Graphs encoding the generating properties of a finite group

Andrea Lucchini

Università di Padova, Italy

Advances in Group Theory and Applications 2017
September 5-8, 2017 - Lecce

Co-authors

- Cristina Acciarri
- Thomas Breuer
- Peter Cameron
- Eleonora Crestani
- Marco Di Summa
- Robert Guralnick
- Claude Marion
- Attila Maróti
- Colva Roney-Dougal
- Gábor Péter Nagy

The generating graph

The generating graph $\Gamma(G)$ of a finite group G is the graph with vertex set G, in which two vertices x and y are joined if and only if $\langle x, y \rangle = G$.

The generating graph

The generating graph $\Gamma(G)$ of a finite group G is the graph with vertex set G, in which two vertices x and y are joined if and only if $\langle x, y\rangle = G$.

Many deep results about finite simple groups G can equivalently be stated as theorems about $\Gamma(G)$.

- 1 is the unique isolated vertex in $\Gamma(G)$ (Guralnick and Kantor).
- $\Gamma(G) \setminus \{1\}$ is connected, with diameter equal to 2 (Breuer, Guralnick and Kantor).

For an arbitrary finite group G, there could be many isolated vertices in $\Gamma(G)$. All the elements in the Frattini subgroup will be isolated vertices, but we can also find isolated vertices outside the Frattini subgroup, for example the nontrivial elements of the Klein subgroup are isolated vertices in $\Gamma(\mathrm{Sym}(4))$.

For an arbitrary finite group G, there could be many isolated vertices in $\Gamma(G)$. All the elements in the Frattini subgroup will be isolated vertices, but we can also find isolated vertices outside the Frattini subgroup, for example the nontrivial elements of the Klein subgroup are isolated vertices in $\Gamma(\mathrm{Sym}(4))$.

Let $\Gamma^*(G)$ be the subgraph of $\Gamma(G)$ that is induced by all the vertices that are not isolated.

For an arbitrary finite group G, there could be many isolated vertices in $\Gamma(G)$. All the elements in the Frattini subgroup will be isolated vertices, but we can also find isolated vertices outside the Frattini subgroup, for example the nontrivial elements of the Klein subgroup are isolated vertices in $\Gamma(\mathrm{Sym}(4))$.

Let $\Gamma^*(G)$ be the subgraph of $\Gamma(G)$ that is induced by all the vertices that are not isolated.

Theorem (E. Crestani and AL 2013 - AL 2017)

Let G be a 2-generated finite soluble group.

- $\Gamma^*(G)$ *is connected;*
- $\mathrm{diam}(\Gamma^*(G)) \leq 3$.

For an arbitrary finite group G, there could be many isolated vertices in $\Gamma(G)$. All the elements in the Frattini subgroup will be isolated vertices, but we can also find isolated vertices outside the Frattini subgroup, for example the nontrivial elements of the Klein subgroup are isolated vertices in $\Gamma(\mathrm{Sym}(4))$.

Let $\Gamma^*(G)$ be the subgraph of $\Gamma(G)$ that is induced by all the vertices that are not isolated.

THEOREM (E. CRESTANI AND AL 2013 - AL 2017)

Let G be a 2-generated finite soluble group.

- $\Gamma^*(G)$ *is connected;*
- $\mathrm{diam}(\Gamma^*(G)) \leq 3$.

The situation is different if the solubility assumption is dropped. It is an open problem whether or not $\Gamma^*(G)$ is connected, but even when $\Gamma^*(G)$ is connected, its diameter can be arbitrarily large: if G is the largest 2-generated direct power of $SL(2, 2^p)$ and p is a sufficiently large odd prime, then $\Gamma^*(G)$ is connected but $\mathrm{diam}(\Gamma^*(G)) \geq 2^{p-2}$.

For soluble groups, the bound $\mathrm{diam}(\Gamma^*(G)) \leq 3$ is best possible.

Let $H = \mathrm{GL}(2,2) \times \mathrm{GL}(2,2)$ and let $W = V_1 \times V_2 \times V_3 \times V_4$ be the direct product of four 2-dimensional vector spaces over the field $\mathbb{F}_2$. Define an action of H on W by setting

$$(v_1, v_2, v_3, v_4)^{(x,y)} = (v_1^x, v_2^x, v_3^y, v_4^y)$$

and consider the semidirect product $G = W \rtimes H$: $\mathrm{diam}(\Gamma^*(G)) = 3$.

For soluble groups, the bound $\mathrm{diam}(\Gamma^*(G)) \leq 3$ is best possible.

