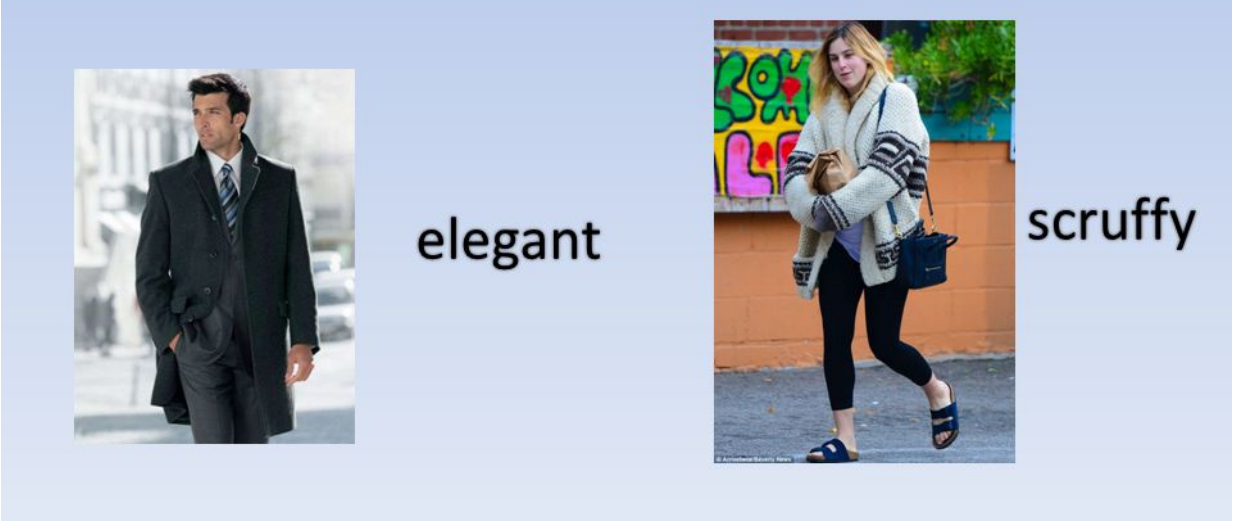
Conversations between groups and graphs

Peter J. Cameron
University of St Andrews

Encontro Nacional SPM 80
15 July 2021

Graphs and groups

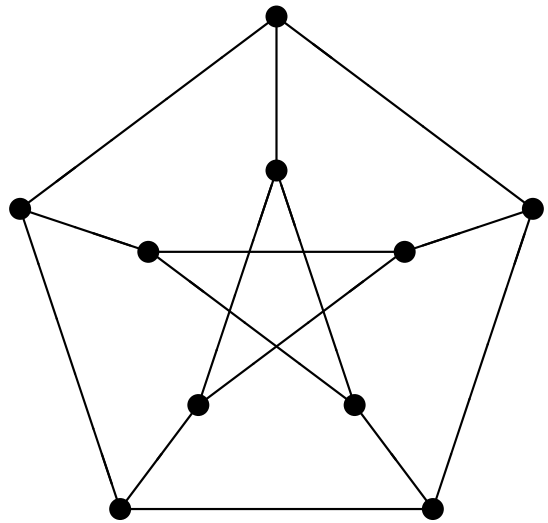
Graphs and groups represent very contrasting parts of the mathematical universe.
Groups measure symmetry; they are highly structured, elegant objects.
Graphs, on the other hand, are "wild": we can put in edges however we please. Some graphs are beautiful, but most are scruffy.



Nevertheless, they have a lot to say to one another.

The Petersen graph

The Petersen graph is a rare example of a beautiful finite graph.



Groups

According to the Jordan–Hölder Theorem, any finite group is constructed from finite simple groups by an extension process. The Classification Theorem for Finite Simple Groups says we know the simple groups. While the extension process is still somewhat mysterious, we can estimate the number of groups of order n reasonably well. Prime power orders are the most prolific, and to a first approximation the number of groups of order p^m is $p^{(2/27)m^3}$.

Infinite groups are a different matter; there is no notion of a "typical" infinite group, and we have to impose some kind of finiteness condition in order to get anywhere (finitely generated or presented, locally finite, profinite, etc.)

