# Endomorphisms and synchronization, 2: Graphs and transformation monoids

Peter J. Cameron

BIRS, November 2014

# Relations and algebras

Given a relational structure $R$, there are several similar ways to produce algebraic structures from $R$, including

- the automorphism group $\mathrm{Aut}(R)$;
- the endomorphism monoid $\mathrm{End}(R)$;
- the polymorphism clone $\mathrm{Poly}(R)$.

What about going in the other direction?

# From algebras to relations

There is a generic method of producing a relational structure from a permutation group, transformation semigroup, or function clone: simply take all the invariant relations.
The power of this method for permutation groups was shown by the results obtained by pioneers such as Helmut Wielandt and Donald Higman.
By contrast, I will discuss a very specific method, which

- applies only to endomorphism monoids;
- produces a (simple undirected) graph.

First a very brief introduction to graph homomorphisms.

# Homomorphisms of graphs

A homomorphism from graph $\Gamma_1$ to $\Gamma_2$ is a map from vertices of $\Gamma_1$ to vertices of $\Gamma_2$ which maps edges to edges. Its action on non-edges is unrestricted: a non-edge may map to a non-edge, or to an edge, or may collapse to a single vertex.
The complete graph $K_r$ on $r$ vertices has all possible edges between its vertices.

## Proposition

- *There is a homomorphism from $K_r$ to $\Gamma$ if and only if $\omega(\Gamma) \geq r$, where $\omega$ denotes clique number.*
- *There is a homomorphism from $\Gamma$ to $K_r$ if and only if $\chi(\Gamma) \leq r$, where $\chi$ denotes the chromatic number.*

# Endomorphisms and cores

An endomorphism of $\Gamma$ is a homomorphism from $\Gamma$ to itself.
The core of a graph $\Gamma$ is the smallest graph $\mathrm{Core}(\Gamma)$ having homomorphisms to and from $\Gamma$. It is unique up to isomorphism, and occurs as an induced subgraph of $\Gamma$ (i.e., some of the vertices of $\Gamma$, all edges of $\Gamma$ within its vertex set), and indeed is the image of a retraction of $\Gamma$.

## Proposition

*The following are equivalent:*

- *the core of* $\Gamma$ *is* $K_r$*;*
- $\omega(\Gamma) = \chi(\Gamma) = r$.

# The graph of a transformation monoid

Let $M$ be a transformation monoid on a set $X$. We define a graph $\mathrm{Gr}(M)$ as follows:

- the vertex set of $\mathrm{Gr}(M)$ is $X$;
- vertices $v$ and $w$ are joined by an edge if and only if there is no element $f \in M$ which identifies them ($vf = wf$).

This is not functorial, but at least has one nice property; it is inclusion-reversing:

## Proposition

*If $M_1 \leq M_2$, then $\mathrm{Gr}(M_2)$ is a spanning subgraph of $\mathrm{Gr}(M_1)$.*

(A spanning subgraph of $\Gamma$ uses all the vertices and some of the edges of $\Gamma$.)

# Going both ways

### Proposition

*For any transformation monoid $M$, we have $M \leq \mathrm{End}(\mathrm{Gr}(M))$.*

### Proof.

Let $\{v, w\}$ be an edge of $\mathrm{Gr}(M)$, and take $f \in M$. We must show that $f$ maps $\{v, w\}$ to an edge of $\mathrm{Gr}(M)$. If not, there are two possibilities:

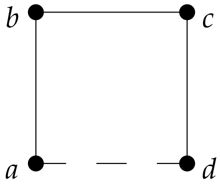
- $vf = wf$: this contradicts the fact that $\{v, w\}$ is an edge of $\mathrm{Gr}(M)$.
- $\{vf, wf\}$ is a non-edge of $\mathrm{Gr}(M)$: then by definition, there exists $g \in M$ such that $(vf)g = (wf)g$. So $v(fg) = w(fg)$ with $fg \in M$, again contradicting the fact that $\{v, w\}$ is an edge of $\mathrm{Gr}(M)$.

