Testing synchronization

Peter J. Cameron

University of St Andrews

Computational Algbra
CAUL, Lisboa, July 2014

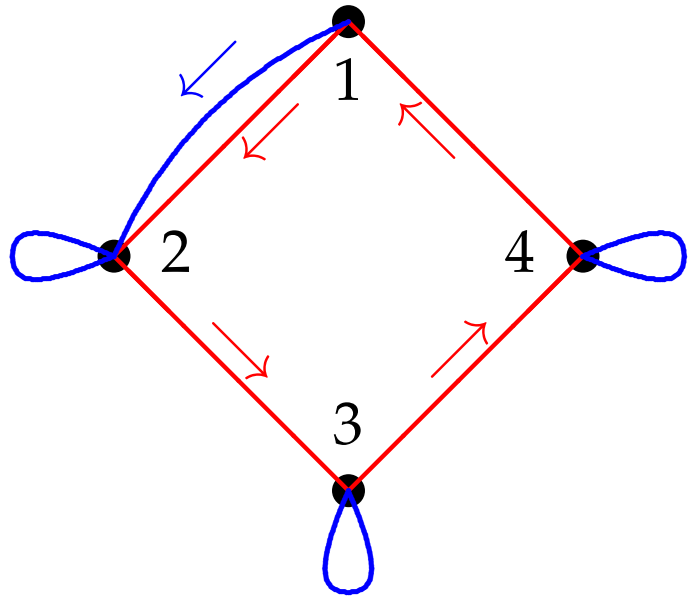
Synchronization

It is easy to test whether a finite-state automaton is synchronizing. However, it appears to be very difficult to tell whether a permutation group is synchronizing; this question includes some hard problems in extremal combinatorics and finite geometry as special cases.
In this talk I will outline the problem and speculate on some approaches which might help.

Definitions

A (finite deterministic) automaton consists of a finite set Ω of states, with a finite set S of transitions, maps from Ω to Ω.
The automaton is synchronizing if there is a word in the transitions (called a reset word) which evaluates to a map of rank 1.
Combinatorially, an automaton is an edge-coloured directed graph on Ω such that every vertex is the source of a unique arc of each colour.
Algebraically, since we are interested in composing maps, an automaton is a transformation semigroup on Ω (a set of transformations closed under composition) with a prescribed set S of generators.

An example



	B	R	R	R	B	R	R	R	B
1	2	3	4	1	2	3	4	1	2
2	2	3	4	1	2	3	4	1	2
3	3	4	1	2	2	3	4	1	2
4	4	1	2	3	3	4	1	2	2

So BRRRBRRRB is a reset word.