Graphs

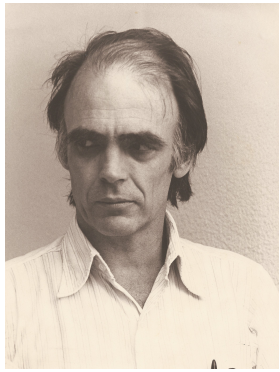
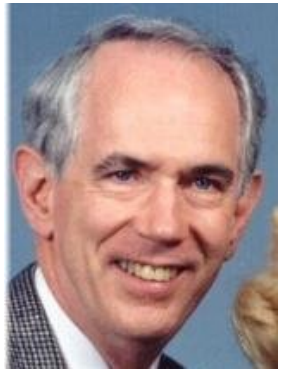
Thinking of all possible graphs that can be drawn on a given vertex set, not only are there very many (about $2^{n(n-1)/2}/n!$ on n vertices), but almost all have no symmetry, and the more symmetric a graph is, the fewer copies there are to find.
For infinite vertex sets, we would expect things to be worse.
But, surprisingly, the following holds:

Theorem

On a countable vertex set, almost all graphs are isomorphic, in either of two senses: there is a graph R such that

- *choosing edges independently with probability $\frac{1}{2}$, the result is almost surely isomorphic to R;*
- *there is a complete metric space structure on the set of graphs, and a comeagre subset of the graphs are isomorphic to R.*

First conversation: Sporadic simple groups

On 3 September 1967, Donald Higman and Charles Sims were at a group theory conference in Oxford. Marshall Hall had just announced the construction of the simple group discovered by Zvonimir Janko, as a permutation group on 100 points. At the conference dinner, Higman and Sims wondered whether there might be another sporadic simple group which was also a permutation group on 100 points. By the end of the evening they had found one.

R. D. Carmichael had constructed in 1931, and Ernst Witt proved unique in 1938, a configuration with 22 points and 77 blocks whose automorphism group contained the Mathieu group M_{22} as a subgroup of index 2. Higman and Sims built a graph from Witt's design. The vertex set consisted of the points and the blocks and one additional point $*$; the edges were given by three simple rules:

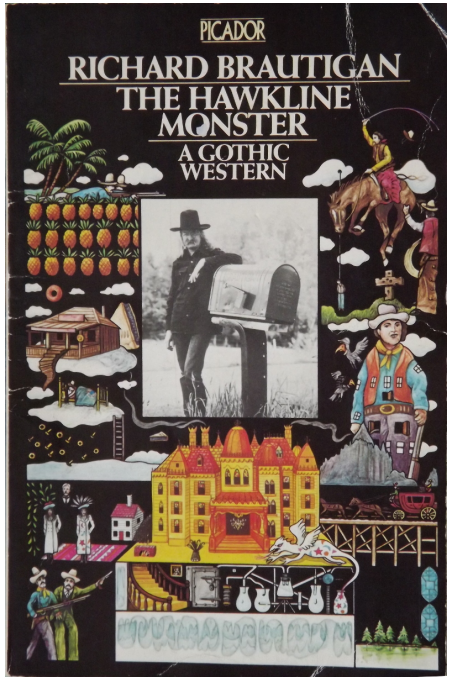
- $*$ is joined to all points;
- a point and block are joined if they are incident;
- two blocks are joined if they are disjoint (no point is incident to both).

Now they had to show that the graph looks the same from any point; this follows from standard properties and uniqueness of the design. It follows that its automorphism group is transitive, and contains a (new) simple group as a subgroup of index 2.

Historical note

It turned out that Dale Mesner, working in combinatorics and statistics, had constructed this graph more than ten years earlier. He had defined a class of graphs he called ”negative Latin square graphs”, and constructed this graph as an example.
He was unaware of the work of Carmichael and Witt, so had to work much harder; and he was not a group theorist, and didn’t think to consider its automorphism group.

Counting

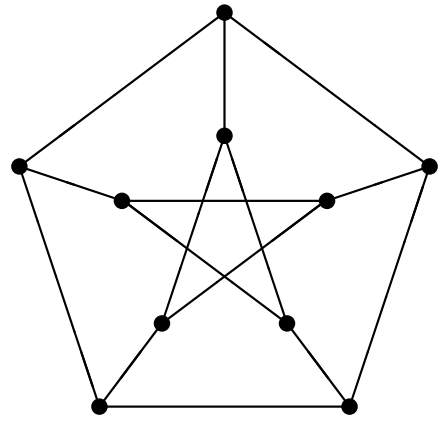


"I count a lot of things that there's no need to count," Cameron said. "Just because that's the way I am. But I count all the things that need to be counted."

Richard Brautigan, *The Hawkline Monster: A Gothic Western*

Second conversation: Orbital chromatic number

Look at the Petersen graph again.



In how many ways can I colour it with q colours, so that adjacent vertices get different colours?
The answer is a monic polynomial in q whose degree is equal to the number of vertices. This is the chromatic polynomial of the graph.

