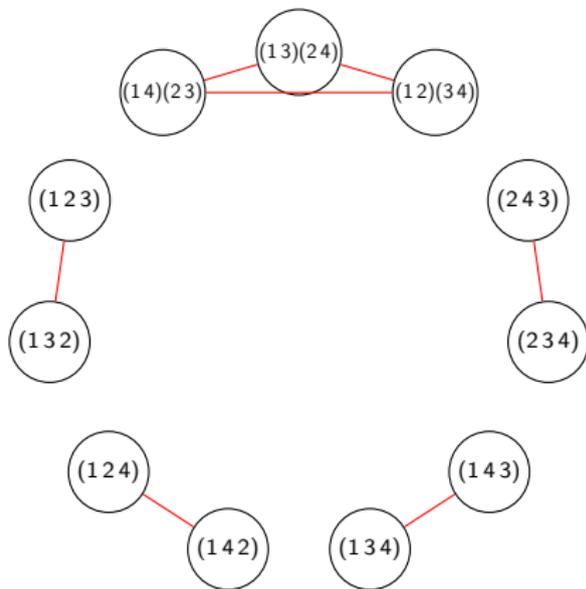
The **generating graph** of a group G is the graph $\Gamma(G)$ such that

- 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_4



Alternating group A_4

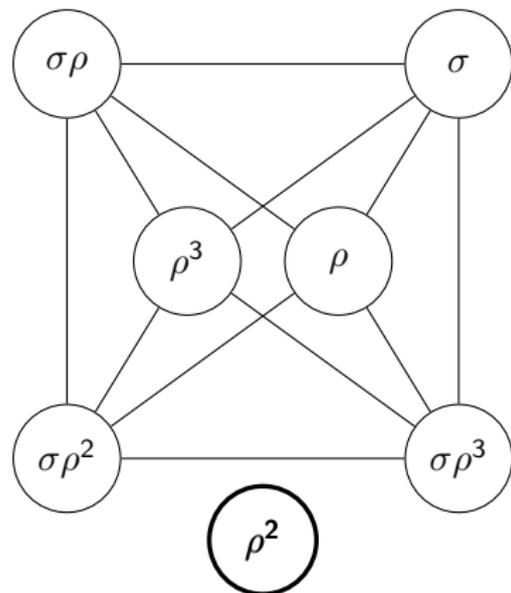


Generating Graphs

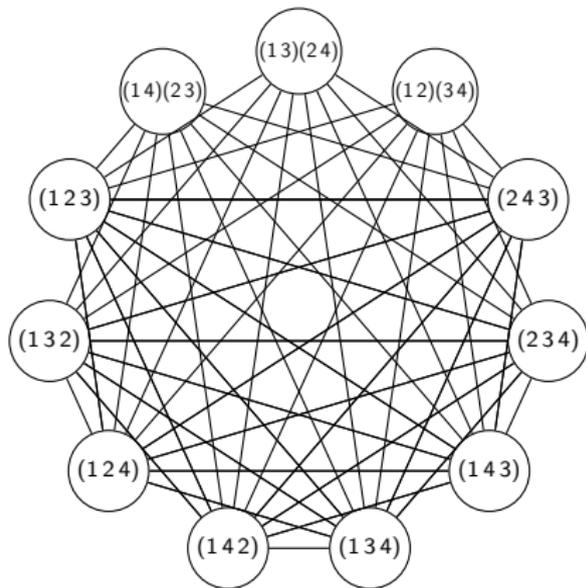
The **generating graph** of a group G is the graph $\Gamma(G)$ such that

- 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_4



Alternating group A_4

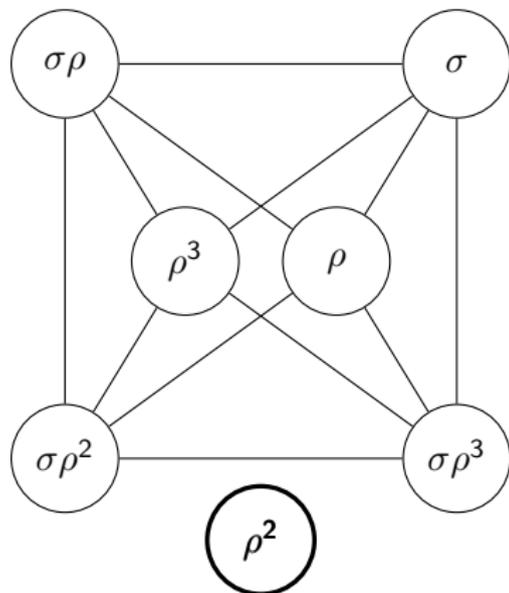


Generating Graphs

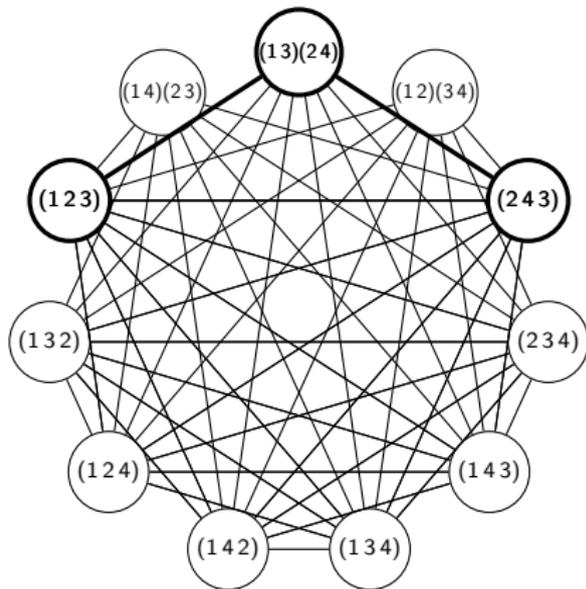
The **generating graph** of a group G is the graph $\Gamma(G)$ such that

