Synchronization and homomorphisms

Peter J. Cameron

Queen Mary University of London

p.j.cameron@qmul.ac.uk

Group Theory, Combinatorics & Computation
Perth, January 2009

This is part of an investigation involving, among others, João Araújo, Πeter Neumann, Jan Saxl, Csaba Schneider, Pablo Spiga, and Ben Steinberg. Nik Ruskuc, Colva Roney-Dougal, Ian Gent and Tom Kelsey have recently been involved. Some of the work also involves Cristy Kazanidis, a student of Cheryl's.

There is far more material than can be presented here; Πeter will talk about other aspects of this topic in his workshop next week. See you there!

Notation

In this talk, X is a graph, G is a group.

For a graph X, we use $\omega(X)$ for the clique number, $\chi(X)$ for the chromatic number, $\overline{X}$ for the complement, $\alpha(X)$ for the independence number (so that $\alpha(X) = \omega(\overline{X})$), and $\mathrm{Aut}(X)$ for the automorphism group of X.

Graph homomorphisms

A *homomorphism* from a graph X to a graph Y is a map from vertices of X to vertices of Y which maps edges to edges. (We don't care what it does to non-edges.)

Write $X \to Y$ if there is a homomorphism, and $X \equiv Y$ if there are homomorphisms in both directions.

We use $\mathrm{End}(X)$ for the monoid of endomorphisms of X (homomorphisms from X to X).

Example:

- $K_m \to X$ if and only if $\omega(X) \geq m$;
- $X \to K_m$ if and only if $\chi(X) \leq m$.

Cores

The *core* of X is the (unique) smallest graph Y such that $Y \equiv X$. It is an induced subgraph (indeed, a retract) of X. (This means that it is the image of an *idempotent* endomorphism of X.)

Note that

- X is equal to its core if and only if all its endomorphisms are automorphisms;
- the core of X is complete if and only if $\omega(X) = \chi(X)$.

Cores and symmetry

Proposition 1. *If X is vertex-transitive, then so is* $\mathrm{core}(X)$. *Similarly for other kinds of transitivity.*

Proof. Let Y be a core of X; we may assume that it is embeddable as an induced subgraph. Let ι be the embedding of Y into X, and ρ a retraction of X onto Y.

Suppose that X is vertex-transitive, and let v and w be vertices of Y. Choose $g \in \mathrm{Aut}(X)$ with $vg = w$. Then $g' = \iota g \rho$ is an endomorphism of Y mapping v to w. Since Y is a core, g' is an automorphism of Y.

Similarly for other kinds of transitivity. □

Complexity

Hell and Nešetřil showed that the problem of deciding whether there is a homomorphism from

X to a fixed graph Y is NP-complete, unless Y has a loop or is bipartite.

Dyer and Greenhill showed that the problem of counting these homomorphisms is #P-complete, again excepting some rather simple graphs Y.

More relevant to us, Hell and Nešetřil showed that the problem of deciding whether a given graph is a core is NP-complete.

Rank 3 graphs

A graph X is a *rank* 3 *graph* if its automorphism group is transitive on vertices, ordered edges and ordered non-edges; in other words, $\mathrm{Aut}(X)$ is a rank 3 permutation group. (The *rank* of a permutation group G on a set V is the number of G-orbits on $V \times V$.)

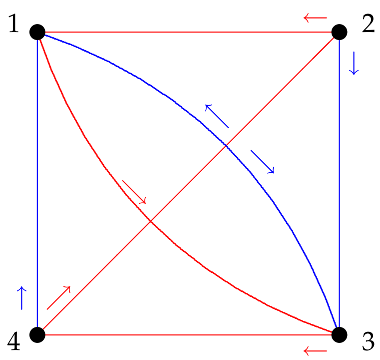
After working out a lot of examples, Cristy Kazanidis and I made the following conjecture:

Conjecture 2. *If X is a rank 3 graph, then either the core of X is complete, or X is a core.*

This is true; the proof came from an unexpected direction: *automata theory*.

The cave

You are in a dungeon consisting of a number of rooms. Passages are marked with coloured arrows. Each room contains a special door; in one room, the door leads to freedom, but in all the others, to instant death. You have a schematic map of the dungeon, but you do not know where you are.



You can check that (Blue, Red, Blue, Blue) is a reset word which takes you to room 3 no matter where you start.