Testing synchronization

Proposition

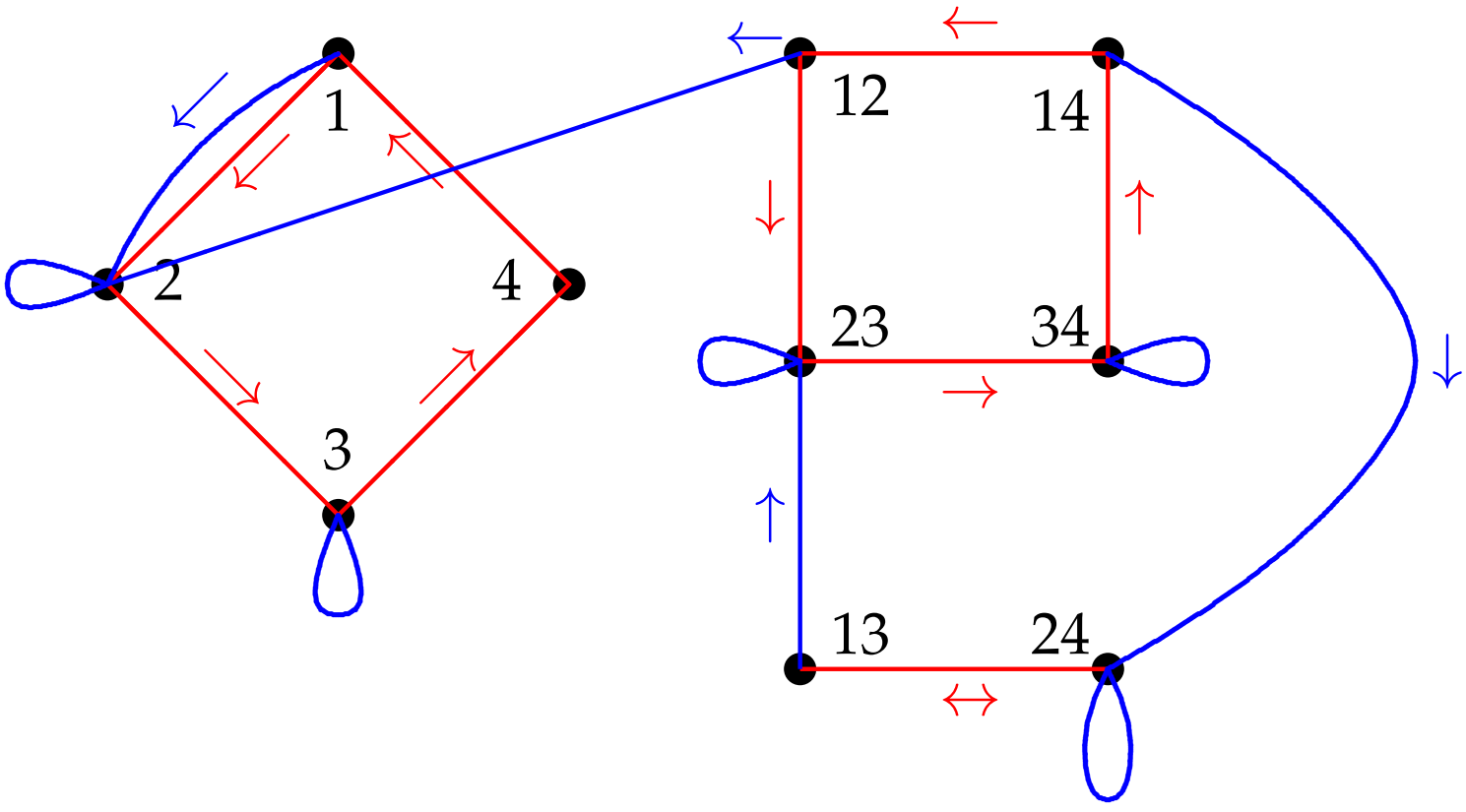
An automaton (Ω, S) is synchronizing if and only if, for any two states $a, b \in \Omega$, there is a word $w_{a,b}$ in the elements of S which maps a and b to the same place.

Proof.

"Only if" is clear, so suppose that the condition holds. Let f be an element of $\langle S \rangle$ of smallest possible rank. If the rank of f is greater than 1, then choose two points a, b in the image; then fw_{ab} has smaller rank than f. So f has rank 1, and the automaton is synchronizing. □

So we only have to consider all pairs of states.

The picture shows the previous example, extended to pairs of states.



Now it suffices to check that there is a path from any vertex on the right to some vertex on the left; this can clearly be done in polynomial time.

Graph homomorphisms

Let Γ and Δ be graphs. A homomorphism from Γ to Δ is a map from the vertex set of Γ to that of Δ which maps edges to edges. (We don't care what happens to non-edges; a non-edge may map to a non-edge, or to an edge, or collapse to a single vertex.) K_r denotes the complete graph on r vertices (with all possible edges).

Proposition

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

Thus a graph Γ has homomorphisms to and from K_r if and only if $\omega(\Gamma) = \chi(\Gamma) = r$.

Graph endomorphisms

An endomorphism of a graph is a homomorphism from the graph to itself. The endomorphisms of Γ form a monoid (semigroup with identity) denoted by $\mathrm{End}(\Gamma)$.
There is a very close connection between transformation semigroups and graphs. The map $\Gamma \mapsto \mathrm{End}(\Gamma)$ takes any graph to a semigroup. We now define a map in the other direction. Given a transformation semigroup S on a set V, we define a graph $\mathrm{Gr}(S)$ on V by the rule that $v \sim w$ if and only if there is no element $f \in S$ for which $vf = wf$.
Note that, if $S \leq T$, then $\mathrm{Gr}(S)$ contains $\mathrm{Gr}(T)$ as a spanning subgraph; the map Gr is "inclusion-reversing". (The map End is not; we do not have a Galois correspondence here.)