Let $H = \mathrm{GL}(2,2) \times \mathrm{GL}(2,2)$ and let $W = V_1 \times V_2 \times V_3 \times V_4$ be the direct product of four 2-dimensional vector spaces over the field $\mathbb{F}_2$. Define an action of H on W by setting

$$(v_1, v_2, v_3, v_4)^{(x,y)} = (v_1^x, v_2^x, v_3^y, v_4^y)$$

and consider the semidirect product $G = W \rtimes H$: $\mathrm{diam}(\Gamma^*(G)) = 3$.

However $\mathrm{diam}(\Gamma^*(G)) \leq 2$ in some relevant cases.

THEOREM (AL 2017)

Suppose that a finite 2-generated soluble group G has the property that $|\mathrm{End}_G(V)| > 2$ for every nontrivial irreducible G-module V which is G-isomorphic to a complemented chief factor of G (this holds for example if the derived subgroup G' is nilpotent or has odd order). Then $\mathrm{diam}(\Gamma^*(G)) \leq 2$, i.e. if $\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle = G$, then there exists $b \in G$ with $\langle a_1, b \rangle = \langle a_2, b \rangle = G$.

Hamiltonian cycle

A Hamiltonian cycle in a graph Γ is a graph cycle that visits each vertex of Γ exactly once.

Theorem (Breuer, Guralnick, Maróti, Nagy, AL 2010)

- *For every sufficiently large finite simple group G, the graph $\Gamma^*(G)$ contains a Hamiltonian cycle.*
- *For every sufficiently large symmetric group S_n, the graph $\Gamma^*(S_n)$ contains a Hamiltonian cycle.*
- *Let G be a finite soluble group. If the identity is the unique isolated vertex of $\Gamma(G)$, then $\Gamma^*(G)$ contains a Hamiltonian cycle.*

Hamiltonian cycle

A Hamiltonian cycle in a graph Γ is a graph cycle that visits each vertex of Γ exactly once.

Theorem (Breuer, Guralnick, Maróti, Nagy, AL 2010)

- *For every sufficiently large finite simple group G, the graph $\Gamma^*(G)$ contains a Hamiltonian cycle.*
- *For every sufficiently large symmetric group S_n, the graph $\Gamma^*(S_n)$ contains a Hamiltonian cycle.*
- *Let G be a finite soluble group. If the identity is the unique isolated vertex of $\Gamma(G)$, then $\Gamma^*(G)$ contains a Hamiltonian cycle.*

It was conjectured that if 1 is the unique isolated vertex of $\Gamma(G)$, then $\Gamma^*(G)$ is Hamiltonian. No counterexample is known to the following stronger conjecture (which holds for example in the nilpotent case):

Hamiltonian cycle

A Hamiltonian cycle in a graph Γ is a graph cycle that visits each vertex of Γ exactly once.

Theorem (Breuer, Guralnick, Maróti, Nagy, AL 2010)

- *For every sufficiently large finite simple group G, the graph $\Gamma^*(G)$ contains a Hamiltonian cycle.*
- *For every sufficiently large symmetric group S_n, the graph $\Gamma^*(S_n)$ contains a Hamiltonian cycle.*
- *Let G be a finite soluble group. If the identity is the unique isolated vertex of $\Gamma(G)$, then $\Gamma^*(G)$ contains a Hamiltonian cycle.*

It was conjectured that if 1 is the unique isolated vertex of $\Gamma(G)$, then $\Gamma^*(G)$ is Hamiltonian. No counterexample is known to the following stronger conjecture (which holds for example in the nilpotent case):

Conjecture

Let G be a finite group. Then $\Gamma^*(G)$ contains a Hamiltonian cycle.

Eulerian graph

A connected graph Γ is Eulerian if it contains a closed trail (a walk with no repeated edges) containing all edges of the graph. A famous result going back to Euler states that a connected graph Γ is Eulerian if and only if every vertex of Γ is of even degree.

Eulerian graph

A connected graph Γ is Eulerian if it contains a closed trail (a walk with no repeated edges) containing all edges of the graph. A famous result going back to Euler states that a connected graph Γ is Eulerian if and only if every vertex of Γ is of even degree.

Proposition (C. Marion, AL 2107)

Let G be a finite group and $1 \neq g \in G$. Let

$$\eta(G) := \begin{cases} 1 \text{ if } |G/G'| \text{ is odd,} \\ 2 \text{ if } |G/G'| \text{ is even.} \end{cases}$$

If $2^{\eta(G)}$ divides $|N_G(\langle g \rangle)|$, then the degree of g in $\Gamma(G)$ is even.