□

# Going both ways, 2

Given a graph $\Gamma$, we call $\mathrm{Gr}(\mathrm{End}(\Gamma))$ the hull of $\Gamma$, denoted by $\mathrm{Hull}(\Gamma)$.
Since edges of $\Gamma$ are not collapsed by endomorphisms, they are edges of $\mathrm{Hull}(\Gamma)$. So $\Gamma$ is a spanning subgraph of its hull.
We see that the construction of the hull does not decrease the symmetry of $\Gamma$.

Example




No endomorphism collapses $a$ and $d$, so $ad$ is an edge in the hull.

# And further ...

**Proposition**

$\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(M))) = \mathrm{Gr}(M)$.

**Proof.**

Since $M \leq \mathrm{End}(\mathrm{Gr}(M))$, we see that $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(M)))$ is a spanning subgraph of $\mathrm{Gr}(M)$.
On the other hand, $\mathrm{Gr}(M)$ is a spanning subgraph of its hull, which is $\mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(M)))$. □

So both the operators $M \mapsto \mathrm{End}(\mathrm{Gr}(M))$ on monoids and $\Gamma \mapsto \mathrm{Hull}(\Gamma)$ on graphs are idempotent.

# Cores and hulls

The hull of a graph is, in some sense, a "dual" to the core. $\mathrm{Core}(\Gamma)$ is an induced subgraph of $\Gamma$ (the smallest graph hom-equivalent to $\Gamma$); $\mathrm{Hull}(\Gamma)$ is a graph containing $\Gamma$ as a spanning subgraph.

- The hull of $\Gamma$ is complete if and only if $\Gamma$ is a core.
- If $\Gamma$ is a hull then the core of $\Gamma$ is complete
- … but the converse of this statement is false.
- In particular, $\mathrm{Core}(\mathrm{Hull}(\Gamma))$ is a complete graph on $\mathrm{Core}(\Gamma)$.

# The graph of a monoid

We are particularly interested in using $\mathrm{Gr}(M)$ as a tool to study $M$.

### Proposition

*The minimum rank of an element of $M$, the clique number of $\mathrm{Gr}(M)$, and the chromatic number of $\mathrm{Gr}(M)$ are all equal.*

### Proof.

If $f \in M$ has minimum rank, then no two elements of the image of $f$ can be identified by any element of $M$, so the image of $f$ is a clique in $\mathrm{Gr}(M)$; and then $f$ is a colouring of $\mathrm{Gr}(M)$. □

### Corollary

- $\mathrm{Gr}(M)$ *is complete if and only if $M$ is a permutation group (i.e., contained in the symmetric group).*
- $\mathrm{Gr}(M)$ *is null if and only if $M$ is synchronizing (i.e. contains a transformation of rank $1$).*

# The obstruction to synchronization

### Theorem

*The transformation monoid $M$ on $X$ fails to be synchronizing if and only if there exists a graph $\Gamma$ on the vertex set $X$ with the properties*

- $\Gamma$ *is not the null graph;*
- $\omega(\Gamma) = \chi(\Gamma)$ *(equivalently,* $\mathrm{Core}(\Gamma)$ *is complete);*
- $M \leq \mathrm{End}(\Gamma)$.

### Proof.

$\mathrm{Gr}(M)$ has the second and third properties of the theorem, and is non-null if and only if $M$ is not synchronizing.
Conversely, if $M$ is contained in the endomorphism monoid of a non-null graph, then no edge of the graph is collapsed by $M$, and so $M$ is not synchronizing. □

# Another graph

For a graph $\Gamma$, we define the derived graph $\Gamma'$ to be the spanning subgraph of $\Gamma$ which contains only those edges of $\Gamma$ which are contained in cliques of maximum size $\omega(\Gamma)$.
Now $\omega(\Gamma) = \omega(\Gamma')$ by definition, while $\chi(\Gamma') \leq \chi(\Gamma)$ (since some edges have been deleted).
Thus, if $\omega(\Gamma) = \chi(\Gamma) = r$, then also $\omega(\Gamma') = \chi(\Gamma') = r$.
Moreover, $\mathrm{End}(\Gamma) \leq \mathrm{End}(\Gamma')$, since endomorphisms preserve cliques of maximum size.
Hence $\mathrm{Gr}'(M)$ has the properties required for the theorem on the preceding slide, together with the additional property that every edge is contained in a clique of maximum size.
This extra property is sometimes useful. An application follows.

