Graphs defined on groups

Peter J. Cameron, University of St Andrews



7th International Conference on Combinatorics, Cryptography, Computer Science and Computation 16 November 2022

As my title slide suggests, there are many people currently working on this topic, in Iran, India, China, and various other countries.

As my title slide suggests, there are many people currently working on this topic, in Iran, India, China, and various other countries.

I will give a few results along the way. But my main purpose is to address the question: Why study graphs on groups? There are several reasons:

As my title slide suggests, there are many people currently working on this topic, in Iran, India, China, and various other countries.

I will give a few results along the way. But my main purpose is to address the question: Why study graphs on groups? There are several reasons:

• We learn new results about groups.

As my title slide suggests, there are many people currently working on this topic, in Iran, India, China, and various other countries.

I will give a few results along the way. But my main purpose is to address the question: Why study graphs on groups? There are several reasons:

- We learn new results about groups.
- Using graphs we can characterise some important classes of groups.

As my title slide suggests, there are many people currently working on this topic, in Iran, India, China, and various other countries.

I will give a few results along the way. But my main purpose is to address the question: Why study graphs on groups? There are several reasons:

- We learn new results about groups.
- Using graphs we can characterise some important classes of groups.
- We might find some beautiful graphs in the process.

I am not talking about Cayley graphs. My graphs will be defined simply in terms of the group structure, and so will be invariant under all automorphisms of the group.

• The commuting graph: $x \sim y$ if xy = yx.

- The commuting graph: $x \sim y$ if xy = yx.
- The generating graph: $x \sim y$ if $\langle x, y \rangle = G$.

- The commuting graph: $x \sim y$ if xy = yx.
- The generating graph: $x \sim y$ if $\langle x, y \rangle = G$.
- The power graph: x ~ y if one of x and y is a power of the other.

The commuting graph

The first appearance of the commuting graph was in a paper of Brauer and Fowler in 1955. Curiously they did not use the word "graph" anywhere in the paper; but central to their argument is the graph distance in this graph on a finite simple group, with the identity removed (since it commutes with everything).

The commuting graph

The first appearance of the commuting graph was in a paper of Brauer and Fowler in 1955. Curiously they did not use the word "graph" anywhere in the paper; but central to their argument is the graph distance in this graph on a finite simple group, with the identity removed (since it commutes with everything).

This very important paper is arguably the first step on the road to the Classification of Finite Simple Groups (though that took 50 years to complete). An involution is an element of order 2; its centraliser is the set of elements which commute with it. Brauer and Fowler proved:

Theorem

The order of a finite simple group of even order is bounded by a function of the order of the centraliser of an involution; so there are only finitely many simple groups having a given involution centraliser.

Remarks

At the time, it was not known that a finite simple group must have even order; the Feit–Thompson Theorem came only eight years later.

Remarks

At the time, it was not known that a finite simple group must have even order; the Feit–Thompson Theorem came only eight years later. Subsequently, characterising simple groups with a given involution centraliser was a key tool in the proof of CFSG.

Remarks

At the time, it was not known that a finite simple group must have even order; the Feit–Thompson Theorem came only eight years later.

Subsequently, characterising simple groups with a given involution centraliser was a key tool in the proof of CFSG. The centraliser of an element of a group is the set of its neighbours in the commuting graph. The argument of Brauer and Fowler went, in brief, like this. They give an absolute bound for the diameter of this graph. Then using the fact that involutions have finite valency, they can convert this into a bound for the number of vertices, using graph-theoretic arguments.

Other groups

In general, to study the diameter of commuting graphs, we should remove the centre of the group, the set of elements which commute with everything in the group, since if these remain then any two vertices are joined by a path of length 2 via the centre.

Other groups

In general, to study the diameter of commuting graphs, we should remove the centre of the group, the set of elements which commute with everything in the group, since if these remain then any two vertices are joined by a path of length 2 via the centre.

On the basis of this and other evidence, Iranmanesh and Jafarzadeh conjectured that there is an absolute bound for the diameter of the commuting graph of any finite group (with the centre removed). Their conjecture was proved for groups with trivial centre by Morgan and Parker; but Giudici and Parker showed that it is false for general groups, where the diameter can be arbitrarily large.