Automata and reset words

An *automaton* is an edge-coloured digraph with one edge of each colour out of each vertex. Vertices are *states*, colours are *transitions*. A *reset word* is a word in the colours such that following edges of these colours from any starting vertex always brings you to the same state. An automaton which possesses a reset word is called *synchronizing*.

Not every finite automaton has a reset word; the *Černý conjecture*, states that, if a reset word exists, then there is one of length at most $(n-1)^2$, where n is the number of states (or rooms in our example).

Algebraically, an automaton is a submonoid of the *full transformation monoid* T_n on $\{1, \ldots, n\}$ with a distinguished set of generators; it is synchronizing if and only if it contains a constant function.

Monoids and graphs

There is a very close connection between transformation monoids and graphs. A graph is *non-trivial* if it is not complete or null.

Theorem 3. *Let M be a submonoid of T_n which is not contained in the symmetric group S_n. Then the following are equivalent:*

- *M is not synchronizing (that is, contains no constant function);*
- *$M \leq \mathrm{End}(X)$, where X is a non-trivial graph which is not a core;*
- *$M \leq \mathrm{End}(X)$, where X is a non-trivial graph whose core is complete.*

Note that the third condition on X is much stronger than the second. We will return to this!

Proof of the theorem

The implications from bottom to top are trivial. We show that the first condition implies the last.

Let M be a submonoid of T_n which is not contained in S_n and contains no constant function. Define a graph X on the vertex set $\{1, \ldots, n\}$ by the rule that $v \sim w$ if and only if there is no $f \in M$ with $vf = wf$.

If $v \sim w$ and $f \in M$, then $vf \neq wf$ by definition. Moreover, if $vf \not\sim wf$ then $(vf)h = (wf)h$

for some h, contradicting the fact that $v \sim w$ (since $fh \in M$). So $M \leq \mathrm{End}(X)$.

Finally, if $f \in M$ has minimum rank, then the image of f carries a complete graph Y (since it cannot be made smaller by any element of M), and so Y is the core of X.

Synchronizing permutation groups

João Araújo and Ben Steinberg proposed a new approach to the Černý conjecture.

A permutation group G on a set V is *synchronizing* if, given any function $f : V \to V$ which is not a permutation, the semigroup generated by G and f contains a constant function.

Theorem 4. *A permutation group G on V is non-synchronizing if and only if there is a non-trivial graph X on V with* $\mathrm{core}(X)$ *complete such that $G \leq \mathrm{Aut}(X)$.*

Proof. In the forward direction, apply the preceding theorem to $M = \langle G, f\rangle$, where f is such that M contains no constant function.

In the reverse direction, if X is non-null, then no endomorphism of it is constant; and if X is not a core, then it has an endomorphism which is not an automorphism. $\square$

Cores revisited

These considerations gave me the idea for the following theorem:

Theorem 5. *Let X be a nonedge-transitive graph. Then either*

- $\mathrm{core}(X)$ *is complete, or*
- *X is a core.*

The hull of a graph

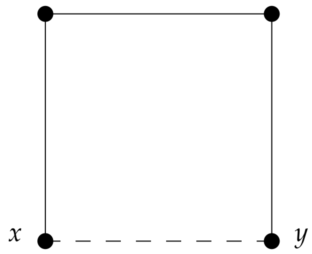
We have seen that we can replace a graph which is not a core by one whose core is complete without losing any endomorphisms. We now formalise this.

The *hull* of a graph X is defined as follows:

- $\mathrm{hull}(X)$ has the same vertex set as X;
- $v \sim w$ in $\mathrm{hull}(X)$ if and only if there is no element $f \in \mathrm{End}(X)$ with $v^f = w^f$.

Theorem 6.
- *X is a spanning subgraph of* $\mathrm{hull}(X)$*;*
- $\mathrm{End}(X) \leq \mathrm{End}(\mathrm{hull}(X))$ *and* $\mathrm{Aut}(X) \leq \mathrm{Aut}(\mathrm{hull}(X))$*;*
- *if* $\mathrm{core}(X)$ *has m vertices then* $\mathrm{core}(\mathrm{hull}(X))$ *is the complete graph on m vertices.*

An example



No homomorphism can identify x and y, so they are joined in the hull.

Note the increase in symmetry: $|\mathrm{Aut}(X)| = 2$ but $|\mathrm{Aut}(\mathrm{hull}(X))| = 8$.