Eulerian graph

A connected graph Γ is Eulerian if it contains a closed trail (a walk with no repeated edges) containing all edges of the graph. A famous result going back to Euler states that a connected graph Γ is Eulerian if and only if every vertex of Γ is of even degree.

Proposition (C. Marion, AL 2107)

Let G be a finite group and $1 \neq g \in G$. Let

$$\eta(G) := \begin{cases} 1 \text{ if } |G/G'| \text{ is odd,} \\ 2 \text{ if } |G/G'| \text{ is even.} \end{cases}$$

If $2^{\eta(G)}$ divides $|N_G(\langle g \rangle)|$, then the degree of g in $\Gamma(G)$ is even.

Theorem (C. Marion, AL 2107)

Let $G = \mathrm{Alt}(n)$ or $G = \mathrm{Sym}(n)$ with $n \geq 3$ and let $1 \neq g \in G$. Then the degree of g in $\Gamma(G)$ is odd if and only if there exists a prime number p congruent to 3 modulo 4 such that $p \in \{n, n-1\}$ and $|g| = p$. In particular, $\Gamma^*(G)$ is Eulerian if and only if n and $n-1$ are not equal to a prime number congruent to 3 modulo 4.

Determines G up to isomorphism?

What kind of group-theoretic information about H can be deduced from knowledge about $\Gamma(H)$ only? We are especially interested in when, if ever, $\Gamma(H)$ determines H up to isomorphism.

If $|G| = |H|$ and $G/\operatorname{Frat} G \cong H/\operatorname{Frat} H$ then $\Gamma(G) \cong \Gamma(H)$. Thus it will be convenient to assume that $\operatorname{Frat} H = 1$. But even this condition is too weak to determine H up to isomorphism.

Determines G up to isomorphism?

What kind of group-theoretic information about H can be deduced from knowledge about $\Gamma(H)$ only? We are especially interested in when, if ever, $\Gamma(H)$ determines H up to isomorphism.

If $|G| = |H|$ and $G/\operatorname{Frat} G \cong H/\operatorname{Frat} H$ then $\Gamma(G) \cong \Gamma(H)$. Thus it will be convenient to assume that $\operatorname{Frat} H = 1$. But even this condition is too weak to determine H up to isomorphism.

Example

Let $C = \langle x \rangle \cong C_5$. Define two actions of C on a vector space $V = \langle a, b \rangle \cong \mathbb{F}_{11}^2$:

$$a^x = 3a,\ b^x = 4b \text{ in the first action,}$$
$$a^x = 3a,\ b^x = 5b \text{ in the second action.}$$

The semidirect product of C with V give rise to two soluble groups, H_1 and H_2, both of order 605 : $H_1 \ncong H_2$, however $\Gamma(H_1) \cong \Gamma(H_2)$.

Theorem (A. Maróti, C. Roney-Dougal, AL 2016)

If H is a sufficiently large simple group with $\Gamma(G) \cong \Gamma(H)$ for a finite group G, then $G \cong H$.

Theorem (A. Maróti, C. Roney-Dougal, AL 2016)

Let G be a finite group.

- *If $\Gamma(G) \cong \Gamma(\mathrm{Alt}(n))$, then $G \cong \mathrm{Alt}(n)$.*
- *If $\Gamma(G) \cong \Gamma(\mathrm{Sym}(n))$, then $G \cong \mathrm{Sym}(n)$.*

Theorem (A. Maróti, C. Roney-Dougal, M. Cervetti, AL)

Let G be a finite soluble group such that $\Gamma(G)$ has a unique isolated vertex, then $\Gamma(G)$ determines G up to isomorphism.

QUESTION

Let G and H be finite groups with $\Gamma(G) \cong \Gamma(H)$.

- *Assume that G is soluble. Is H soluble?*
- *Assume that G is nilpotent. Is H nilpotent?*

QUESTION

Let G and H be finite groups with $\Gamma(G) \cong \Gamma(H)$.

- *Assume that G is soluble. Is H soluble?*
- *Assume that G is nilpotent. Is H nilpotent?*

Only a weak result in this direction is available: if G is nilpotent, H is supersoluble and $\Gamma(G) \cong \Gamma(H)$, then H is nilpotent.

Other graphs

$\Gamma(G)$ encodes significant information only when G is a 2-generator group. We want to introduce a wider family of graphs which encode the generating property of G when G is an arbitrary finite group.