# Maximal non-synchronizing monoids

### Theorem

*Let $M$ be a transformation monoid on $n$ points which is maximal with respect to being non-synchronizing. Then there are graphs $\Gamma$ and $\Delta$ such that*

- $\mathrm{End}(\Gamma) = \mathrm{End}(\Delta) = M$;
- $\omega(\Gamma) = \omega(\Delta) = \chi(\Gamma) = \chi(\Delta)$;
- $\Gamma = \mathrm{Hull}(\Delta)$ *and* $\Delta = \Gamma'$.

### Theorem

*Let $\Gamma$ be a non-null graph satisfying $\Gamma = \mathrm{Hull}(\Gamma) = \Gamma'$. Then $\mathrm{End}(\Gamma)$ is a maximal non-synchronizing transformation monoid.*

### Problem

*Find a necessary and sufficient condition!*

# Permutation groups

For the next part of the lecture, we need to revise some properties of permutation groups. A permutation group on $X$ is a subgroup of the symmetric group on $X$.

Note that the theory of finite permutation groups, the oldest part of group theory, has been revolutionised by the classification of finite simple groups. I will have more to say about this later.

# Properties of permutation groups

In order to define the next few properties, we say that a structure of some kind on $X$ is trivial if it is invariant under the symmetric group on $X$, and non-trivial otherwise.
Now a permutation group $G$ on $X$ is

- transitive if it preserves no non-trivial subset of $X$;
- primitive if it preserves no non-trivial partition of $X$;
- basic if it preserves no non-trivial Cartesian power structure on $X$;
- 2-homogeneous if it preserves no non-trivial graph on $X$;
- 2-transitive if it preserves no non-trivial binary relation on $X$.

If you know other definitions of these concepts you should have no trouble matching them up with the ones given here.

# Synchronizing groups

A permutation group $G$ is said to synchronize a map $f$ if the monoid $\langle G, f \rangle$ is synchronizing.
The following theorem is due to Rystsov:

**Theorem**

*A permutation group $G$ on $n$ points is primitive if and only if it synchronizes every map of rank $n-1$.*

**Proof.**

$\Leftarrow$: If $G$ preserves a non-trivial equivalence relation $\equiv$, and $v \equiv w$, then the map sending $v$ to $w$ and fixing all other points is not synchronized by $G$. $\square$

Proof.

$\Rightarrow$: Conversely, suppose that $M = \langle G, f \rangle$ is not synchronizing, where $f$ has rank $n-1$, and let $\Gamma = \mathrm{Gr}(M)$. Suppose that $v$ and $w$ have the same image under $f$. Then $v$ and $w$ are not joined in $\Gamma$. So the neighbours of $v$ and of $w$ are both mapped bijectively to the neighbours of $vf = wf$ by $f$, and thus these neighbour sets are equal. Putting $x \equiv y$ if $x$ and $y$ have the same neighbour sets, we obtain a non-trivial $G$-invariant equivalence relation, so $G$ is imprimitive. □

# A note on primitivity

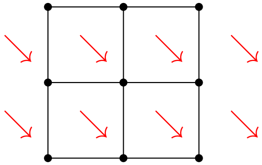
We saw that primitivity, as I defined it earlier, is exactly equivalent to synchronizing every map of rank $n - 1$. However, there is one small awkwardness. According to this definition, the trivial group acting on a set of cardinality 2 is primitive, even though it is not transitive!
It is usual to exclude this exceptional case, and to re-define primitivity in such a way that a primitive group is transitive. If this is done (as I shall assume in future), then we must add to Rystsov's Theorem the assumption that $n > 2$.

# Primitivity and synchronization

We say that a permutation group $G$ is synchronizing if it synchronizes every non-permutation. By Rystsov's Theorem, a synchronizing group of degree greater than 2 is primitive. Does the converse hold?

The answer is no. The picture shows the $3 \times 3$ grid, whose automorphism group is the primitive group $G = S_3 \wr S_2$. (Vertices in the same row or the same column are joined.)