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

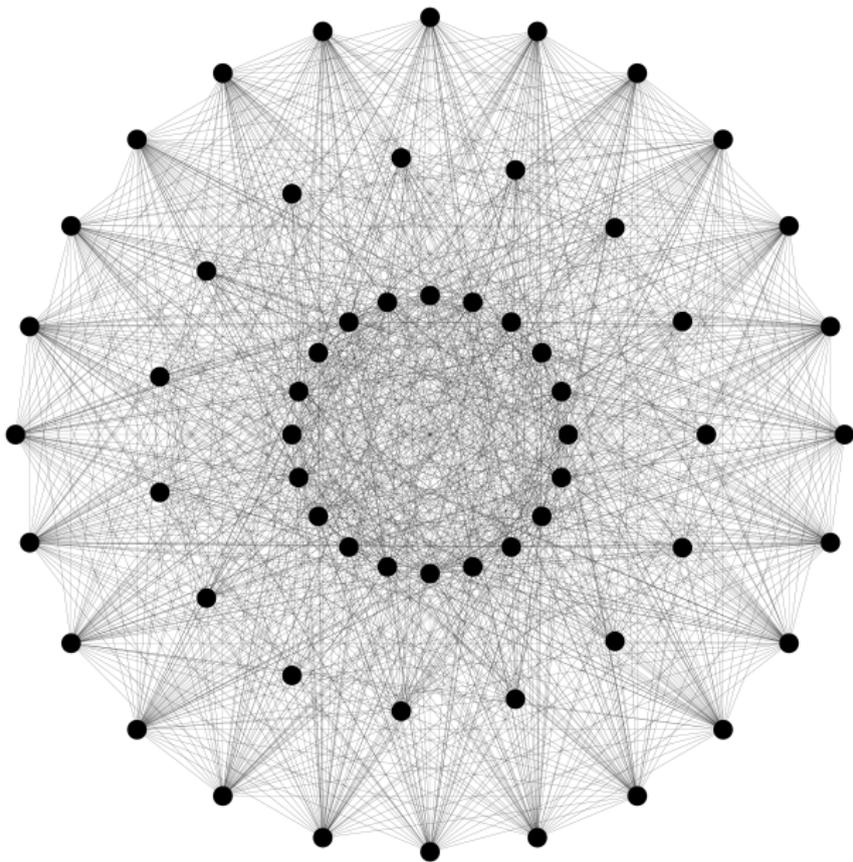
Dihedral group D_{\square}



Alternating group A_4



Alternating group A_5



Spread

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

Spread

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

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

Spread

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

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

Dihedral group D_n

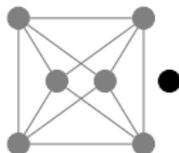
Alternating groups A_4 and A_5

Spread

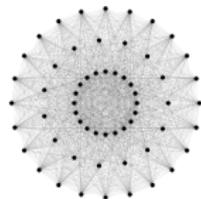
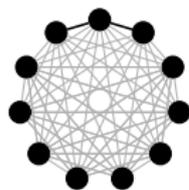
A group G has **spread** k if for any elements $x_1, \dots, x_k \in G \setminus 1$ there exists an element $z \in G$ such that $\langle x_1, z \rangle = \dots = \langle x_k, z \rangle = G$.

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

Dihedral group D_4



Alternating groups A_4 and A_5

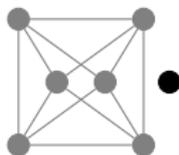


Spread

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

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

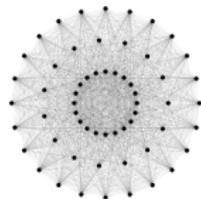
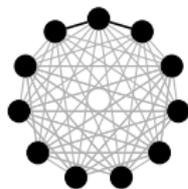
Dihedral group D_{\square}



$$s(D_{\square}) = 0$$

$\Gamma(D_{\square})$ has an isolated vertex

Alternating groups A_4 and A_5

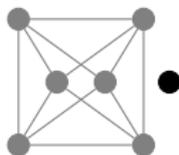


Spread

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

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

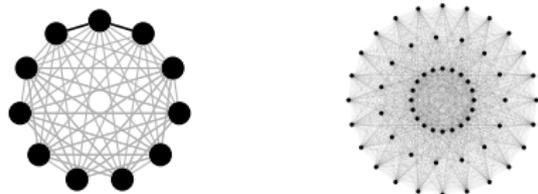
Dihedral group D_{\square}



$$s(D_{\square}) = 0$$

$\Gamma(D_{\square})$ has an isolated vertex

Alternating groups A_4 and A_5



$$s(A_4), s(A_5) \geq 2$$

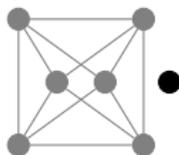
$\Gamma(A_4)$ and $\Gamma(A_5)$ have diameter 2

Spread

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

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

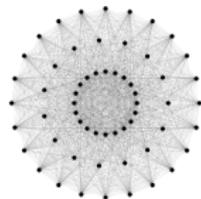
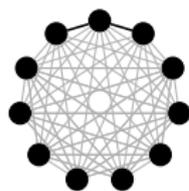
Dihedral group D_{\square}



$$s(D_{\square}) = 0$$

$\Gamma(D_{\square})$ has an isolated vertex

Alternating groups A_4 and A_5



$$s(A_4), s(A_5) \geq 2$$

$\Gamma(A_4)$ and $\Gamma(A_5)$ have diameter 2

Theorem (Breuer, Guralnick & Kantor, 2008)

Every finite simple group G has (at least) 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 ,

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

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

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

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

Which 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 ,

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.

A group G is **almost simple** if $T \leq G \leq \text{Aut}(T)$ 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 ,

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.