Definition

Assume that G is a finite group and let a and $b \in \mathbb{N}$. We define an undirected graph $\Gamma_{a,b}(G)$ whose vertices correspond to the elements of $G^a \cup G^b$ and in which two tuples $(x_1, \ldots, x_a)$ and $(y_1, \ldots, y_b)$ are adjacent if and only $\langle x_1, \ldots, x_a, y_1, \ldots, y_b \rangle = G$.

Other graphs

$\Gamma(G)$ encodes significant information only when G is a 2-generator group. We want to introduce a wider family of graphs which encode the generating property of G when G is an arbitrary finite group.

Definition

Assume that G is a finite group and let a and $b \in \mathbb{N}$. We define an undirected graph $\Gamma_{a,b}(G)$ whose vertices correspond to the elements of $G^a \cup G^b$ and in which two tuples $(x_1, \dots, x_a)$ and $(y_1, \dots, y_b)$ are adjacent if and only $\langle x_1, \dots, x_a, y_1, \dots, y_b \rangle = G$.

Notice that $\Gamma_{1,1}(G) = \Gamma(G)$, so these graphs can be viewed as a natural generalization of the generating graph.

Other graphs

$\Gamma(G)$ encodes significant information only when G is a 2-generator group. We want to introduce a wider family of graphs which encode the generating property of G when G is an arbitrary finite group.

Definition

Assume that G is a finite group and let a and $b \in \mathbb{N}$. We define an undirected graph $\Gamma_{a,b}(G)$ whose vertices correspond to the elements of $G^a \cup G^b$ and in which two tuples $(x_1, \ldots, x_a)$ and $(y_1, \ldots, y_b)$ are adjacent if and only $\langle x_1, \ldots, x_a, y_1, \ldots, y_b \rangle = G$.

Notice that $\Gamma_{1,1}(G) = \Gamma(G)$, so these graphs can be viewed as a natural generalization of the generating graph.

Definition

We denote by $\Gamma^*_{a,b}(G)$ the graph obtained from $\Gamma_{a,b}(G)$ by deleting the isolated vertices.

Definition

The swap graph $\Sigma_d(G)$ is the graph in which the vertices are the ordered generating d-tuples and two vertices $(x_1, \ldots, x_d)$ and $(y_1, \ldots, y_d)$ are adjacent if and only if they differ only by one entry.

Definition

The swap graph $\Sigma_d(G)$ is the graph in which the vertices are the ordered generating d-tuples and two vertices $(x_1, \ldots, x_d)$ and $(y_1, \ldots, y_d)$ are adjacent if and only if they differ only by one entry.

Proposition

If $\Sigma_{a+b}(G)$ is connected, then $\Gamma^*_{a,b}(G)$ is also connected.

Definition

The swap graph $\Sigma_d(G)$ is the graph in which the vertices are the ordered generating d-tuples and two vertices $(x_1, \ldots, x_d)$ and $(y_1, \ldots, y_d)$ are adjacent if and only if they differ only by one entry.

Proposition

If $\Sigma_{a+b}(G)$ is connected, then $\Gamma^*_{a,b}(G)$ is also connected.

Tennant and Turner conjectured that the swap graph is connected for every group. Roman'kov proved that the free metabelian group of rank 3 does not satisfy this conjecture but no counterexample is known in the class of finite groups.

Theorem (E. Crestani, M. Di Summa, AL)

$\Sigma_d(G)$ is connected if either $d > d(G)$ or $d = d(G)$ and G is soluble (where $d(G)$ is the minimum number of generators of G).

Definition

The swap graph $\Sigma_d(G)$ is the graph in which the vertices are the ordered generating d-tuples and two vertices $(x_1, \dots, x_d)$ and $(y_1, \dots, y_d)$ are adjacent if and only if they differ only by one entry.

Proposition

If $\Sigma_{a+b}(G)$ is connected, then $\Gamma^*_{a,b}(G)$ is also connected.

Tennant and Turner conjectured that the swap graph is connected for every group. Roman'kov proved that the free metabelian group of rank 3 does not satisfy this conjecture but no counterexample is known in the class of finite groups.

Theorem (E. Crestani, M. Di Summa, AL)

$\Sigma_d(G)$ is connected if either $d > d(G)$ or $d = d(G)$ and G is soluble (where $d(G)$ is the minimum number of generators of G).

Corollary

The graphs $\Gamma^*_{a,b}(G)$ are connected, except possibly when $a + b = d(G)$ and G is not soluble.