Graphs and transformation semigroups

These correspondences have several further properties.

Theorem

Let S be a transformation semigroup on V.

- $S \leq \mathrm{End}(\mathrm{Gr}(S))$, *and* $\mathrm{Gr}(S) = \mathrm{Gr}(\mathrm{End}(\mathrm{Gr}(S)))$.
- *The three numbers $\omega(\mathrm{Gr}(S))$, $\chi(\mathrm{Gr}(S))$, and the minimal rank of an element of S are equal.*
- *S is non-synchronizing if and only if there exists a non-null graph Γ on the vertex set V with $S \leq \mathrm{End}(\Gamma)$; the graph Γ can be assumed to further satisfy $\omega(\Gamma) = \chi(\Gamma)$.*
- $\mathrm{Gr}(S)$ *is the null graph if and only if S is synchronizing, and is the complete graph if and only if $S \leq \mathrm{Sym}(V)$.*

Synchronizing groups

The notion of a "synchronizing permutation group" is due to João Araújo and Benjamin Steinberg.

Let G be a permutation group on V. By abuse of language, we say that G is synchronizing if the semigroup $\langle G, f \rangle$ generated by G and f is synchronizing for any non-permutation f of V.
The notion has led to a very rich theory and raised some very difficult computational questions about permutation groups, some of which I will describe below.
The take-home message is that testing the synchronizing property of a permutation group appears to be much harder than other natural properties such as transitivity and primitivity, and for specific classes of groups leads to very hard problems in extremal combinatorics, finite geometry, etc.

How to recognise synchronizing groups

I will say that a subset, partition, graph, etc., on the set V is trivial if it is invariant under the symmetric group on V, and non-trivial otherwise. Thus, the trivial graphs are the complete and null graphs.

Theorem

A permutation group G on V is non-synchronizing if and only if there is a non-trivial graph Γ on V with $\omega(\Gamma) = \chi(\Gamma)$ and $G \leq \mathrm{Aut}(\Gamma)$.

Proof.

In one direction, if $\langle G, f\rangle$ is not synchronizing, set $\Gamma = \mathrm{Gr}(\langle G, f\rangle)$; then $\langle G, f\rangle \leq \mathrm{End}(\Gamma)$, so $G \leq \mathrm{Aut}(\Gamma)$.
In the other direction, if a graph Γ with the stated properties exists, choose f to be an endomorphism of Γ whose image is a maximal clique; then $\langle G, f\rangle \leq \mathrm{End}(\Gamma)$, so $\langle G, f\rangle$ is not synchronizing. □

Primitive and basic groups

A permutation group G on V is said to be

- transitive if it preserves no non-trivial subset of V;
- primitive if it is transitive and preserves no non-trivial partition of V;
- basic if it is primitive and preserves no non-trivial Hamming scheme (Cartesian product structure) on V;
- 2-transitive if it preserves no non-trivial binary relation on V (and $|V| \geq 2$).

All these properties of a permutation group can be tested in polynomial time.

Synchronizing groups are basic

Theorem

- *A synchronizing group is primitive.*
- *A synchronizing group is basic.*
- *A 2-transitive group is synchronizing.*

To prove this, observe that an imprimitive group preserves a complete multipartite graph, while a non-basic group preserves a Hamming graph, and these graphs have clique number equal to chromatic number. On the other hand, a 2-transitive group preserves no non-trivial graph.

O'Nan–Scott and CFSG

According to the O'Nan–Scott Theorem, a basic group is of one of three types:

- affine: generated by the translations of a finite vector space V and a primitive group of linear transformations of V;
- diagonal: harder to describe, but the prototype is the group $S \times S$ acting on S by left and right multiplication (the multiplication group of S, regarding S as a loop), where S is non-abelian simple;
- almost simple, that is, lying between a simple group and its automorphism group.

The Classification of Finite Simple Groups tells us a lot about all these types (in the affine case, it helps us understand the primitive linear groups). It was hoped that this might lead to a classification of synchronizing groups. But things are not so easy ...