The chromatic polynomial

The chromatic polynomial of a graph was introduced by Birkhoff as a tool to prove the (then) conjecture that planar graphs can be coloured with four colours: in other words, the chromatic polynomial P_Γ of a planar graph Γ does not have 4 as a root.
His attempt was unsuccessful, and the proof of the Four-Colour Conjecture required quite different methods.
But it is still of great interest. Not so long ago, Alan Sokal overturned a long-standing conjecture by proving that (complex) roots of chromatic polynomials of graphs are dense in the complex plane. This result is related to the Lee–Yang theory of phase transitions in the Potts model in statistical mechanics.

Back to the Petersen graph

A polynomial of degree 10 grows quite rapidly. Indeed, the Petersen graph has 2055598560 colourings with 10 colours.
For some applications such as radio frequency allocation, we don't care about the actual colourings; only the partitions into colour classes are useful. Can we find this number?
Yes: the parts of a partition are all non-empty, so the first job is to count the colourings in which all colours are actually used. This is a job for the Inclusion-Exclusion Principle. Having found the answer, we simply divide by $q!$ to give the number of partitions.

Up to symmetry

Another approach would be to say that the Petersen graph has a lot of symmetry (indeed, its automorphism group has order 120 and is isomorphic to the symmetric group S_5), and we don't want to count colourings as distinct if they are related by an automorphism of the graph.

There is another polynomial that does this job, the orbital chromatic polynomial. This takes account of both the graph and the group of automorphisms. (We are not constrained to use all the automorphisms if a subgroup is more convenient.) It is a polynomial whose degree is the number of vertices, and whose leading coefficient is $1/|G|$, where G is the group of automorphisms being used.

What if we want to combine the two approaches, and count colour partitions up to the action of an automorphism group? Finding a formula for this is an unsolved problem. It can be worked out by brute-force computation.

The table below gives results for the Petersen graph. The first row gives the number of colourings (the evaluation of the chromatic polynomial). The second gives the number of partitions into colour classes. The third gives the number of colourings up to the action of the full automorphism group, and the fourth the number of partitions up to the action of the automorphism group.

q	3	4	5	6	7	8	9	10
	120	12960	332880	3868080	27767880	144278400	594347040	2055598560
	20	520	2244	2865	1435	315	30	1
	6	208	3624	36654	248234	1254120	5089392	17449788
	1	10	30	36	20	7	1	1

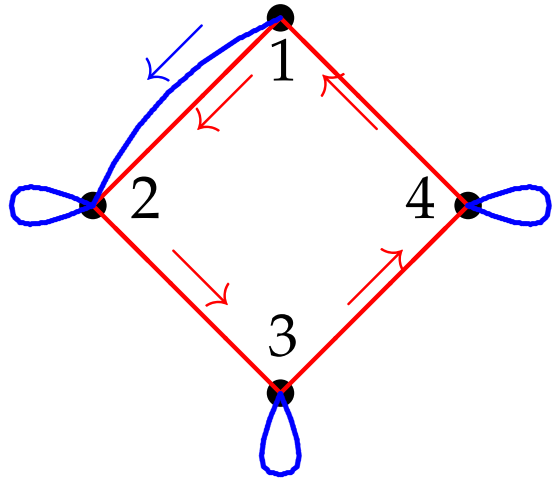
I contend that the last row is in some sense the most meaningful. I would very much like to have a formula for it!

Third conversation: Synchronizing automata

For this, I must turn first to automata and semigroups.
An automaton is a machine which has a set Ω of states, and can read symbols from an alphabet A. It is a very simple machine: all it does at a given time step is to read a symbol and change its state.
An automaton can read a word or sequence of symbols; each symbol causes a state change.
An automaton is synchronizing if there is a word, called a reset word, such that when the automaton reads this word, it ends up in a fixed state, no matter where it starts.
Reset words are useful to bring a machine into a known state before applying further transformations to it.

An infamous problem

Here is a synchronizing automaton.



It can be verified that BRRRBRRRB is a reset word (and indeed that it is the shortest possible reset word for this automaton).

Problem

Show that, if an n-state automaton is synchronizing, it has a reset word of length at most $(n-1)^2$.

This is the Černý conjecture, posed in the 1960s and still open.

Transformation monoids

The Černý conjecture seems to have nothing to do with either graphs or groups; but wait ...
Each letter of the alphabet corresponds to a transition on the set Ω of states. Reading a word corresponds to composing the transitions. So the set of all possible transitions is closed under composition and contains the identity map (corresponding to the empty word): so

> An automaton can be represented as a transformation monoid on the set Ω of states, having a distinguished set of generators.