BOUNDING THE DIAMETER OF $\Gamma^*_{a,b}(G)$

THEOREM (C. ACCIARRI, AL 2017)

Assume that G is a finite soluble group and that $(x_1, \ldots, x_b)$ *and* $(y_1, \ldots, y_b)$ *are non-isolated vertices of* $\Gamma_{a,b}(G)$. *If either* $a \neq 1$ *or* $|\mathrm{End}_G(V)| > 2$ *for every non-trivial irreducible G-module V which is G-isomorphic to a complemented chief factor of G, then there exists* $z_1, \ldots, z_a \in G$ *s.t.* $G = \langle z_1, \ldots, z_a, x_1, \ldots, x_b \rangle = \langle z_1, \ldots, z_a, y_1, \ldots, y_b \rangle$.

The previous statement does not remain true if we drop off the assumption on the endomorphism group of irreducible *G*-module.

Bounding the diameter of $\Gamma^*_{a,b}(G)$

Theorem (C. Acciarri, AL 2017)

Assume that G is a finite soluble group and that $(x_1, \dots, x_b)$ and $(y_1, \dots, y_b)$ are non-isolated vertices of $\Gamma_{a,b}(G)$. If either $a \neq 1$ or $|\operatorname{End}_G(V)| > 2$ for every non-trivial irreducible G-module V which is G-isomorphic to a complemented chief factor of G, then there exists $z_1, \dots, z_a \in G$ s.t. $G = \langle z_1, \dots, z_a, x_1, \dots, x_b \rangle = \langle z_1, \dots, z_a, y_1, \dots, y_b \rangle$.

The previous statement does not remain true if we drop off the assumption on the endomorphism group of irreducible G-module.

Corollary

$\operatorname{diam}(\Gamma^*_{a,b}(G)) \leq 4$ *whenever G is soluble and $a + b \geq d(G)$.*

Corollary

If G is soluble and $|\operatorname{End}_G(V)| > 2$ for every non-trivial irreducible G-module V which is G-isomorphic to a complemented chief factor of G, then the diameter of the swap graph $\Sigma_d(G)$ is at most $2d - 1$.

The bound $\mathrm{diam}(\Gamma^*_{a,b}(G)) \leq 4$ that holds for finite soluble groups cannot be generalized to an arbitary finite group.

Assume that S is a finite non-abelian simple group and, for $d \geq 2$, let $\tau_d(S)$ be the largest positive integer r such that S^r can be generated by d elements. If a and b are positive integers, then

$$\lim_{p\to\infty} \mathrm{diam}(\Gamma^*_{a,b}(\mathrm{SL}(2,2^p)^{\tau_{a+b}(\mathrm{SL}(2,2^p))})) = \infty.$$

PROPERTIES OF G ENCODED BY THE GRAPHS $\Gamma^*_{a,b}(G)$

DEFINITION

Denote by $\Lambda^*(G)$ the collection of all the connected components of the graphs $\Gamma^*_{a,b}(G)$, for all the possible choices of a, b in $\mathbb{N}$. However for each of the graphs in this family, we don't assume to know from which choice of a, b it arises.

We can think that we packaged all the graphs $\Gamma^*_{a,b}(G)$ in a (quite spacious) box but that we did not pay enough attention during this operation and we lost the information to which group G these graphs correspond and the labels a, b.

PROPERTIES OF G ENCODED BY THE GRAPHS $\Gamma^*_{a,b}(G)$

DEFINITION

Denote by $\Lambda^*(G)$ the collection of all the connected components of the graphs $\Gamma^*_{a,b}(G)$, for all the possible choices of a, b in $\mathbb{N}$. However for each of the graphs in this family, we don't assume to know from which choice of a, b it arises.

We can think that we packaged all the graphs $\Gamma^*_{a,b}(G)$ in a (quite spacious) box but that we did not pay enough attention during this operation and we lost the information to which group G these graphs correspond and the labels a, b. Do not panic.

Properties of G encoded by the graphs $\Gamma^*_{a,b}(G)$

Definition

Denote by $\Lambda^*(G)$ the collection of all the connected components of the graphs $\Gamma^*_{a,b}(G)$, for all the possible choices of a, b in $\mathbb{N}$. However for each of the graphs in this family, we don't assume to know from which choice of a, b it arises.

We can think that we packaged all the graphs $\Gamma^*_{a,b}(G)$ in a (quite spacious) box but that we did not pay enough attention during this operation and we lost the information to which group G these graphs correspond and the labels a, b. Do not panic. A big amount of the lost information can be reconstructed!

Properties of G encoded by the graphs $\Gamma^*_{a,b}(G)$

Definition

Denote by $\Lambda^*(G)$ the collection of all the connected components of the graphs $\Gamma^*_{a,b}(G)$, for all the possible choices of a, b in $\mathbb{N}$. However for each of the graphs in this family, we don't assume to know from which choice of a, b it arises.