Other groups

In general, to study the diameter of commuting graphs, we should remove the centre of the group, the set of elements which commute with everything in the group, since if these remain then any two vertices are joined by a path of length 2 via the centre.

On the basis of this and other evidence, Iranmanesh and Jafarzadeh conjectured that there is an absolute bound for the diameter of the commuting graph of any finite group (with the centre removed). Their conjecture was proved for groups with trivial centre by Morgan and Parker; but Giudici and Parker showed that it is false for general groups, where the diameter can be arbitrarily large.

It may be worth looking at the Giudici–Parker graphs to see if they have interesting graph-theoretic properties.

I would like to mention another example where graphs are used to prove a result about groups.

I would like to mention another example where graphs are used to prove a result about groups. In 1903, Landau proved:

I would like to mention another example where graphs are used to prove a result about groups. In 1903, Landau proved:

Theorem

The order of a group G is bounded by a function of the number k(G) of conjugacy classes.

I would like to mention another example where graphs are used to prove a result about groups. In 1903, Landau proved:

Theorem

The order of a group G is bounded by a function of the number k(G) of conjugacy classes.

The proof goes like this. The conjugacy classes are orbits of the group acting on itself by conjugation; the stabiliser of a point is its centraliser. So the Orbit-Stabiliser Theorem shows that $|C_G(x)| = |G|/|x^G|$, where $C_G(x)$ is the centraliser of x and x^G the conjugacy class containing x.

Since the conjugacy classes partition *G*, we have

$$|G| = \sum_{i=1}^{k} |G| / |C_G(x_i)|,$$

where x_i runs over a set of conjugacy class representatives. Putting $n_i = |C_G(x_i)|$ and dividing by *G*, we have

$$\sum_{i=1}^k 1/n_i = 1.$$

For given *k*, this equation has only finitely many solutions in positive integers. (This is an exercise!)

Since the conjugacy classes partition *G*, we have

$$|G| = \sum_{i=1}^{k} |G| / |C_G(x_i)|,$$

where x_i runs over a set of conjugacy class representatives. Putting $n_i = |C_G(x_i)|$ and dividing by *G*, we have

$$\sum_{i=1}^k 1/n_i = 1.$$

For given *k*, this equation has only finitely many solutions in positive integers. (This is an exercise!) Now $|G| = |C_G(1)|$ is the largest value of n_i to occur in a solution arising from a group *G*. So there are only finitely many possible groups.

Estimates

To a combinatorialist, this theorem demands good upper bounds on the function involved. Equivalently, a lower bound on the least number f(n) of conjugacy classes of a group of order n.

Estimates

To a combinatorialist, this theorem demands good upper bounds on the function involved. Equivalently, a lower bound on the least number f(n) of conjugacy classes of a group of order n.

The first into the fray were Erdős and Rényi, who showed that $f(n) \ge \log \log n$ (logarithms to base 2). This was improved by Laci Pyber to $\epsilon \log n / (\log \log n)^8$ by Pyber; the exponent 8 was reduced to 7 by Keller, and to $3 + \epsilon$ by Baumeister, Maróti and Tong-Viet. It is conjectured that a bound of the form $f(n) \ge C \log n$ holds for some constant *C*. In the other direction, $f(n) \le (\log n)^3$.

Estimates

To a combinatorialist, this theorem demands good upper bounds on the function involved. Equivalently, a lower bound on the least number f(n) of conjugacy classes of a group of order n.

The first into the fray were Erdős and Rényi, who showed that $f(n) \ge \log \log n$ (logarithms to base 2). This was improved by Laci Pyber to $\epsilon \log n / (\log \log n)^8$ by Pyber; the exponent 8 was reduced to 7 by Keller, and to $3 + \epsilon$ by Baumeister, Maróti and Tong-Viet. It is conjectured that a bound of the form $f(n) \ge C \log n$ holds for some constant *C*. In the other direction, $f(n) \le (\log n)^3$.

I am going to show a different development of Landau's theorem.

The solvable conjugacy class graph of the group *G* is defined as follows: the vertices are the conjugacy classes; two classes x^G and y^G are joined if there exist $x' \in x^G$ and $y' \in y^G$ such that $\langle x', y' \rangle$ is a solvable group.

