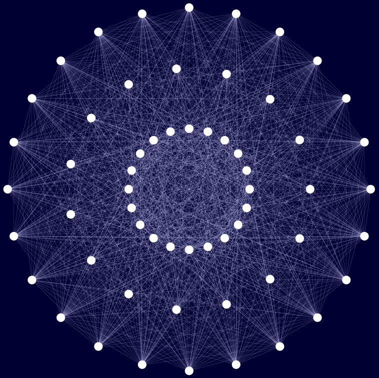
Generating Graphs of Finite Groups



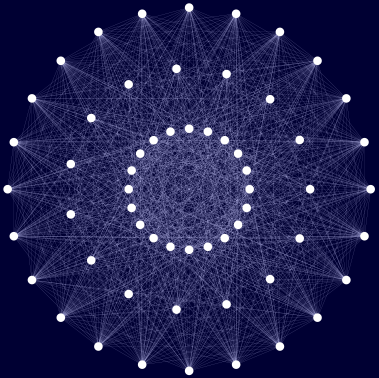
Scott Harper

(University of Bristol)

LMS Graduate Meeting

8th July 2016

Generating Graphs of Finite Groups



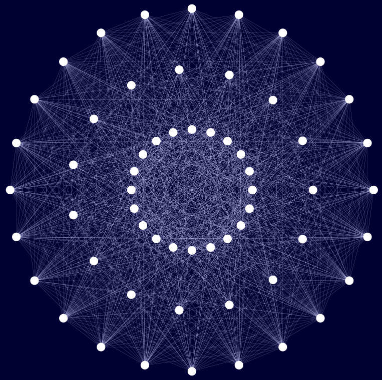
Scott Harper

(University of Bristol)

LMS Graduate Meeting

8th July 2016

Generating Graphs of Finite Groups



Scott Harper

(University of Bristol)

LMS Graduate Meeting

8th July 2016

Generating Finite Groups

Generating Finite Groups

Let G be a finite group.

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

Generating Finite Groups

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

Generating Finite Groups

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

Generating Finite Groups

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

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

Generating Finite Groups

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

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

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

Generating Finite Groups

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

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

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

Are other important families of finite groups 2-generated?

Finite Simple Groups

Finite Simple Groups

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

Finite Simple Groups

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

Theorem (The Classification of Finite Simple Groups)

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

Finite Simple Groups

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

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;*

Finite Simple Groups

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

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;*

Finite Simple Groups

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

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;*

Finite Simple Groups

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

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;*

Finite Simple Groups

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

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.*

Finite Simple Groups

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

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.

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)

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)

Probabilistic Generation

Write

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

Probabilistic Generation

Write

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

Theorem (Dixon, 1969)

$P(A_n) \to 1$ *as* $n \to \infty$.

Probabilistic Generation

Write

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

Theorem (Dixon, 1969)

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

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

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

Probabilistic Generation

Write

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

Theorem (Dixon, 1969)