We can think that we packaged all the graphs $\Gamma^*_{a,b}(G)$ in a (quite spacious) box but that we did not pay enough attention during this operation and we lost the information to which group G these graphs correspond and the labels a, b. Do not panic. A big amount of the lost information can be reconstructed!

Proposition (C. Acciarri, AL)

From the knowledge of $\Lambda^*(G)$ we may recover $d(G)$, $|G|$ and the labels a, b, at least when $a + b > d(G)$.

Philip Hall observed that the probability of generating a given finite group G by a random t-tuple of elements is given by

$$P_G(t) = \frac{\phi_G(t)}{|G|^t} = \sum_{n \in \mathbb{N}} \frac{a_n(G)}{n^t} \text{ where } a_n(G) = \sum_{|G:H|=n} \mu_G(H)$$

and μ is the Möbius function on the subgroup lattice of G. In other words there exists a uniquely determined Dirichlet polynomial $P_G(s)$ with the property that, for every $t \in \mathbb{N}$, the number $P_G(t)$ coincides with the probability of generating G by t random elements.

Philip Hall observed that the probability of generating a given finite group G by a random t-tuple of elements is given by

$$P_G(t) = \frac{\phi_G(t)}{|G|^t} = \sum_{n \in \mathbb{N}} \frac{a_n(G)}{n^t} \text{ where } a_n(G) = \sum_{|G:H|=n} \mu_G(H)$$

and μ is the Möbius function on the subgroup lattice of G. In other words there exists a uniquely determined Dirichlet polynomial $P_G(s)$ with the property that, for every $t \in \mathbb{N}$, the number $P_G(t)$ coincides with the probability of generating G by t random elements.

Let $t = a + b$. The number $\phi_G(t)$ of the ordered generating t-tuples of G may be determined by counting the edges of the graph $\Gamma^*_{a,b}(G)$.

We may determine $P_G(s)$ from the knowledge of $\Lambda^*(G)$. Consequently we may also recover from $\Lambda^*(G)$ all the information that can be determined from $P_G(s)$. In particular we may determine whether G is soluble, whether G is supersoluble and, for every prime power n, the number of maximal subgroups of G of index n.

$\Lambda^*(G)$ encodes information on G that cannot be deduced from $P_G(s)$.

THEOREM (C. ACCIARRI, AL)

Let G be a finite nilpotent group. If $\Lambda^*(H) = \Lambda^*(G)$, then H is nilpotent.

PROPOSITION (C. ACCIARRI, AL)

We may determine $|\mathrm{Frat}\, G|$ from the knowledge of $\Lambda^*(G)$.

COROLLARY (C. ACCIARRI, AL)

Let G be a finite non-abelian simple group. If $\Lambda^*(H) = \Lambda^*(G)$, then $H \cong G$.

$\Lambda^*(G)$ encodes information on G that cannot be deduced from $P_G(s)$.

Theorem (C. Acciarri, AL)

Let G be a finite nilpotent group. If $\Lambda^*(H) = \Lambda^*(G)$, then H is nilpotent.

Proposition (C. Acciarri, AL)

We may determine $|\mathrm{Frat}\, G|$ from the knowledge of $\Lambda^*(G)$.

Corollary (C. Acciarri, AL)

Let G be a finite non-abelian simple group. If $\Lambda^*(H) = \Lambda^*(G)$, then $H \cong G$.

All the above mentioned properties of G could be deduced taking into account only the graphs of the form $\Gamma^*_{1,b}(G)$ for $b \in \mathbb{N}$.

A NEW FAMILY OF RELATIONS

We may define an equivalence relation $\equiv_{\mathrm{m}}$ on G as follows: two elements are equivalent if each can be substituted for the other in any generating set for G. It can be easily seen that $x \equiv_{\mathrm{m}} y$ if and only if x and y lie in exactly the same maximal subgroups of G.

A new family of relations

We may define an equivalence relation $\equiv_{\mathrm{m}}$ on G as follows: two elements are equivalent if each can be substituted for the other in any generating set for G. It can be easily seen that $x \equiv_{\mathrm{m}} y$ if and only if x and y lie in exactly the same maximal subgroups of G.

We may refine this to a sequence $\equiv_{\mathrm{m}}^{(r)}$ of equivalence relations. Let $r \in \mathbb{N}$. For $x, y \in G$, say $x \equiv_{\mathrm{m}}^{(r)} y$ if, for every $z_1, \ldots, z_{r-1} \in G$,

$$\langle x, z_1, \ldots, z_{r-1} \rangle = G \quad \Leftrightarrow \quad \langle y, z_1, \ldots, z_{r-1} \rangle = G.$$

So x and y can be interchanged in any generating set of size $\leq r$.