So the Černý conjecture is a question about transformation monoids.

Graphs

An endomorphism of a graph is a map from the vertex set to itself which carries edges to edges. The action on nonedges is not specified; a nonedge may map to a nonedge, or to an edge, or collapse to a single vertex.
The endomorphisms of a graph form a transformation monoid.
Now we have a pleasant surprise:

Theorem

A transformation monoid M is non-synchronizing if and only if there is a non-trivial graph Γ on the domain such that M is contained in the endomorphism monoid of Γ. Moreover, we can assume that the clique number and chromatic number of Γ are equal.

A graph is trivial if it is complete (all possible edges) or null (no edges at all). The clique number is the number of vertices in the largest complete subgraph, while the chromatic number is the number of colours required to colour the vertices so that adjacent vertices get different colours.

Groups

A permutation group is a transformation monoid in which every element is a bijection. Permutation groups form the oldest part of group theory, going back to the work of Galois or earlier.

A permutation group cannot be synchronizing as a transformation monoid (unless the domain has just one point). So we hijack the word for a different use:

The permutation group G on Ω is synchronizing if, for every non-permutation f of Ω, the transformation monoid $\langle G, f \rangle$ generated by G and f is synchronizing.

Theorem

The permutation group G is non-synchronizing if and only if it is contained in the automorphism group of a non-trivial graph on Ω, which can be taken to have clique number equal to chromatic number.

Which permutation groups are synchronizing?

A long-running project aims to answer this question. Here is a summary of what we know.

A synchronizing permutation group G on Ω must be transitive (no non-trivial subset of Ω is fixed by G) and primitive (no non-trivial partition of Ω is fixed by G).

According to the O'Nan–Scott Theorem, a finite primitive permutation group is of one of four types: affine, wreath product, diagonal, or almost simple.

Wreath products preserve Hamming graphs, coming from the theory of error-correcting codes; they have clique number equal to chromatic number and so are non-synchronizing.

For all the other types, there are both synchronizing and non-synchronizing groups. But recently, using the truth of the Hall–Paige conjecture from the theory of Latin squares, it has been shown that only the easiest type of diagonal group could possibly be synchronizing, essentially those of the form $T \times T$ acting on T by left and right multiplication.

Two historical oddities

The O'Nan–Scott Theorem was proved independently by Michael O'Nan and Leonard Scott in 1979. The Classification of Finite Simple Groups was imminent, and it provides a machine for applying this result to many problems in permutation group theory and beyond. However, much of the theorem was already in Jordan's work from 1872, and had been forgotten.

The Hall–Paige conjecture gives a necessary and sufficient condition for the Cayley table of a finite group (a Latin square) to have an orthogonal mate. The conjecture was made in 1955. In 2009 it was proved: Stewart Wilcox showed how to reduce it to consideration of finite simple groups, and dealt with the groups of Lie type except for the Tits group (the alternating groups having been settled by Hall and Paige); Tony Evans did the Tits group and all the sporadic groups except the fourth Janko group; the last group was settled by John Bray. The first two papers were published in 2009, but Bray's took another eleven years to appear.

Fourth conversation: Graphs on groups

There are several types of graph which "live" on a group, in that their vertex set is the set of group elements, which tells us something about the group.
In all cases, the graph has some symmetries related to the group.
The first type consists of Cayley graphs. A Cayley graph for a group G is a graph on the vertex set G for which right translations $x \mapsto xg$ by group elements $g \in G$ are automorphisms.
I will content myself with a short comment or two ...

Cayley graphs

Cayley graphs form a huge topic. It has been argued that algebraic graph theory is primarily about Cayley graphs for finite groups, and also that geometric group theory is about Cayley graphs for finitely generated infinite groups.
The idea goes back to Arthur Cayley in the 19th century, as does the action of the group on its Cayley graph.

Let G be a group and S a subset of G. Form a directed graph by joining x to y whenever $y = sx$ for some $s \in S$. This is the Cayley graph $\mathrm{Cay}(G, S)$.

The associative law guarantees that G is invariant under right translation by G. ($y = sx \Rightarrow yg = s(xg)$.)

The graph is undirected if and only if $S = S^{-1}$; loopless if and only if $1 \notin S$; and connected if and only if S generates G.

There are many different Cayley graphs for a group G. But, in the case where G is infinite and finitely generated, a Cayley graph $\mathrm{Cay}(G, S)$ for a finite generating set S defines a metric on G, and different generating sets give quasi-isometric metrics, so the geometry imposed on G is more or less independent of the generating set. In particular, concepts such as hyperbolicity don't depend on the generating set.