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

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

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

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

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

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

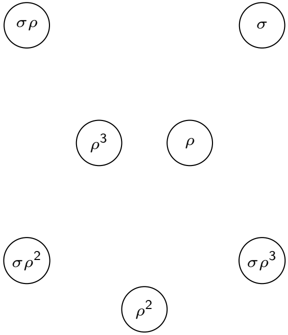
Dihedral group D_8

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

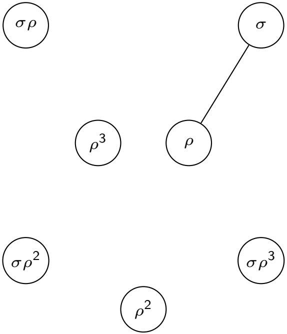
Dihedral group D_8



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

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

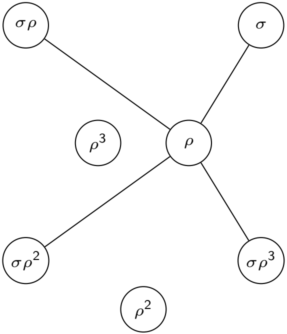
Dihedral group D_8



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

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

Dihedral group D_8

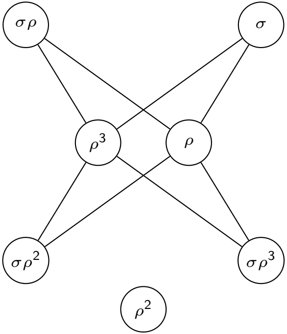


Generating Graphs

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

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

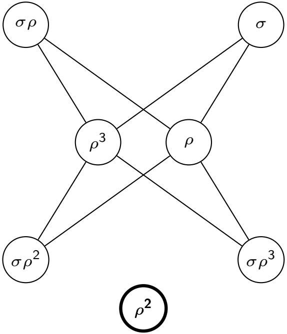
Dihedral group D_8



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

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

Dihedral group D_8

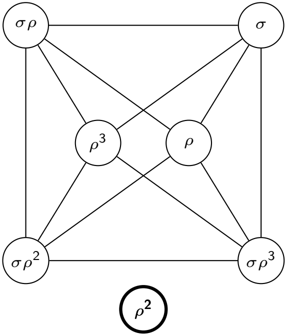


Generating Graphs

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

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

Dihedral group D_8

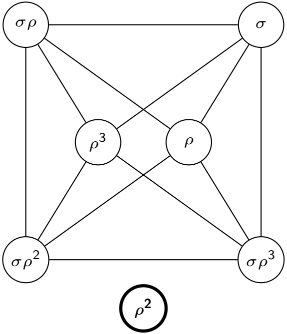


Generating Graphs

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

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

Dihedral group D_8



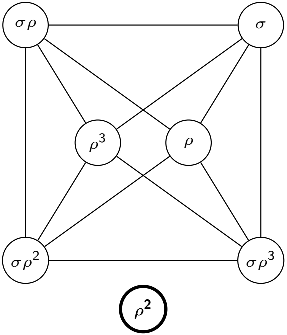
Alternating group A_4

Generating Graphs

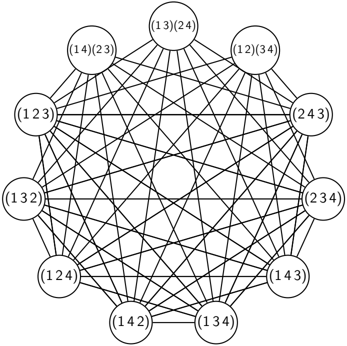
The generating graph of a group G is the graph $\Gamma(G)$ such that

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

Dihedral group D_8



Alternating group A_4

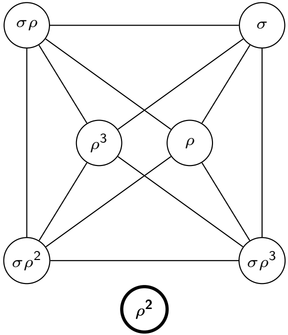


Generating Graphs

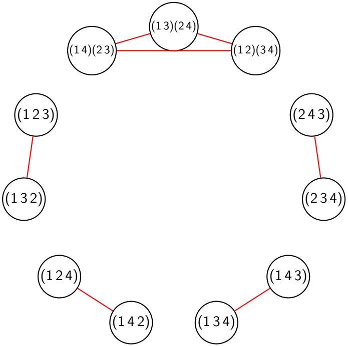
The generating graph of a group G is the graph $\Gamma(G)$ such that

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

Dihedral group D_8



Alternating group A_4

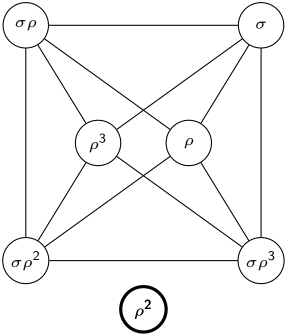


Generating Graphs

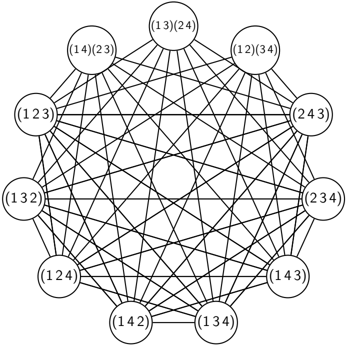
The generating graph of a group G is the graph $\Gamma(G)$ such that

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

Dihedral group D_8



Alternating group A_4

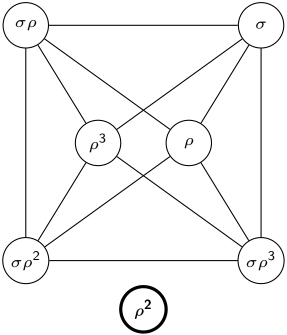


Generating Graphs

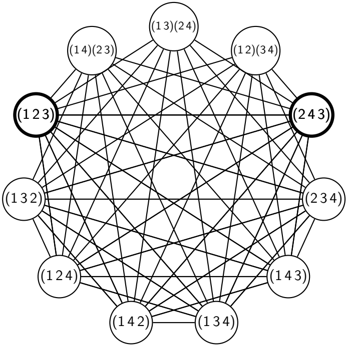
The generating graph of a group G is the graph $\Gamma(G)$ such that