A group G is **almost simple** if $T \leq G \leq \text{Aut}(T)$ for a simple group T .

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

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 $g \in \text{Aut}(T)$.

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 $g \in \text{Aut}(T)$.

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 $g \in \text{Aut}(T)$.

Alternating groups Brenner & Wiegold, 1975 & 1980

Sporadic groups Breuer, Guralnick & Kantor, 2008

Groups of Lie type

$\text{PSL}_n(q)$: Burness & Guest, 2013

The rest: **To be done!**

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 $g \in \text{Aut}(T)$.

Alternating groups Brenner & Wiegold, 1975 & 1980

Sporadic groups Breuer, Guralnick & Kantor, 2008

Groups of Lie type

$\text{PSL}_n(q)$: Burness & Guest, 2013

The rest: **To be done!**

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

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 spread k .

Probabilistic Method

Let $s \in G$. Write

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

Lemma 1

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

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

Probabilistic Method

Let $s \in G$. Write

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

Lemma 1

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

$\langle x, s^g \rangle \neq G \implies x$ 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 spread k .

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

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

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

Probabilistic Method

Let $s \in G$. Write

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

Lemma 1

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

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

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

Lemma 2

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

“Things done without example, in their issue, are to be fear’d”

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

- 1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

- 1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

Maximal subgroups of A_5

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

- 1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

Maximal subgroups of A_5

- 10 isomorphic to S_3

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

Maximal subgroups of A_5

- 10 isomorphic to S_3
- 5 isomorphic to A_4

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

Maximal subgroups of A_5

- 10 isomorphic to S_3
- 5 isomorphic to A_4
- 6 isomorphic to D_{\square}

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

Maximal subgroups of A_5

- 10 isomorphic to S_3
- 5 isomorphic to A_4
- 6 isomorphic to D_{\square}

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

“Things done without example, in their issue, are to be fear’d”

Proposition

The alternating group A_5 has spread two.

Proof

1 Choose $s \in A_5$ and determine $\mathcal{M}(G, s)$

Maximal subgroups of A_5

- 10 isomorphic to S_3
- 5 isomorphic to A_4
- 6 isomorphic to D_{\square}

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

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

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

In this case

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

In this case

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

x has order 2

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

In this case

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

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

In this case

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

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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 $|x^G \cap H| = 0$

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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 $|x^G| = 12$

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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 $|x^G \cap H| = 2$

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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

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

Conjugacy classes of $G = A_5$:

$$\text{id}^G, (123)^G, (12)(34)^G, (12345)^G, (13524)^G$$

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 $s(A_5) \geq 2$. ■

Groups of Lie Type

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Classical groups of Lie type

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Classical groups of Lie type

Linear $\mathrm{PSL}_n(q)$

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Classical groups of Lie type

Linear $\mathrm{PSL}_n(q)$

Symplectic $\mathrm{PSp}_{2m}(q)$

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Classical groups of Lie type

Linear $\mathrm{PSL}_n(q)$

Symplectic $\mathrm{PSp}_{2m}(q)$

Orthogonal $\mathrm{P}\Omega_{2m+1}(q)$ for odd q

$\mathrm{P}\Omega_{2m}^+(q), \mathrm{P}\Omega_{2m}^-(q)$

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Classical groups of Lie type

Linear $\mathrm{PSL}_n(q)$

Symplectic $\mathrm{PSp}_{2m}(q)$

Orthogonal $\mathrm{P}\Omega_{2m+1}(q)$ for odd q

$\mathrm{P}\Omega_{2m}^+(q), \mathrm{P}\Omega_{2m}^-(q)$

Unitary $\mathrm{PSU}_n(q)$

Groups of Lie Type

There is a dichotomy: **classical** and **exceptional**.

Classical groups of Lie type

Linear $\mathrm{PSL}_n(q)$

Symplectic $\mathrm{PSp}_{2m}(q)$

Orthogonal $\mathrm{P}\Omega_{2m+1}(q)$ for odd q

$\mathrm{P}\Omega_{2m}^+(q), \mathrm{P}\Omega_{2m}^-(q)$

Unitary $\mathrm{PSU}_n(q)$

Exceptional groups of Lie type

Chevalley $E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$

Steinberg ${}^3D_4(q), {}^2E_6(q)$

Suzuki and Ree ${}^2B_2(q), {}^2F_4(q), {}^2G_2(q)$

What is the simple group T ?

What is the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

What is the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

Summary You take a natural subgroup of $GL_n(q)$ and then you quotient by scalar matrices to make sure it is simple.

What is the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

Summary You take a natural subgroup of $GL_n(q)$ and then you quotient by scalar matrices to make sure it is simple.

Symplectic Groups

What is the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

Summary You take a natural subgroup of $GL_n(q)$ and then you quotient by scalar matrices to make sure it is simple.

Symplectic Groups

Let $n = 2m$ and let f be a non-degenerate alternating bilinear form on V .

What is the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

Summary You take a natural subgroup of $GL_n(q)$ and then you quotient by scalar matrices to make sure it is simple.

Symplectic Groups

Let $n = 2m$ and 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 the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

Summary You take a natural subgroup of $GL_n(q)$ and then you quotient by scalar matrices to make sure it is simple.

Symplectic Groups

Let $n = 2m$ and let f be a non-degenerate alternating bilinear form on V .

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

Then $PSp_n(q) = Sp_n(q)/Z(Sp_n(q))$ where $Z(Sp_n(q)) = \{I, -I\}$.

What is the simple group T ?

Let $q = p^k$ be a prime power and let $n \in \mathbb{N}$. Write $V = \mathbb{F}_q^n$.

Summary You take a natural subgroup of $GL_n(q)$ and then you quotient by scalar matrices to make sure it is simple.

Symplectic Groups

Let $n = 2m$ and let f be a non-degenerate alternating bilinear form on V .