The solvable conjugacy class graph of the group *G* is defined as follows: the vertices are the conjugacy classes; two classes x^G and y^G are joined if there exist $x' \in x^G$ and $y' \in y^G$ such that $\langle x', y' \rangle$ is a solvable group.

Thus Landau showed that |G| is bounded by a function of the number of vertices of this graph. With Parthajit Bhowal, Rajat Kanti Nath and Benjamin Sambale, I showed:

The solvable conjugacy class graph of the group *G* is defined as follows: the vertices are the conjugacy classes; two classes x^G and y^G are joined if there exist $x' \in x^G$ and $y' \in y^G$ such that $\langle x', y' \rangle$ is a solvable group.

Thus Landau showed that |G| is bounded by a function of the number of vertices of this graph. With Parthajit Bhowal, Rajat Kanti Nath and Benjamin Sambale, I showed:

Theorem

For any finite group G, |G| is bounded by a founction of the clique size of the solvable conjugacy class graph.

The solvable conjugacy class graph of the group *G* is defined as follows: the vertices are the conjugacy classes; two classes x^G and y^G are joined if there exist $x' \in x^G$ and $y' \in y^G$ such that $\langle x', y' \rangle$ is a solvable group.

Thus Landau showed that |G| is bounded by a function of the number of vertices of this graph. With Parthajit Bhowal, Rajat Kanti Nath and Benjamin Sambale, I showed:

Theorem

For any finite group G, |G| is bounded by a founction of the clique size of the solvable conjugacy class graph.

The proof uses the Classification of Finite Simple Groups, but in a "light-touch" way. Two open problems are finding a proof not using the Classification, and finding decent bounds for the function involved.

For the remainder of the talk, I will consider one particular graph, which I will call the difference graph of the group. It is defined like this:

For the remainder of the talk, I will consider one particular graph, which I will call the difference graph of the group. It is defined like this:

The power graph of G has x ~ y if one of x and y is a power of the other.

For the remainder of the talk, I will consider one particular graph, which I will call the difference graph of the group. It is defined like this:

- The power graph of G has x ~ y if one of x and y is a power of the other.
- ► The enhanced power graph of *G* has *x* ~ *y* if there exists *z* such that both *x* and *y* are powers of *z*; equivalently, if the subgroup (*x*, *y*) generated by *x* and *y* is cyclic.

For the remainder of the talk, I will consider one particular graph, which I will call the difference graph of the group. It is defined like this:

- The power graph of G has x ~ y if one of x and y is a power of the other.
- ► The enhanced power graph of *G* has *x* ~ *y* if there exists *z* such that both *x* and *y* are powers of *z*; equivalently, if the subgroup (*x*, *y*) generated by *x* and *y* is cyclic.
- The difference graph of G, which I will denote by D(G), has as edge set the edges of the enhanced power graph which are not edges of the power graph.
The difference graph

For the remainder of the talk, I will consider one particular graph, which I will call the difference graph of the group. It is defined like this:

- The power graph of G has x ~ y if one of x and y is a power of the other.
- ► The enhanced power graph of *G* has *x* ~ *y* if there exists *z* such that both *x* and *y* are powers of *z*; equivalently, if the subgroup ⟨*x*, *y*⟩ generated by *x* and *y* is cyclic.
- The difference graph of G, which I will denote by D(G), has as edge set the edges of the enhanced power graph which are not edges of the power graph.

The power graph and enhanced power graph seem quite similar; indeed, each determines the other. So we expect the difference graph to be relatively sparse. But the analysis I give here could be repeated for many other graphs defined on *G*, and my guess is that many similar results can be obtained.

Groups with edgeless difference graph

Theorem

For a finite group G, the graph D(G) has no edges if and only if every element of G has prime power order.

Groups with edgeless difference graph

Theorem

For a finite group G, the graph D(G) has no edges if and only if every element of G has prime power order.

One way round this is easy to see. If $g \in G$ has order divisible by two different primes p and q, then x^p and x^q are joined in the enhanced power graph but not in the power graph. The other direction is fairly easy too.

Groups with edgeless difference graph

Theorem

For a finite group G, the graph D(G) has no edges if and only if every element of G has prime power order.