Proof of the theorem

Let X be non-edge transitive. Then $\mathrm{hull}(X)$ consists of X with some orbits on non-edges changed to edges. So there are two possibilities:

- $\mathrm{hull}(X) = X$. Then $\mathrm{core}(X) = \mathrm{core}(\mathrm{hull}(X))$ is complete;
- $\mathrm{hull}(X)$ is the complete graph on the vertex set of X. Then $\mathrm{core}(X)$ has as many vertices as X, so that $\mathrm{core}(X) = X$.

Remark: For any graph X,

- $\mathrm{hull}(X)$ is complete if and only if X is a core;
- if $\mathrm{hull}(X) = X$ then $\mathrm{core}(X)$ is complete (but our example shows that the converse is false).

Questions about hulls

Let $h(X)$ be the smallest number of vertices of a graph containing X as induced subgraph which is a hull.

Theorem 7. $h(X) \in \{\chi(X) - \omega(X), \chi(X) - \omega(X) + 1\}$.

Problem 8. *Given a graph X, what is the complexity of deciding:*

- *Is X a hull?*
- *Is $h(X) = \chi(X) - \omega(X)$?*
- *Is X a hull, given that $\chi(X) = \omega(X)$?*

If the third question is hard, so are the other two.

Note that deciding if $\mathrm{hull}(X)$ is a complete graph is NP-complete (this is equivalent to deciding if X is a core).

Strongly regular graphs

A graph X is *strongly regular*, with parameters k, λ, μ, if

- every vertex has k neighbours;
- two adjacent vertices have λ neighbours;
- two non-adjacent vertices have μ neighbours.

Thus, a rank 3 graph is strongly regular, but the converse is far from true; many strongly regular graphs have no non-trivial automorphisms at all.

Problem 9. *Is it true that, if X is strongly regular, then either the core of X is complete, or X is a core?*

Godsil and Royle have some results on this question.

Homomorphisms revisited

We've seen that, if X is edge-transitive and not a core, then its core is complete, so that among its endomorphisms we have both *automorphisms* (of maximum rank) and *proper colourings* (of minimum rank).

There may be other endomorphisms intermediate between these two extremes. For example, in a complete k-partite graph, with partite sets $B_1, \ldots, B_k$, take any map f_i from B_i to itself for $i = 1, \ldots, k$; combining these will be a homomorphism.

Perhaps in other cases things are more restricted.

Pseudocores

Let us say that a graph X is a *pseudocore* if every endomorphism of X is either an automorphism or a proper colouring (a homomorphism onto a complete graph).

Clearly a pseudocore has the property we showed for nonedge-transitive graphs: either it is a core or its core is complete.

Problem 10. *Let X be a rank* 3 *graph whose automorphism group is primitive (so X is connected and not complete multipartite). Is it true that X is a pseudocore?*

This is true for the triangular graphs $T(n) = L(K_n)$ for $n \geq 5$, for example.

Maybe this is also true for strongly regular graphs which are not complete multipartite ...

Core-transitive graphs

A graph X is *core-transitive* if any isomorphism between cores of X can be extended to an automorphism of X.

This looks like a very strong symmetry condition until you realise that any core is core-transitive. On the other hand, for graphs whose core is complete, it is indeed a strong condition.

So I will state a fairly vague question here:

Problem 11. *What can be said about core-transitive graphs?*

Other classes of permutation groups

We defined the class of *synchronizing* permutation groups earlier, and saw that a synchronizing group is primitive. Further, such a group is *basic*, and so by the O'Nan–Scott theorem, it is affine (with the stabiliser of the origin a primitive linear group), simple diagonal, or almost simple.

Thus, wreath products (in the product action), twisted wreath products, and "compound diagonal" groups cannot be synchronizing.

Not every basic group is synchronizing, however. For example, the symmetric group S_n acting on 2-sets is primitive and basic for $n \geq 5$ but is synchronizing if and only if n is odd.

There is a body of work about which such groups are synchronizing, but we do not have complete answers yet.

Other classes of permutation groups

The connection with automata leads to other interesting classes of permutation groups. For example, a permutation group G on Ω is *QI* if the rational permutation module $\mathbb{Q}\Omega$ is the sum of a 1-dimensional trivial module and an irreducible module. Arnold and Steinberg showed that this condition (which is stronger than synchronizing) suffices to prove the Černý conjecture for automata containing G in their transition monoid.

In fact, a formally weaker condition which we have called *spreading* suffices for this implication. But as yet we have no example of a group which is spreading but not QI.

Πeter Neuman's workshop next week will give more details about this.