An example

Let G be the symmetric group S_m of degree m in its induced action on the 2-element subsets of $\{1, \ldots, m\}$, with $n = m(m-1)/2$. This group is primitive (and basic) if $m \geq 5$. It is a rank 3 group, and so there are just two G-invariant graphs:

- The triangular graph $T(m)$, the line graph of K_m. This graph has clique number $m-1$ (a maximal clique consisting of all pairs containing a fixed element of $\{1, \ldots, m\}$), and chromatic number $m-1$ if m is even, m if m is odd. (If m is odd, the elements of a colour class are pairwise disjoint, so there are at most $\lfloor m/2 \rfloor$ of them.)
- The complement of $T(m)$ is the Kneser graph. Its clique number is $\lfloor m/2 \rfloor$, as above, but by a theorem of Lovász its chromatic number is $m-2$.

So G is synchronizing if and only if m is odd.

Classical groups

In many cases, testing a family of primitive basic groups for the synchronizing property leads to intractible combinatorial problems. Here is one class of examples. Apologies to those not very familiar with the terminology.

Let G be a finite classical group (symplectic, orthogonal, or unitary), acting on its associated polar space. There are just two non-trivial G invariant graphs: the orthogonality graph and its complement. So we have to decide whether these graphs can have clique number equal to chromatic number.

A maximal clique in the collinearity graph is a maximal totally isotropic (or totally singular) subspace.
The largest possible size of a clique in the non-collinearity graph corresponds to an ovoid (a set meeting every maximal subspace in a point).
So G is non-synchronizing if and only if *either*

- the polar space contains an ovoid and a spread (a collection which partitions the point set) of maximal subspaces; *or*
- the polar space has a partition into ovoids.

Despite decades of work by finite geometers, we still do not have a complete list of which classical polar spaces have either of the structures described. Can the new techniques for deciding if strongly regular graphs are cores resolve this?

Other types of groups

Other types of basic primitive groups such as affine and diagonal groups raise further interesting problems.
For just one example, let S be a simple group, and $G = S \times S$ acting on S, where the factors act by left and right multiplication. The G-invariant graphs are the normal Cayley graphs for S (the Cayley graphs whose connection sets are invariant under conjugation), and cliques and colourings correspond to subgroups of S meeting a restricted set of conjugacy classes. So G fails to be synchronizing if it has a factorization $G = AB$, where $A \cap B = \{1\}$, and A and B meet disjoint collections of conjugacy classes.

Testing synchronization

As we saw, the property of being synchronizing is stronger than those of being transitive, primitive or basic, and weaker than 2-transitivity. In contrast to these, we do not have an efficient test. The best we can do to test a given group G is

- construct all non-trivial G-invariant graphs (there are $2^r - 2$ of these, where r is the number of G-orbits on 2-sets);
- test each of these graphs Γ to find whether its clique number and chromatic number are equal.

This involves exponentially many NP-hard problems! But the graphs are rather special, since they admit basic primitive groups. Permutation groups with degrees in the thousands have been tested by this method.

Other ideas

Testing synchronization of a given semigroup is easy, as we saw; but there are far too many maps f for testing $\langle G, f \rangle$ to be feasible.

Once we have constructed the graphs, could we short-cut finding the clique and chromatic numbers by finding their endomorphism semigroups by some `nauty`-like program? The complexity of finding graph automorphism groups is not known, but the complexity of finding endomorphism semigroups is, unfortunately, known to be NP-hard.

In recent times a number of graph parameters which lie between clique number and chromatic number (and which may be easier to compute) have been studied. The most famous of these is the Lovász parameter $\vartheta(\Gamma)$, related to Shannon capacity; other invariants are due to Schrijver and Szegedy, and there is vector chromatic number, quantum chromatic number, ...

These may be useful in proving synchronization in some cases! Of course, it must be remembered that, even if the problems are hard, the graphs with which we have to work are far from typical, having primitive (and even basic) automorphism groups.

We might also hope to learn more about graphs admitting automorphism groups which are primitive on the vertices, in particular, such graphs which have clique number equal to chromatic number.

Synchronizing non-uniform maps

I conclude with two important open problems. In each case the problem suggests that, while there are primitive non-synchronizing groups, primitivity is in some sense the important watershed.