One way round this is easy to see. If $g \in G$ has order divisible by two different primes p and q, then x^p and x^q are joined in the enhanced power graph but not in the power graph. The other direction is fairly easy too.

Such groups are called EPPO groups (acronym for "Elements of Prime Power Order"). Their classification has an interesting history; the problem was introduced by Higman and studied by Suzuki. The classification was achieved by Brandl in 1981 and published in a rather obscure journal, so has been rediscovered a number of times. Similarities between power graph and enhanced power graph

Even if these graphs are not equal, they are not too far apart.

Theorem

The clique number of the enhanced power graph is bounded by a function of the clique number of the power graph. The function has order about n log n. Similarities between power graph and enhanced power graph

Even if these graphs are not equal, they are not too far apart.

Theorem

- The clique number of the enhanced power graph is bounded by a function of the clique number of the power graph. The function has order about n log n.
- The matching numbers of the power graph and enhanced power graph are equal.

Similarities between power graph and enhanced power graph

Even if these graphs are not equal, they are not too far apart.

Theorem

- The clique number of the enhanced power graph is bounded by a function of the clique number of the power graph. The function has order about n log n.
- The matching numbers of the power graph and enhanced power graph are equal.

The proof of the last fact, by Swathi, Sunitha and me, follows familiar graph-theoretic arguments about matchings. If we have a matching in the enhanced power graph containing edges not in the power graph, we can replace it by a matching of the same size with fewer edges not in the power graph. Other group classes defined by graphs

Several further interesting classes of groups can be defined by requiring certain pairs of graphs defined on the groups to be equal. For example,

Other group classes defined by graphs

Several further interesting classes of groups can be defined by requiring certain pairs of graphs defined on the groups to be equal. For example,

Theorem

The enhanced power graph and the commuting graph of G are equal if and only if G has cyclic or generalized quaternion Sylow subgroups.

Other group classes defined by graphs

Several further interesting classes of groups can be defined by requiring certain pairs of graphs defined on the groups to be equal. For example,

Theorem

The enhanced power graph and the commuting graph of *G* are equal if and only if *G* has cyclic or generalized quaternion Sylow subgroups. Other classes defined in similar ways include Dedekind groups (those in which every subgroup is normal), minimal non-abelian groups (or non-nilpotent, or non-solvable), and 2-Engel groups (those satisfying the identity [[x, y], y] = 1, where [x, y] is the commutator $x^{-1}y^{-1}xy$. Some years ago, my colleague Colva Roney-Dougal and I were looking at the generating graph of a group *G*, in which *x* and *y* are joined whenever $\langle x, y \rangle = G$.

Some years ago, my colleague Colva Roney-Dougal and I were looking at the generating graph of a group *G*, in which *x* and *y* are joined whenever $\langle x, y \rangle = G$.

We computed the generating graph of the alternating group A_5 , and asked the computer to tell us the order of its automorphism group. The answer was a shock to us: it was 23482733690880. Things are even worse for the power graph: its automorpism group has order 668594111536199848062615552000000.

Some years ago, my colleague Colva Roney-Dougal and I were looking at the generating graph of a group *G*, in which *x* and *y* are joined whenever $\langle x, y \rangle = G$.

We computed the generating graph of the alternating group A_5 , and asked the computer to tell us the order of its automorphism group. The answer was a shock to us: it was 23482733690880. Things are even worse for the power graph: its automorpism group has order 668594111536199848062615552000000. Why are we getting these huge numbers?

Twins

In brief, the explanation is that, if *x* is an element of order m > 2, then for every positive integer *d* with gcd(m, d) = 1, each of *x* and x^d is a power of the other; so these two elements have the same neighbours (apart from possibly one another) in most of the interesting graphs on *G*: power graph, commuting graph, generating graph, ...

Twins

In brief, the explanation is that, if *x* is an element of order m > 2, then for every positive integer *d* with gcd(m, d) = 1, each of *x* and x^d is a power of the other; so these two elements have the same neighbours (apart from possibly one another) in most of the interesting graphs on *G*: power graph, commuting graph, generating graph, ...