$x \equiv_{\mathrm{m}}^{(r)} y$ if and only if x and y have the same neighbours in $\Gamma_{1,r-1}(G)$.

A new family of relations

We may define an equivalence relation $\equiv_{\mathrm{m}}$ on G as follows: two elements are equivalent if each can be substituted for the other in any generating set for G. It can be easily seen that $x \equiv_{\mathrm{m}} y$ if and only if x and y lie in exactly the same maximal subgroups of G.

We may refine this to a sequence $\equiv_{\mathrm{m}}^{(r)}$ of equivalence relations. Let $r \in \mathbb{N}$. For $x, y \in G$, say $x \equiv_{\mathrm{m}}^{(r)} y$ if, for every $z_1, \ldots, z_{r-1} \in G$,

$$\langle x, z_1, \ldots, z_{r-1} \rangle = G \quad \Leftrightarrow \quad \langle y, z_1, \ldots, z_{r-1} \rangle = G.$$

So x and y can be interchanged in any generating set of size $\leq r$.

$x \equiv_{\mathrm{m}}^{(r)} y$ if and only if x and y have the same neighbours in $\Gamma_{1,r-1}(G)$.

The relations $\equiv_{\mathrm{m}}^{(r)}$ become finer as r increases. We define $\psi(G)$ to be the value of r at which the relations $\equiv_{\mathrm{m}}^{(r)}$ stabilise to $\equiv_{\mathrm{m}}$.

Theorem (P. Cameron, C. Roney-Dougal, AL 2016)

If G is a finite group, then $d(G) \leq \psi(G) \leq d(G) + 5$. Furthermore, if G is simple, then $\psi(G) \leq 5$, and if G is almost simple then $\psi(G) \leq 7$.

Theorem (P. Cameron, C. Roney-Dougal, AL 2016)

If G is a finite soluble group, then $d(G) \leq \psi(G) \leq d(G) + 1$.

Theorem (P. Cameron, C. Roney-Dougal, AL 2016)

Let G be a finite soluble group. The following are equivalent:

- $\psi(G) = d(G)$.
- *If g is an isolated vertex of $\Gamma_{1,d(G)-1}(G)$, then $g \in \mathrm{Frat}(G)$.*

Let G be an almost simple group with socle of order less than 10.000 such that all proper quotients of G are cyclic. Then $\psi(G) = 2$.

Question

Does there exist a group G for which $\psi(G) > d(G) + 1$?

A FINER RELATION

DEFINITION

Let G be a finite group and let $x, y \in G$. We define $x \equiv_{\mathrm{c}} y$ if $\langle x \rangle = \langle y \rangle$.

THEOREM (P. CAMERON, C. RONEY-DOUGAL, AL 2016)

Let G be a group for which $\equiv_{\mathrm{c}}$ coincides with $\equiv_{\mathrm{m}}$.

1. *We have a (messy) characterisation of such soluble G.*
2. $\operatorname{Frat} G = 1$.
3. *$G/\operatorname{soc} G$ is soluble, and if G has a nonabelian minimal normal subgroup $N \cong S_1 \times \cdots \times S_t$ then either $t = 1$ or $t = 2$ and $S_1 \cong \mathrm{P}\,\Omega_8^+(q)$ with $q \leq 3$.*

QUESTION

Characterise the insoluble G for which $\equiv_{\mathrm{c}}$ coincides with $\equiv_{\mathrm{m}}$.

Automorphism group of $\Gamma(G)$

$\mathrm{Aut}(\Gamma(G))$ is MASSIVE! For example $|\mathrm{Aut}(\Gamma(\mathrm{Alt}(5)))| = 2^{31} \cdot 3^{7} \cdot 5$.

Automorphism group of $\Gamma(G)$

$\mathrm{Aut}(\Gamma(G))$ is MASSIVE! For example $|\mathrm{Aut}(\Gamma(\mathrm{Alt}(5)))| = 2^{31} \cdot 3^7 \cdot 5$.

A graph reduction

For vertices x, y of a graph Γ, say $x \equiv_\Gamma y$ if x and y have the same neighbours. By identifying equivalence classes, we get the quotient graph $\overline{\Gamma}$.

- If $\Gamma = \Gamma(G)$ then $\equiv_\Gamma$ is $\equiv_{\mathrm{m}}^{(2)}$.
- If $x \equiv_\Gamma y$ then $(x, y) \in \mathrm{Aut}(\Gamma)$.