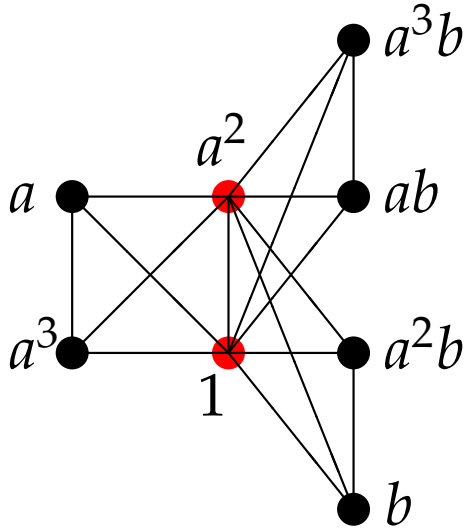
Aut(G)-invariant graphs

I will speak about the other type, which are invariant under the action of the automorphism group of G on G.
The commuting graph of a group G is the graph with vertex set G, in which two vertices x and y are joined if $xy = yx$.
It first appeared in the seminal paper of Brauer and Fowler in 1955, which can be regarded as the first step in the long journey to the Classification of the Finite Simple Groups.
There are two curious things about the Brauer–Fowler paper.

- It is remembered for the theorem that, given a group H with a central involution, there are only finitely many finite simple groups with an involution centralizer isomorphic to H. Brauer and Fowler do not state this explicitly; they simply mention it as an afterthought.
- They do not use the word "graph" anywhere in the paper. But the paper begins with the definition of a metric on a group, which is just the distance in the commuting graph.

An example

Here are the commuting graphs of the two non-abelian groups of order 8: $D_8 = \langle a, b : a^4 = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$ and $Q_8 = \langle a, b : a^4 = 1, b^2 = a^2, b^{-1}ab = a^{-1} \rangle$.



An application

Suppose you have a large unknown group, and you want to find representatives of the conjugacy classes.

In the symmetric group S_n of order $n!$, the n-cycles form a conjugacy class of size $(n-1)!$, so it is easy to find one by choosing, say, n^2 random elements. But the transpositions form a class of size $n(n-1)/2$, and resemble a needle in a haystack.

Take the commuting graph, and put a loop at each vertex. Now a random walk on this graph has limiting distribution which is uniform on conjugacy classes (that is, the probability of being at any element is inversely proportional to its conjugacy class size). This makes small classes findable.

In the example on the last slide, the random walk will spend twice as long on each red vertex as on each of the other vertices.

Persi Diaconis and Maryanthe Malliaris have used this idea to argue that the problem of determining the conjugacy classes in large-dimensional Heisenberg groups over finite fields has no reasonable solution.

Determining the group

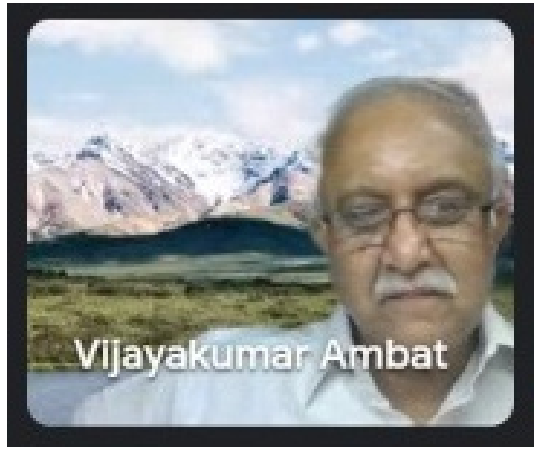
There is a relation called "isoclinism" between groups, invented by Philip Hall, which says roughly that the commutation structure in the two groups is the same.
It is not hard to show that isoclinic groups of the same order have isomorphic commuting graphs. The dihedral and quaternion groups of order 8 provide examples.

Problem

Is the converse true?

A hierarchy

The commuting graph is just one of a number of graphs defined on a group (including the power graph and the non-generating graph) which form a hierarchy.
All these graphs have been studied individually, but we are beginning to look at them as a hierarchy, and study comparative properties, properties of their differences, and so on.
There are other related graphs, such as the Gruenberg–Kegel graph and the intersection graph of non-trivial proper subgroups, which are related to the hierarchy, and are involved in the story.



Ambat Vijayakumar, in Kerala, India, is currently running a research discussion on these graphs, from which I have just come.

There is far more that could be said (including the strange constant 2.6481017597 . . .), but that will suffice for now . . .

. . . for your attention.