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

Dihedral group D_8



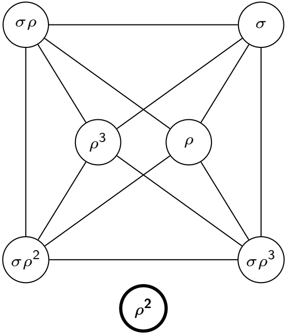
Alternating group A_4



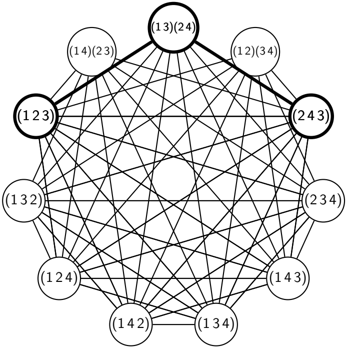
The generating graph of a group G is the graph $\Gamma(G)$ such that

- 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



Isolated Vertices

For which finite groups G does $\Gamma(G)$ have

- no isolated vertices?
- diameter two?

Isolated Vertices

For which finite groups G does $\Gamma(G)$ have

- no isolated vertices?
- diameter two?

Theorem

If G is simple then $\Gamma(G)$ has

Isolated Vertices

For which finite groups G does $\Gamma(G)$ have

- no isolated vertices?
- diameter two?

Theorem

If G is simple then $\Gamma(G)$ has

- *no isolated vertices;*
  [Stein 1998; Guralnick & Kantor 2000]

Isolated Vertices

For which finite groups G does $\Gamma(G)$ have

- no isolated vertices?
- diameter two?

Theorem

If G is simple then $\Gamma(G)$ has

- *no isolated vertices;*
  [Stein 1998; Guralnick & Kantor 2000]
- *diameter two.*
  [Breuer, Guralnick & Kantor, 2008]

Isolated Vertices

For which finite groups G does $\Gamma(G)$ have

- no isolated vertices?
- diameter two?

Theorem

If G is simple then $\Gamma(G)$ has

- *no isolated vertices;*
  [Stein 1998; Guralnick & Kantor 2000]
- *diameter two.*
  [Breuer, Guralnick & Kantor, 2008]

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

Isolated Vertices

For which finite groups G does $\Gamma(G)$ have

- no isolated vertices?
- diameter two?

Theorem

If G is simple then $\Gamma(G)$ has

- *no isolated vertices;*
  [Stein 1998; Guralnick & Kantor 2000]
- *diameter two.*
  [Breuer, Guralnick & Kantor, 2008]

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

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

Isolated Vertices

Proposition

If $\Gamma(G)$ *has no isolated vertices then every proper quotient of* G *is cyclic.*

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

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

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since $\Gamma(G)$ has no isolated vertices, there exists $x \in G$ such that $\langle x, n \rangle = G$.

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since $\Gamma(G)$ has no isolated vertices, there exists $x \in G$ such that $\langle x, n \rangle = G$.

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

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since $\Gamma(G)$ has no isolated vertices, 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, $G/N = \langle xN \rangle$.

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since $\Gamma(G)$ has no isolated vertices, 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. ∎

Isolated Vertices

Proposition

If $\Gamma(G)$ has no isolated vertices then every proper quotient of G is cyclic.

Proof

Let $1 \neq N \trianglelefteq G$ and fix $1 \neq n \in N$. Since $\Gamma(G)$ has no isolated vertices, 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

The following are equivalent

- Every proper quotient of G is cyclic.
- $\Gamma(G)$ has no isolated vertices.
- $\Gamma(G)$ has diameter two.

Current Research

Aim: Show $\Gamma(\langle T, g \rangle)$ has diameter two for T simple and $g \in \mathrm{Aut}(T)$.

Current Research

Aim: Show $\Gamma(\langle T, g \rangle)$ has diameter two for T simple and $g \in \mathrm{Aut}(T)$.

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

Current Research

Aim: Show $\Gamma(\langle T, g \rangle)$ has diameter two for T simple and $g \in \mathrm{Aut}(T)$.