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

Then $PSp_n(q) = Sp_n(q)/Z(Sp_n(q))$ where $Z(Sp_n(q)) = \{I, -I\}$.

Odd-Dimensional Orthogonal Groups

Let $n = 2m + 1$ and let f be a non-deg. symmetric bilinear form on V .

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

Then $P\Omega_n(q) = \Omega_n(q)$.

What are the automorphisms of T ?

What are the automorphisms of T ?

Field automorphisms

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

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Fact

- If $T = \text{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\text{Aut}(T) = \langle T, \sigma \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms

If q is even and $T = \text{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Fact

- If $T = \text{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\text{Aut}(T) = \langle T, \sigma \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms

If q is even and $T = \text{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Fact

- If $T = \text{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\text{Aut}(T) = \langle T, \sigma \rangle$.
- If $T = \text{PSp}_4(q)$ where q is even then $\text{Aut}(T) = \langle T, \rho \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms ... These are weird.

If q is even and $T = \text{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Fact

- If $T = \text{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\text{Aut}(T) = \langle T, \sigma \rangle$.
- If $T = \text{PSp}_4(q)$ where q is even then $\text{Aut}(T) = \langle T, \rho \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms ... These are weird.

If q is even and $T = \text{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Diagonal automorphisms

Fact

- If $T = \text{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\text{Aut}(T) = \langle T, \sigma \rangle$.
- If $T = \text{PSp}_4(q)$ where q is even then $\text{Aut}(T) = \langle T, \rho \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms ... These are weird.

If q is even and $T = \mathrm{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Diagonal automorphisms

If q is odd, let $\delta \in \mathrm{PGL}_n(q) \setminus T$ be a diagonal matrix normalising T .

Fact

- If $T = \mathrm{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\mathrm{Aut}(T) = \langle T, \sigma \rangle$.
- If $T = \mathrm{PSp}_4(q)$ where q is even then $\mathrm{Aut}(T) = \langle T, \rho \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms ... These are weird.

If q is even and $T = \mathrm{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Diagonal automorphisms

If q is odd, let $\delta \in \mathrm{PGL}_n(q) \setminus T$ be a diagonal matrix normalising T .

Fact

- If $T = \mathrm{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\mathrm{Aut}(T) = \langle T, \sigma \rangle$.
- If $T = \mathrm{PSp}_4(q)$ where q is even then $\mathrm{Aut}(T) = \langle T, \rho \rangle$.
- If $T = \mathrm{PSp}_{2m}(q)$ where q is odd then $\mathrm{Aut}(T) = \langle T, \delta, \sigma \rangle$.
- If $T = \Omega_{2m+1}(q)$ then $\mathrm{Aut}(T) = \langle T, \delta, \sigma \rangle$.

What are the automorphisms of T ?

Field automorphisms ... These are typical.

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

Graph-field automorphisms ... These are weird.

If q is even and $T = \mathrm{PSp}_4(q)$, let ρ such that $\rho^2 = \sigma$.

Diagonal automorphisms ... These are innocuous.

If q is odd, let $\delta \in \mathrm{PGL}_n(q) \setminus T$ be a diagonal matrix normalising T .

Fact

- If $T = \mathrm{PSp}_{2m}(q)$ where q is even and $2m \geq 6$ then $\mathrm{Aut}(T) = \langle T, \sigma \rangle$.
- If $T = \mathrm{PSp}_4(q)$ where q is even then $\mathrm{Aut}(T) = \langle T, \rho \rangle$.
- If $T = \mathrm{PSp}_{2m}(q)$ where q is odd then $\mathrm{Aut}(T) = \langle T, \delta, \sigma \rangle$.
- If $T = \Omega_{2m+1}(q)$ then $\mathrm{Aut}(T) = \langle T, \delta, \sigma \rangle$.

Results on Spread

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Roughly, if G_1, G_2, G_3, \dots is a sequence of finite simple groups such that $|G_i| \rightarrow \infty$ then $s(G_i) \rightarrow \infty$

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Roughly, if G_1, G_2, G_3, \dots is a sequence of finite simple groups such that $|G_i| \rightarrow \infty$ then $s(G_i) \rightarrow \infty$ unless (G_i) has one of three types of “bad subsequence”

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Roughly, if G_1, G_2, G_3, \dots is a sequence of finite simple groups such that $|G_i| \rightarrow \infty$ then $s(G_i) \rightarrow \infty$ unless (G_i) has one of three types of “bad subsequence” (Guralnick & Shalev, 2003).

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Roughly, if G_1, G_2, G_3, \dots is a sequence of finite simple groups such that $|G_i| \rightarrow \infty$ then $s(G_i) \rightarrow \infty$ unless (G_i) has one of three types of “bad subsequence” (Guralnick & Shalev, 2003).

Theorem (H, 2017)

Let $G_n = \langle T_n, g_n \rangle$ for $T_n \in \mathcal{T}$ and $g_n \in \mathrm{Aut}(T_n)$. Assume that $|G_n| \rightarrow \infty$.

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Roughly, if G_1, G_2, G_3, \dots is a sequence of finite simple groups such that $|G_i| \rightarrow \infty$ then $s(G_i) \rightarrow \infty$ unless (G_i) has one of three types of “bad subsequence” (Guralnick & Shalev, 2003).

Theorem (H, 2017)

Let $G_n = \langle T_n, g_n \rangle$ for $T_n \in \mathcal{T}$ and $g_n \in \mathrm{Aut}(T_n)$. Assume that $|G_n| \rightarrow \infty$.
Then $s(G_n) \rightarrow \infty$

Results on Spread

Write $\mathcal{T} = \{\mathrm{PSp}_{2m}(q) \mid m \geq 2, q \neq 2\} \cup \{\Omega_{2m+1}(q) \mid m \geq 3\}$.