Call two vertices v, w of a graph Γ twins if they have the same neighbours except possibly for one another. (One can distinguish between open twins, with the same open neighbourhoods, and closed twins, with the same closed neighbourhoods, but we will not require this.) Now the relation of being equal or twins is an equivalence relation on the vertex set, and the transposition swapping twins and fixing everything else is an automorphism. Now the relation of being equal or twins is an equivalence relation on the vertex set, and the transposition swapping twins and fixing everything else is an automorphism. Thus, the direct product of symmetric groups on the twin classes is a subgroup of the automorphism group of the graph. This goes some way towards explaining those huge groups we were finding. Now the relation of being equal or twins is an equivalence relation on the vertex set, and the transposition swapping twins and fixing everything else is an automorphism. Thus, the direct product of symmetric groups on the twin classes is a subgroup of the automorphism group of the graph. This goes some way towards explaining those huge groups we were finding.

For example, A_5 has ten subgroups of order 3 (so ten twin classes of size 2) and six subgroups of order 5 (so six twin classes of size 4); so we get a group of order $(2!)^{10}.(4!)^6$ fixing the twin classes. These automorphisms are of no interest! How do we strip them away?

Twin reduction is the process where we find a pair of twins and identify them, continuing until no further twins remain. I will call the result of twin reduction the cokernel of the graph.

Twin reduction is the process where we find a pair of twins and identify them, continuing until no further twins remain. I will call the result of twin reduction the cokernel of the graph. A graph is called a cograph if it contains no induced subgraph isomorphic to the 4-vertex path. Cographs form an interesting and important class: it is the smallest graph class containing the 1-vertex graph and closed under complementation and disjoint union. Moreover, cographs are perfect.

Twin reduction is the process where we find a pair of twins and identify them, continuing until no further twins remain. I will call the result of twin reduction the cokernel of the graph. A graph is called a cograph if it contains no induced subgraph isomorphic to the 4-vertex path. Cographs form an interesting and important class: it is the smallest graph class containing the 1-vertex graph and closed under complementation and disjoint union. Moreover, cographs are perfect.

Theorem

The result of twin reduction is, up to isomorphism, independent of the order in which the reduction steps are done.

Twin reduction is the process where we find a pair of twins and identify them, continuing until no further twins remain. I will call the result of twin reduction the cokernel of the graph. A graph is called a cograph if it contains no induced subgraph isomorphic to the 4-vertex path. Cographs form an interesting and important class: it is the smallest graph class containing the 1-vertex graph and closed under complementation and disjoint union. Moreover, cographs are perfect.

Theorem

- The result of twin reduction is, up to isomorphism, independent of the order in which the reduction steps are done.
- The cokernel of a graph Γ is the 1-vertex graph if and only if Γ is a cograph.

Twin reduction is the process where we find a pair of twins and identify them, continuing until no further twins remain. I will call the result of twin reduction the cokernel of the graph. A graph is called a cograph if it contains no induced subgraph isomorphic to the 4-vertex path. Cographs form an interesting and important class: it is the smallest graph class containing the 1-vertex graph and closed under complementation and disjoint union. Moreover, cographs are perfect.

Theorem

- The result of twin reduction is, up to isomorphism, independent of the order in which the reduction steps are done.
- The cokernel of a graph Γ is the 1-vertex graph if and only if Γ is a cograph.

Problem

Choose a type of graph on groups. For which groups G is this graph defined on G a cograph?

What follows is experimental mathematics. I have done some computations for the power graph and the difference graph (I will concentrate here on the difference graph), but I guess that similar things happen for other types.

What follows is experimental mathematics. I have done some computations for the power graph and the difference graph (I will concentrate here on the difference graph), but I guess that similar things happen for other types.

As a result of computations, I tentatively identify four types of finite simple groups:

What follows is experimental mathematics. I have done some computations for the power graph and the difference graph (I will concentrate here on the difference graph), but I guess that similar things happen for other types.

As a result of computations, I tentatively identify four types of finite simple groups:

Type 1: These are EPPO groups, whose difference graph has no edges at all. As we have seen, all EPPO groups have been determined; the only simple ones are PSL(2,q) and Sz(q) for a few small values of q, together with PSL(3,4).

What follows is experimental mathematics. I have done some computations for the power graph and the difference graph (I will concentrate here on the difference graph), but I guess that similar things happen for other types.