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

Current Research

Aim: Show $\Gamma(\langle T, g \rangle)$ has diameter two for T simple and $g \in \mathrm{Aut}(T)$.

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

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

Current Research

Aim: Show $\Gamma(\langle T, g\rangle)$ has diameter two for T simple and $g \in \mathrm{Aut}(T)$.

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

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

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 $n \neq 4$ and write $G = \langle T, g\rangle$ where $T = PSp_n(q)$ and $g \in \mathrm{Aut}(T)$. Then $\Gamma(G)$ has diameter two.

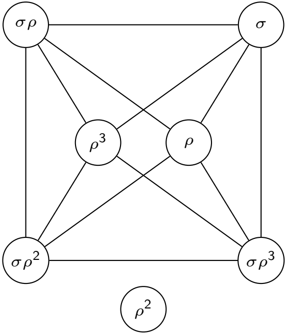
Further Questions

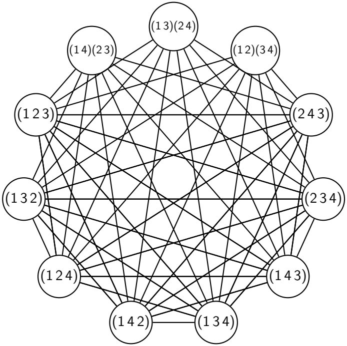
Further Questions

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

Further Questions

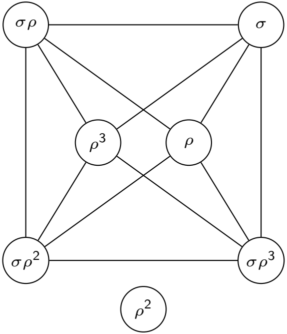
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?

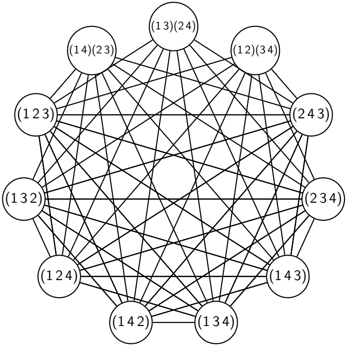




Further Questions

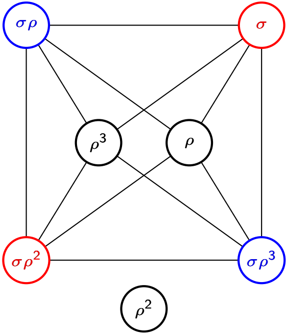
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?

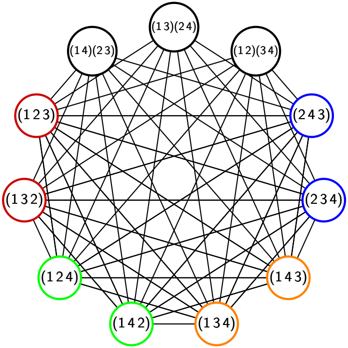




Further Questions

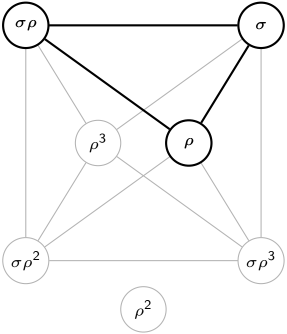
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?

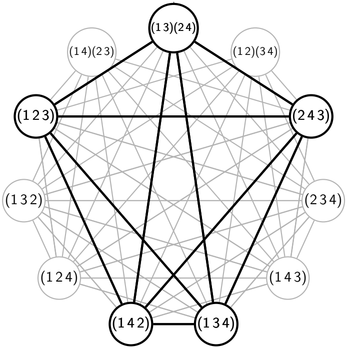




Further Questions

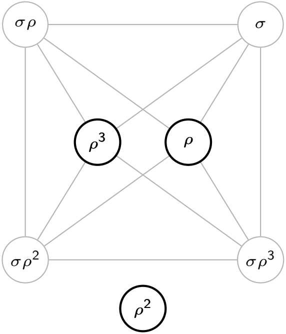
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?