Theorem (H, 2017)

Let $G = \langle T, g \rangle$ where $T \in \mathcal{T}$ and $g \in \mathrm{Aut}(T)$. Then $s(G) \geq 2$.

Roughly, if G_1, G_2, G_3, \dots is a sequence of finite simple groups such that $|G_i| \rightarrow \infty$ then $s(G_i) \rightarrow \infty$ unless (G_i) has one of three types of “bad subsequence” (Guralnick & Shalev, 2003).

Theorem (H, 2017)

Let $G_n = \langle T_n, g_n \rangle$ for $T_n \in \mathcal{T}$ and $g_n \in \mathrm{Aut}(T_n)$. Assume that $|G_n| \rightarrow \infty$. Then $s(G_n) \rightarrow \infty$ if and only if there is no subsequence of (T_n) of groups over a field of fixed size which are either

- odd-dimensional orthogonal groups, or
- symplectic groups in even characteristic.

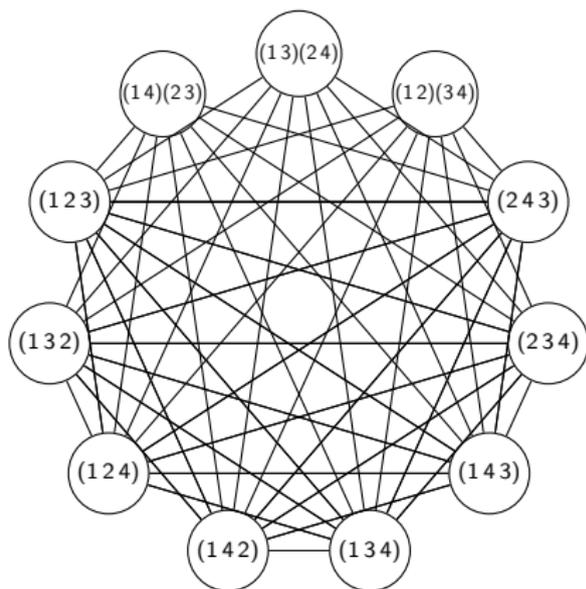
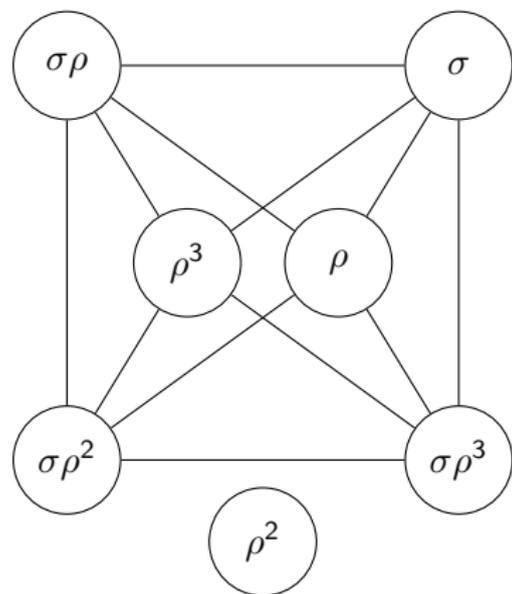
Further Questions

Further Questions

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

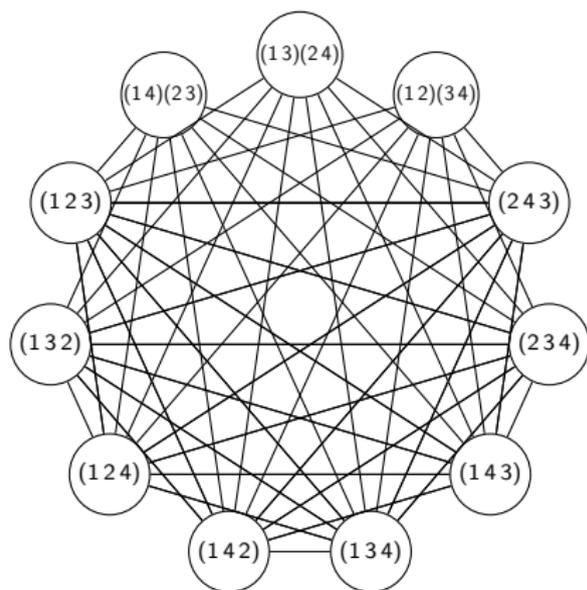
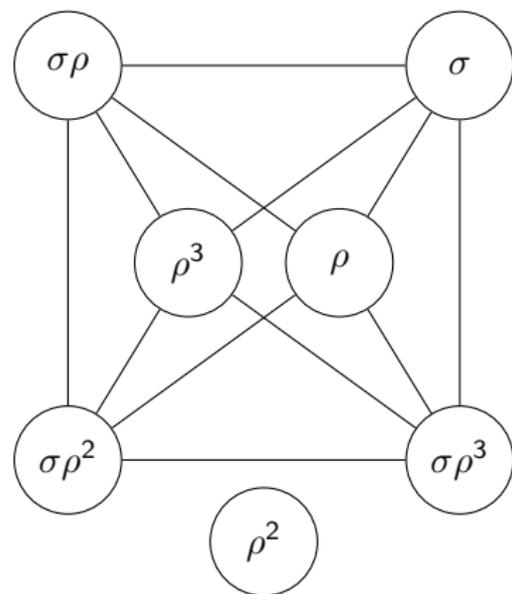
Further Questions