The map taking each vertex to the vertex in the bottom row obtained by moving south-east (wrapping round if necessary) is a graph endomorphism and so is not synchronized by $G$.



# Testing synchronization

Many permutation group properties can be tested efficiently (in polynomial time); these include transitivity, primitivity, and 2-homogeneity.

This is not known for synchronization, which seems more difficult.

Here is an algorithm for a permutation group $G$, which is not too far from state-of-the-art.

- Compute all the non-trivial $G$-invariant graphs.
- For each graph in the list, test whether its clique number and chromatic number are equal.
- If the answer is ever "yes", then $G$ is non-synchronizing; otherwise it is synchronizing.

This seems like a very inefficient algorithm:

- If $G$ has $m$ orbits on the set of 2-sets, then there are $2^m - 2$ non-trivial $G$-invariant graphs: all unions of orbits except for the complete and null graphs.
- Clique number and chromatic number are both NP-hard properties of graphs.

However, the algorithm is often better than it seems, and has been used to test the synchronizing property for groups with degrees up to several thousand.

1. Although the number of orbits on 2-sets can be linear in $n$, and so the number of graphs to be checked can be exponential, for many families of graphs these numbers are bounded. For example, if a permutation group $G$ has just two orbits on unordered pairs of elements of the domain, then just one complementary pair of graphs has to be tested.

2. Although both problems are NP-hard, in practice the clique number is much easier to compute than the chromatic number (and indeed parametrised complexity theory gives an explanation of this), and often synchronization can be proved with just clique nunber calculations.

# Non-basic groups

Recall that a permutation group is non-basic if it preserves a Cartesian power structure (aka Hamming scheme) on the point set, and is basic if it preserves no such structure.

The $k$-dimensional cube graph over an alphabet of size $m$ (with $n = m^k$ vertices) has endomorphisms onto the $l$-dimensional subcube for $1 \leq l \leq k$, with image of size $m^l$ and kernel classes of size $m^{k-l}$.

Observing that the example on the last slide is non-basic, we might wonder whether basic primitive groups are necessarily synchronizing.

# Basic groups

This also is false: there are various known families of graphs whose with clique number equal to chromatic number, whose automorphism groups are basic primitive groups. For example:

- The line graph of the complete graph $K_m$ has clique number $m - 1$, and chromatic number $m - 1$ if $m$ is even. Its automorphism group is the symmetric group $S_n$ (acting on 2-sets).
- A classical polar space defines two graphs, where the adjacency relation is orthogonality or non-orthogonality respectively. The first has $\omega = \chi$ if and only if the polar space has a partition into ovoids, and the second if and only if the polar space has both an ovoid and a spread. The automorphism group is the corresponding classical group.

# The O'Nan–Scott Theorem

One part of the O'Nan–Scott Theorem says that basic primitive groups are of three types:

- affine, generated by the translations of a finite vector space and an irreducible group of linear transformations;
- diagonal, which I will not describe here;
- almost simple, groups for which the unique minimal normal subgroup is simple (but the action is not specified.

The two examples on the preceding slide are almost simple.
Examples of other types also occur.
So far, we are some way from a classification of the synchronizing groups which are basic primitive groups.

# Uniform endomorphisms

Recall that a map $f$ is uniform if the kernel classes of $f$ all have the same size.

## Proposition

*If a vertex-transitive graph has clique number equal to chromatic number, then the colouring endomorphisms are uniform.*

## Proof.

Let $A$ be a maximum clique, and $B$ a colour class in a minimum colouring. Then $Ag \cap B \neq \emptyset$ for all automorphisms $g$. But this inequality for all elements of a transitive group implies that $|A| \cdot |B| = n$, the number of vertices. So $|B|$ is independent of the chosen colour class. □

Many other examples of uniform endomorphisms can be constructed, such as the endomorphisms of the $k$-dimensional cube graph mentioned earlier.

# Araújo's conjecture

These considerations lead João Araújo to the following

## Conjecture

*A primitive permutation group synchronizes every non-uniform map.*

Various special cases of the conjecture were proved.
However, last month the first counterexample appeared, and now we have an extremely interesting list of non-uniform maps synchronized by primitive groups. We'll see them in the final lecture …