We define a weighting of $\overline{\Gamma}$, by assigning to each vertex a weight which is the cardinality of the corresponding $\equiv_\Gamma$-class. Let $\overline{\Gamma}_{\mathrm{w}}(G)$ denote the weighted graph, and let $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ be the group of weight-preserving automorphisms of $\overline{\Gamma}_{\mathrm{w}}(G)$.

AUTOMORPHISM GROUP OF $\Gamma(G)$

$\mathrm{Aut}(\Gamma(G))$ is MASSIVE! For example $|\mathrm{Aut}(\Gamma(\mathrm{Alt}(5)))| = 2^{31} \cdot 3^7 \cdot 5$.

A GRAPH REDUCTION

For vertices x, y of a graph Γ, say $x \equiv_\Gamma y$ if x and y have the same neighbours. By identifying equivalence classes, we get the quotient graph $\overline{\Gamma}$.

- If $\Gamma = \Gamma(G)$ then $\equiv_\Gamma$ is $\equiv_{\mathrm{m}}^{(2)}$.
- If $x \equiv_\Gamma y$ then $(x, y) \in \mathrm{Aut}(\Gamma)$.

We define a weighting of $\overline{\Gamma}$, by assigning to each vertex a weight which is the cardinality of the corresponding $\equiv_\Gamma$-class. Let $\overline{\Gamma}_{\mathrm{w}}(G)$ denote the weighted graph, and let $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$ be the group of weight-preserving automorphisms of $\overline{\Gamma}_{\mathrm{w}}(G)$.

PROPOSITION

Let the $\equiv_\Gamma$-classes of a finite group G be of sizes $k_1, \ldots, k_n$. Then

$$\mathrm{Aut}(\Gamma(G)) = (\mathrm{Sym}(k_1) \times \cdots \times \mathrm{Sym}(k_n)) \rtimes \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)).$$

Example ($G = \mathrm{Alt}(5)$)

- $\psi(G) = 2$ and the relations $\equiv_{\mathrm{m}}$, $\equiv_{\Gamma}$ and $\equiv_{\mathrm{c}}$ are all equal.
- There are: 6 classes containing 4 of elements of order 5, 10 classes containing 2 elements of order 3 and 16 singletons.
- The kernel of the action of $\mathrm{Aut}(\Gamma(G))$ on the classes is isomorphic to $(\mathrm{Sym}(4))^6 \times (\mathrm{Sym}(2))^{10}$.
- $\mathrm{Aut}(\overline{\Gamma}_w(\mathrm{Alt}(5))) = \mathrm{Aut}(\overline{\Gamma}(\mathrm{Alt}(5)) = \mathrm{Sym}(5)$.
- $\mathrm{Aut}(\Gamma(G)) \cong \big((\mathrm{Sym}(4))^6 \times (\mathrm{Sym}(2))^{10}\big) \rtimes \mathrm{Sym}(5).$

DEFINITION

G has spread k if k is the largest number such that for any set S of k nonidentity elements, there exists x such that $\langle x, s\rangle = G$ for all $s \in S$.

- The spread is nonzero if and only if no vertex of the generating graph except the identity is isolated.
- Breuer, Guralnick and Kantor conjectured that G has nonzero spread if and only if every proper quotient is cyclic.

Definition

G has spread k if k is the largest number such that for any set S of k nonidentity elements, there exists x such that $\langle x, s \rangle = G$ for all $s \in S$.

- The spread is nonzero if and only if no vertex of the generating graph except the identity is isolated.
- Breuer, Guralnick and Kantor conjectured that G has nonzero spread if and only if every proper quotient is cyclic.

Question

Let G be insoluble and of nonzero spread. Is $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G))$*?*

We know of no examples where this is not the case. For example if G is an almost simple group with socle of order less than 10.000 such that all proper quotients of G are cyclic, then $\mathrm{Aut}(\overline{\Gamma}_{\mathrm{w}}(G)) = \mathrm{Aut}(G)$.

A more general definition of nonzero spread

Generalizing the definition given before, we say that G has nonzero spread if g is not isolated in $\Gamma_{1,d(G)-1}(G)$ whenever $g \neq 1$.

Conjecture

A finite group G has nonzero spread if and only if $d(G/N) < d(G)$ for every nontrivial normal subgroup N of G.

Let L be a monolithic primitive group and let A be its unique minimal normal subgroup. For each positive integer k, the crown-based power of L of size k is the subgroup L_k of L^k defined by

$$L_k = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod A\}.$$

Theorem (C. Acciarri, AL)

The previous conjecture is true except possibly when $d(G) = 2$.