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



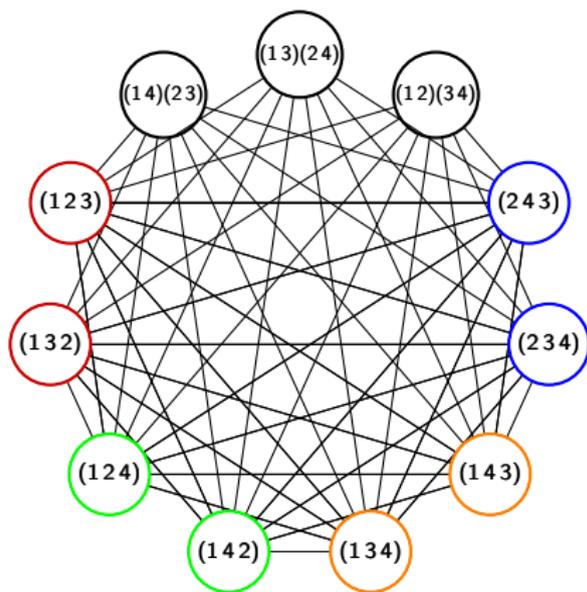
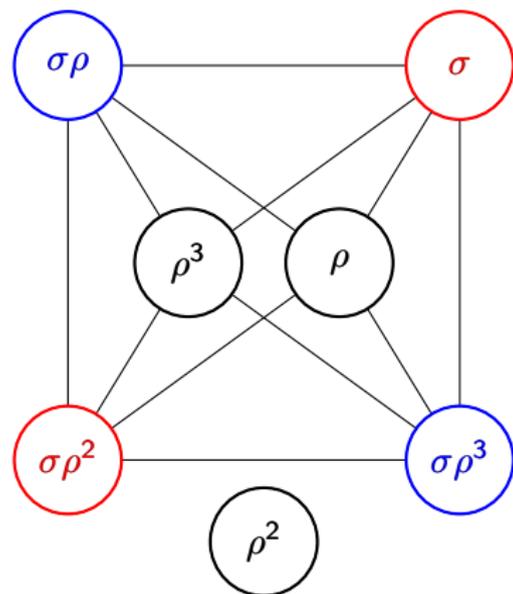
Further Questions

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



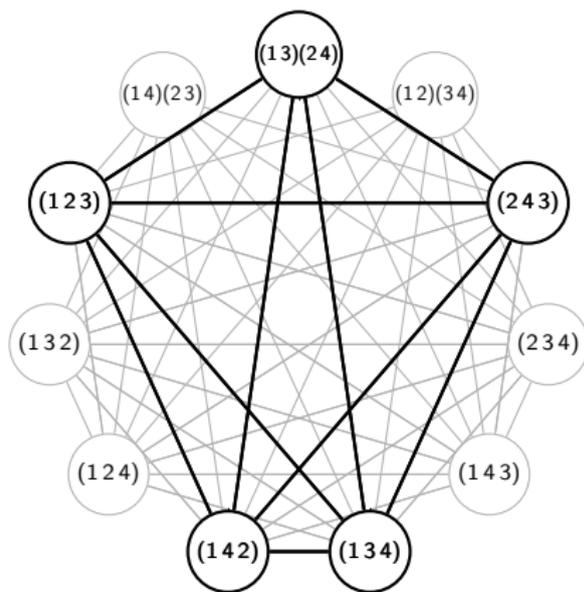
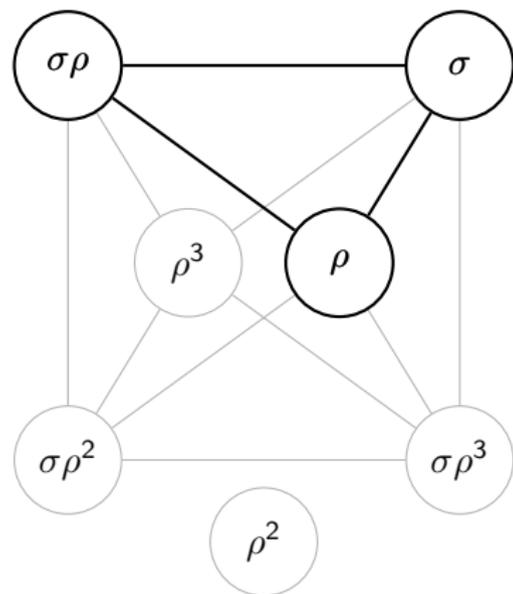
Further Questions

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



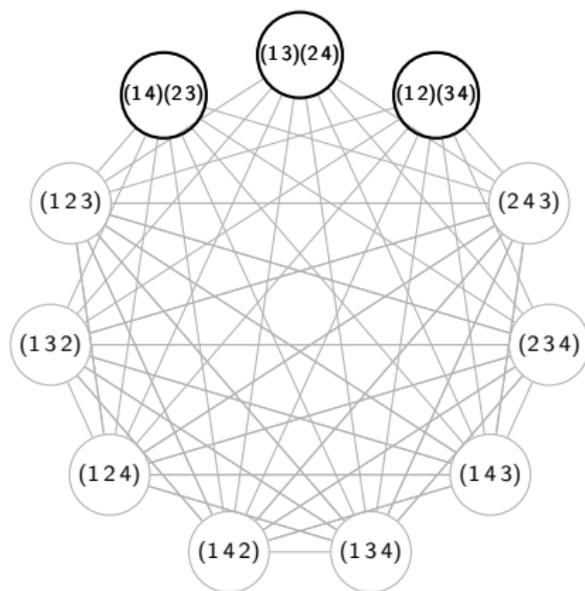
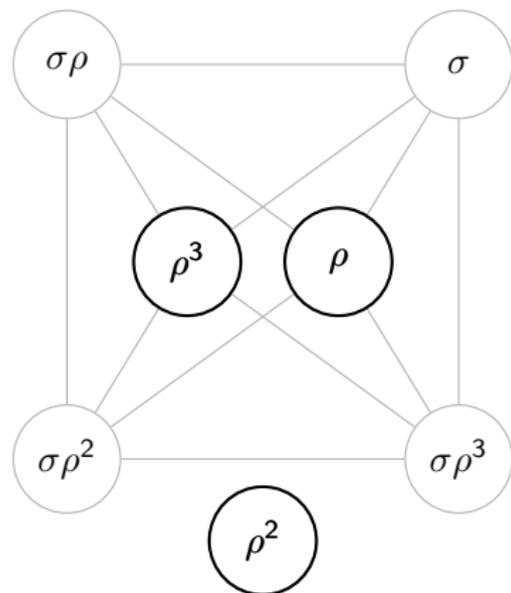
Further Questions

