The power graph of a group

Peter J. Cameron
Queen Mary, University of London

LTCC Open Day, 8 January 2010

Groups and graphs

A group is an algebraic structure: a set with a binary operation satisfying the associative, identity and inverse laws.

A graph is a combinatorial structure: a set of vertices, some pairs of which are joined by (undirected or directed) edges.

But it is possible for algebra and combinatorics to talk to each other!

Groups and graphs

Groups have a very tight structure; graphs are much looser.

For example, there are only five different groups with eight elements, but there are 12346 different graphs with eight vertices.

Nevertheless, there are very close connections between groups and graphs.

On one hand, any graph has a group of automorphisms; we can study a permutation group G by means of the graphs which it preserves (and G is contained in the automorphism group of any such graph).

For example, several of the sporadic simple groups were constructed as groups of automorphisms of graphs.

Graphs from groups

Here I want to discuss the reverse procedure, starting with a group and constructing a graph. First, a few examples. Let G be a group.

- The *commuting graph* of G, whose vertices are the group elements, two of them joined if they commute.
- The graph whose vertices are the group elements, two of them joined if they generate G.
- The *power graph*, in which two elements are joined if one is a power of the other. This is what I want to talk about today.

Directed and undirected

There are directed and undirected versions of the power graph.

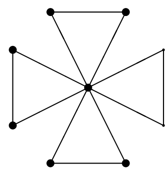
In the directed version $\vec{P}(G)$, we put a directed edge from a to b if b is a power of a.

In the undirected version $P(G)$, we join a and b with an undirected edge if one is a power of the other.

It seems clear that $\vec{P}(G)$ contains much more information than $P(G)$, but neither contains complete information about G.

Examples

- Let G be a finite group in which every element g satisfies $g^3 = 1$. If $|G| = n$, then $P(G)$ consists of $(n-1)/2$ triangles sharing a common vertex (the identity):



The directed version has edges directed inwards to the centre, and the remaining edges directed both ways.

Direct products of cyclic groups of order 3 give examples. But there are non-abelian groups with this property too: for example, the group

$$\left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\}.$$

Examples, continued

- Let p be a prime. The group C_{p^∞} is defined as the quotient $Q_p/\mathbb{Z}$, where Q_p consists of all rational numbers whose whose denominator is a power of p.

  This group has the property that all its proper subgroups are finite cyclic groups: the rationals with denominator dividing p^m, taken mod 1, form a cyclic group of order p^m.

  Thus, given any two elements of the group, one is a power of the other; so $P(C_{p^\infty})$ is an infinite complete graph, irrespective of the prime p. We cannot tell what p is from the undireected power graph.

  However, the directed power graph does give us the value of p.

What the directed power graph tells us

Take the directed power graph of a group G, and make it reflexive by adding a loop at every point.

The relation is now reflexive and transitive, hence a *preorder*.

In any preorder, put $a \equiv b$ if $a \to b$ and $b \to a$. Then $\equiv$ is an equivalence relation; and the equivalence classes are partially ordered by $[b] \leq [a]$ if $a \to b$.

In the case of the directed power graph, $a \equiv b$ if and only if a and b generate the same cyclic subgroup. The minimal element in the partial order is the identity; minimal elements above the identity have prime order (and if the order of a is p, then $|[a]| = p - 1$).

Continuing in this way, we can calculate the numbers of elements of each order in the group.

A surprising theorem

Theorem 1. *Let G_1 and G_2 be finite groups such that $P(G_1)$ and $P(G_2)$ are isomorphic. Then $\vec{P}(G_1)$ and $\vec{P}(G_2)$ are isomorphic.*

In other words, the undirected power graph contains exactly the same information as the directed power graph! This information is not enough to determine the group, as we have seen.

Corollary 2. *Let G_1 and G_2 be finite abelian groups such that $P(G_1)$ and $P(G_2)$ are isomorphic. Then G_1 and G_2 are isomorphic.*

A taste of the proof

Given the undirected power graph, we cannot recover the preorder or the equivalence relation $\equiv$. However, we can "almost" do so.

Here is a taste. Could there be an element (other than the identity) which is joined to all others? If G is cyclic, then any generator has this property; if G is cyclic of prime power order, then every element has this property (and the graph is complete).

We can reduce to the case where $|G|$ is a power of a prime p, and the element a joined to all others has order p. In this case, G has a unique subgroup of order p. A theorem of Burnside now allows us to conclude that G is either cyclic or *generalised quaternion* (with $p = 2$ in the latter case).

Some things we don't know

- Given a (directed or undirected) graph X, how do we tell whether it is the power graph of a group? What is the computational complexity of deciding this?
- What can be said about the number of groups of order n which are not determined by their power graphs, or the maximum number of non-isomorphic groups of order n which have isomorphic power graphs?
- Can "natural" graph-theoretic properties of $P(G)$, such as chromatic number, be related to "natural" group-theoretic properties of G?
- What is special about groups? Does the theorem hold more generally, e.g. for classes of semigroups or loops?
- For infinite groups, what extra information do we need to distinguish, for example, different groups C_{p^∞} with the same power graph?
- What about other graphs defined from groups?