As a result of computations, I tentatively identify four types of finite simple groups:

Type 1: These are EPPO groups, whose difference graph has no edges at all. As we have seen, all EPPO groups have been determined; the only simple ones are PSL(2, q) and Sz(q) for a few small values of q, together with PSL(3, 4).

Type 2: Groups for which the difference graph is a cograph, so that twin reduction gives a graph with a single vertex. The simple groups with this property have been determined, up to some number-theoretic problems which will probably not be solved soon. For example, $D(PSL(2, 2^a))$ is a cograph if and only if each of q - 1 and q + 1 is either a prime power or the product of two distinct primes. Type 3: The cokernel of D(G) is a disjoint union of many copies of a small graph. This seems to happen for the remaining groups PSL(2, q) or Sz(q). For example, for q = 23 or q = 25, it consists of 253 or 325 copies of the graph $K_5 - P_4$.

- Type 3: The cokernel of D(G) is a disjoint union of many copies of a small graph. This seems to happen for the remaining groups PSL(2, q) or Sz(q). For example, for q = 23 or q = 25, it consists of 253 or 325 copies of the graph $K_5 - P_4$.
- Type 4: The cokernel of D(G) is an interesting graph. I mention a few examples.

Type 3: The cokernel of D(G) is a disjoint union of many copies of a small graph. This seems to happen for the remaining groups PSL(2, q) or Sz(q). For example, for q = 23 or q = 25, it consists of 253 or 325 copies of the graph $K_5 - P_4$.

Type 4: The cokernel of D(G) is an interesting graph. I mention a few examples.

For G = PSL(3,3), the cokernel of D(G) has vertex set the set of point-line pairs in the projective plane of order 3. There are two types of pair, flags and antiflags: this gives a bipartition of the graph. The antiflag (P, L) is joined to the flag (Q, M) if and only if $Q \in L$ and $O \in M$. This graph has 169 vertices, diameter 5 and girth 6. The valencies of antiflags are 4, those of flags are 9. This simple graph construction may be worth investigating for other projective planes.

For $G = M_{11}$ (the Mathieu group), the cokernel of D(G) is also bipartite, with bipartite sets of sizes 165 and 220; the graph is semiregular, with valencies 4 and 3 respectively in the two partite sets, and has diameter and girth 10.

For $G = M_{11}$ (the Mathieu group), the cokernel of D(G) is also bipartite, with bipartite sets of sizes 165 and 220; the graph is semiregular, with valencies 4 and 3 respectively in the two partite sets, and has diameter and girth 10. In all Type 4 cases I have looked at, going to the cokernel strips away all the unwanted automorphisms: the automorphism group of the graph turns out to be the same as the automorphism group of the group *G* we start with. For $G = M_{11}$ (the Mathieu group), the cokernel of D(G) is also bipartite, with bipartite sets of sizes 165 and 220; the graph is semiregular, with valencies 4 and 3 respectively in the two partite sets, and has diameter and girth 10.

In all Type 4 cases I have looked at, going to the cokernel strips away all the unwanted automorphisms: the automorphism group of the graph turns out to be the same as the automorphism group of the group *G* we start with.

Problem

Have we seen all the types of behaviour of cokernels of difference graphs of simple groups? Is there a reason why the girth is often large, or why the automorpism group is Aut(G)?

For $G = M_{11}$ (the Mathieu group), the cokernel of D(G) is also bipartite, with bipartite sets of sizes 165 and 220; the graph is semiregular, with valencies 4 and 3 respectively in the two partite sets, and has diameter and girth 10.

In all Type 4 cases I have looked at, going to the cokernel strips away all the unwanted automorphisms: the automorphism group of the graph turns out to be the same as the automorphism group of the group *G* we start with.

Problem

Have we seen all the types of behaviour of cokernels of difference graphs of simple groups? Is there a reason why the girth is often large, or why the automorpism group is Aut(G)?

Further computation would surely find more interesting examples!

More?

Recently a number of new ideas have been introduced into the theory, including supergraphs, invariable generation, and the independence graph. But there is no time to discuss these ...

More?

Recently a number of new ideas have been introduced into the theory, including supergraphs, invariable generation, and the independence graph. But there is no time to discuss these ...



... for your attention.