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



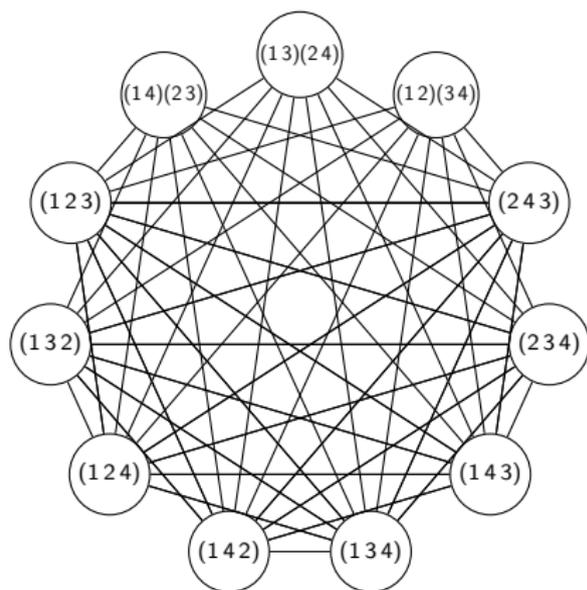
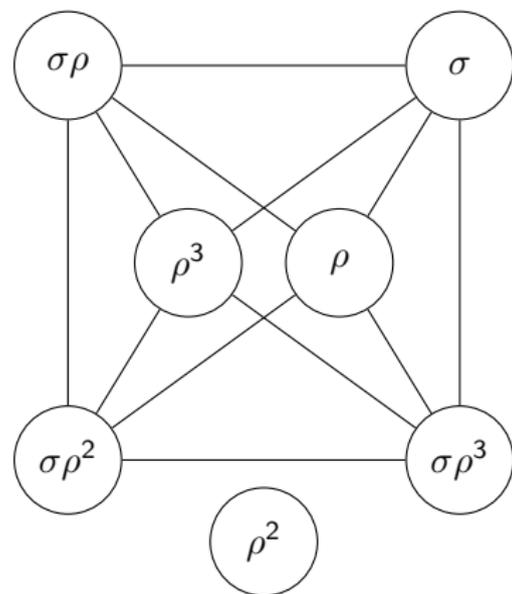
Further Questions

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



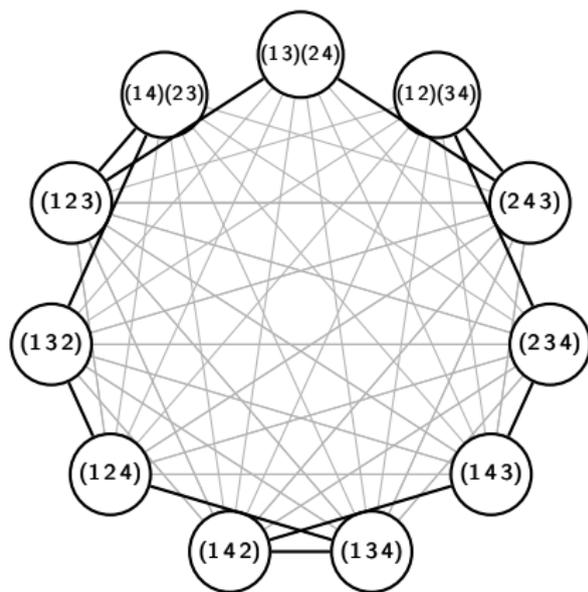
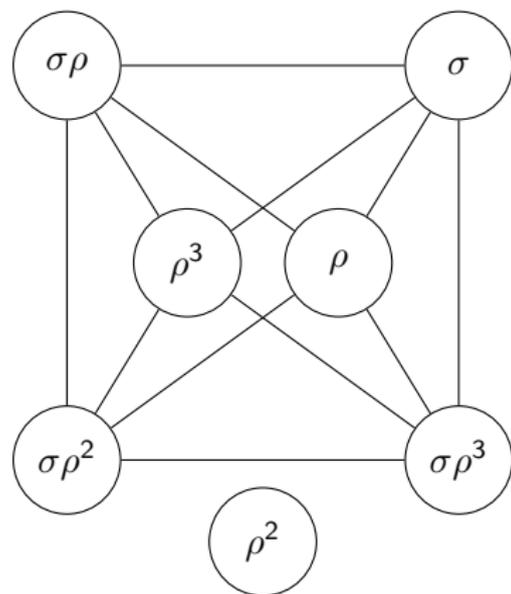
Further Questions

- 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?