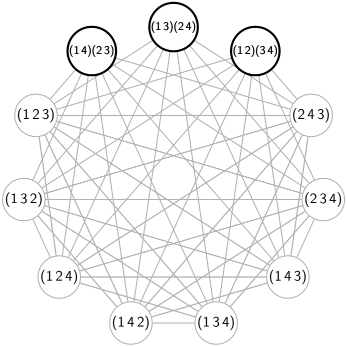




Further Questions

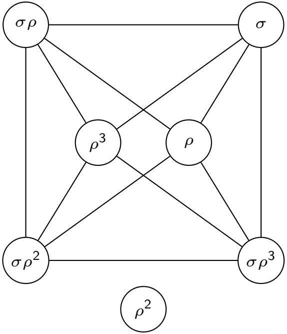
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number . . . ?

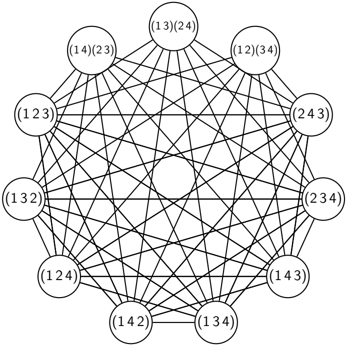




Further Questions

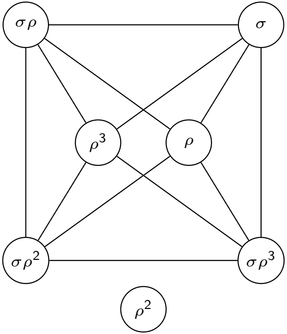
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?
- When does $\Gamma(G)$ have a Hamiltonian cycle?

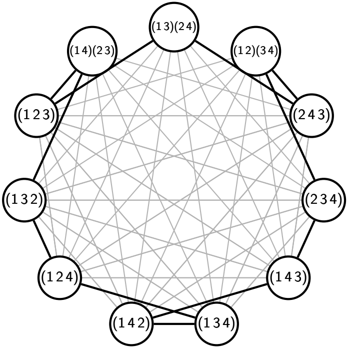




Further Questions

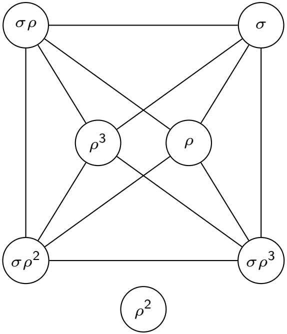
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number . . . ?
- When does $\Gamma(G)$ have a Hamiltonian cycle?

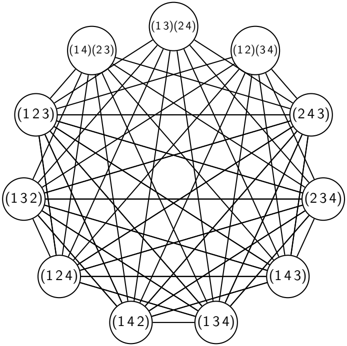




Further Questions

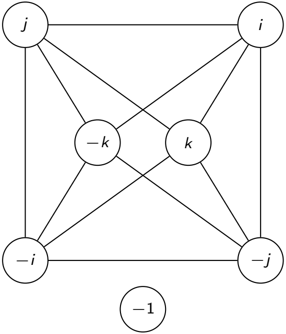
- If the isolated vertices of $\Gamma(G)$ are removed then is $\Gamma(G)$ connected?
- Chromatic number, clique number, coclique number ...?
- When does $\Gamma(G)$ have a Hamiltonian cycle?
- When is $G \ncong H$ but $\Gamma(G) \cong \Gamma(H)$?

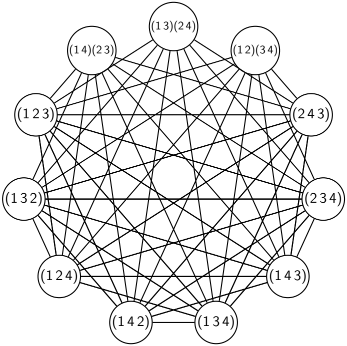




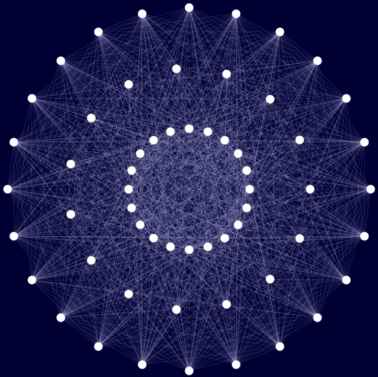
Further Questions

- 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 $G \ncong H$ but $\Gamma(G) \cong \Gamma(H)$?





Generating Graphs of Finite Groups



Scott Harper

(University of Bristol)

LMS Graduate Meeting

8th July 2016