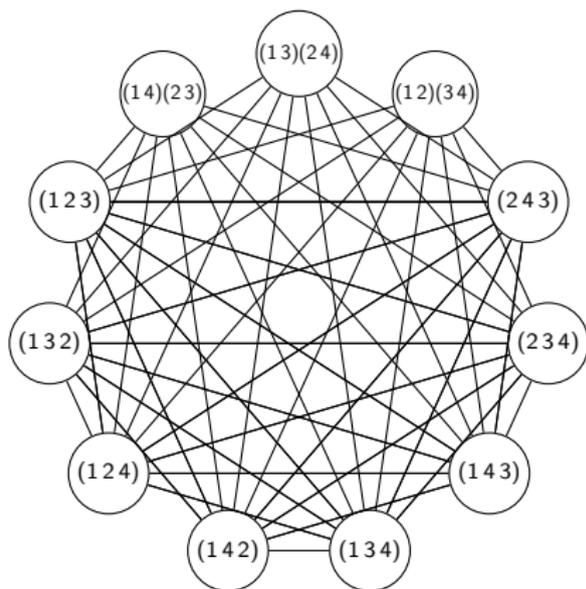
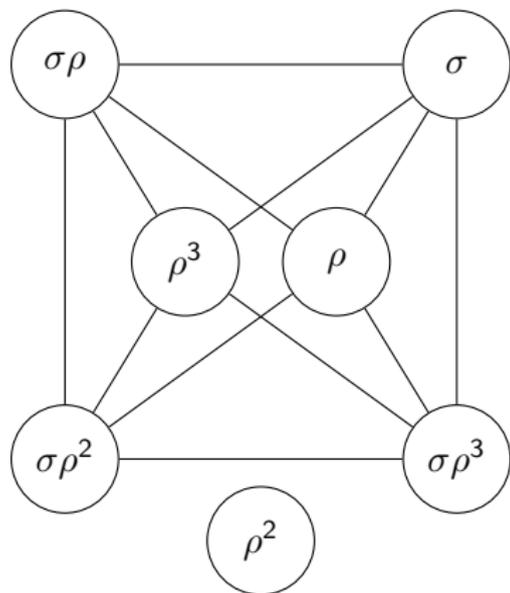
Further Questions

- 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?



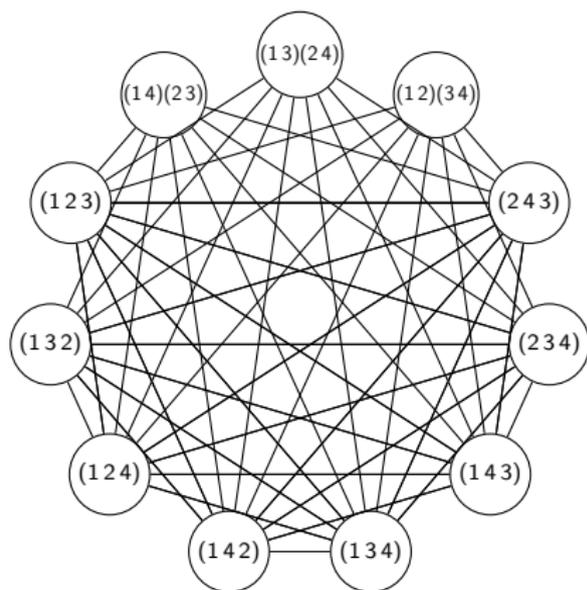
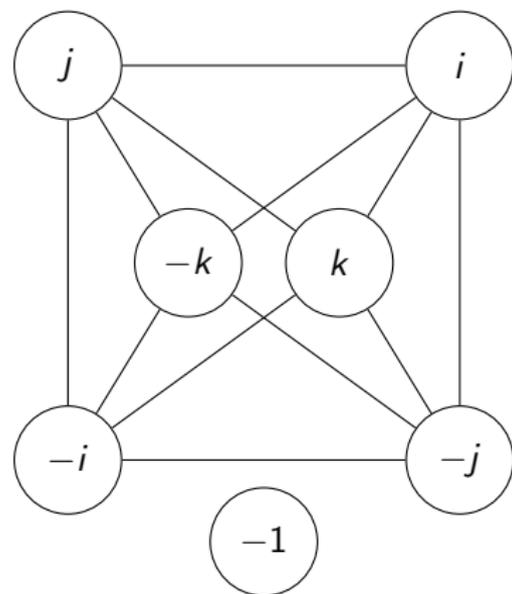
Further Questions

- 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 $G \not\cong H$ but $\Gamma(G) \cong \Gamma(H)$?



Further Questions

- 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 $G \not\cong H$ but $\Gamma(G) \cong \Gamma(H)$?



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

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

Conjecture

For a finite group G , the following are equivalent.

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

Conjecture

For a finite group G , the following are equivalent.

- Every proper quotient of G is cyclic.
- $s(G) \geq 1$ (i.e. G is $\frac{3}{2}$ -generated).

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

Conjecture

For a finite group G , the following are equivalent.

- Every proper quotient of G is cyclic.
- $s(G) \geq 1$ (i.e. G is $\frac{3}{2}$ -generated).
- $s(G) \geq 2$.

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

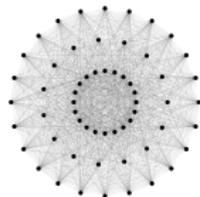
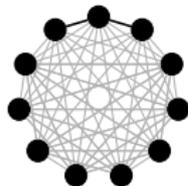
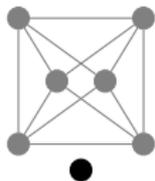
Conjecture

For a finite group G , the following are equivalent.

- Every proper quotient of G is cyclic.
- $s(G) \geq 1$ (i.e. G is $\frac{3}{2}$ -generated).
- $s(G) \geq 2$.

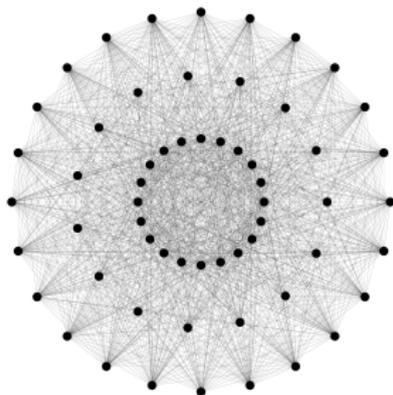
Combinatorial interpretation

Any generating graph either has an isolated vertex or is connected with diameter two.



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

Scott Harper



Pure Postgraduate Seminar

10th March 2017