The first is due to João Araújo. A transformation of V is called non-uniform if not all inverse images of points in its image have the same cardinality. Also, we say that the permutation G synchronizes the map f if $\langle G, f \rangle$ is synchronizing.

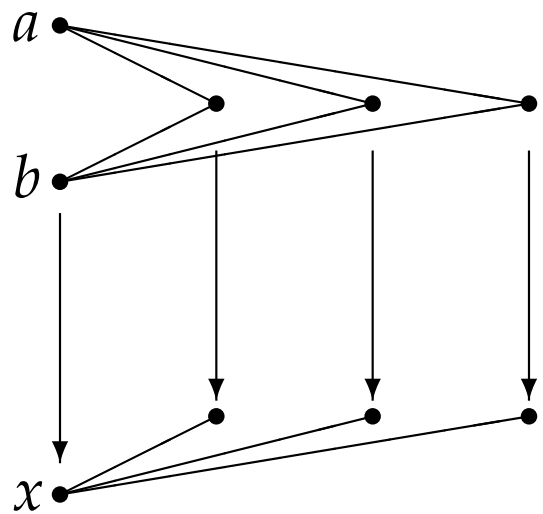
Conjecture

Let G be a primitive permutation group. Then G synchronizes every non-uniform map.

The first case is a theorem of Rystsov, which asserts that a permutation group of degree n is primitive if and only if it synchronizes every map of rank $n-1$. This is easily deduced by graph-theoretic methods: see next slide.

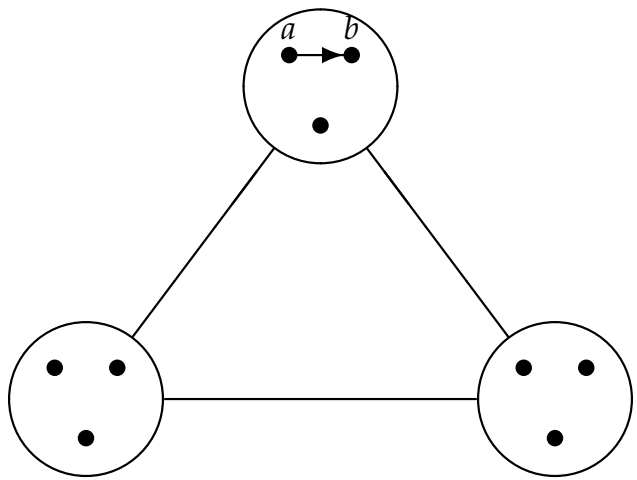
Rystsov's Theorem

Suppose that G is primitive but fails to synchronize some map f of rank $n-1$. Then there is a graph Γ (with clique number and chromatic number equal) with $\langle G, f \rangle \leq \mathrm{End}(\Gamma)$.



Suppose that a and b are mapped to x by f; the remaining points are mapped bijectively. So the neighbours of a are mapped bijectively to the neighbours of x, and so are the neighbours of b. So a and b have the same neighbours, and the relation "same neighbours" is an equivalence relation preserved by G, contradicting primitivity.

Conversely, suppose that G is imprimitive. Then G preserves a complete multipartite graph Γ whose parts are the blocks of imprimitivity.
Choose f to map a to b, where a and b are two points in the same multipartite block, and to fix everything else.



Then $f \in \mathrm{End}(\Gamma)$, so f is a rank 1 map not synchronized by G.

Pushing further

João Araújo, Wolfram Bentz, and I have managed to prove the conjecture for maps of rank very close to n, and also for small ranks.

In some cases one can do better. For example, my student Artur Schaefer has shown that, if G is a primitive permutation group of rank 3 (this means that G has just three orbits on pairs of points, so there is just one complementary pair of non-trivial G-invariant graphs), then G synchronizes any non-uniform map of rank at least roughly $n - \sqrt{n}$.

But for the general case we need a new idea!

Non-synchronizing ranks

Let G be a permutation group of degree n. A number r with $2 \leq r \leq n-1$ is an non-synchronizing rank of G if there is a map of rank r not synchronized by G.

Proposition

An imprimitive group of degree n has at least $(\frac{3}{4} - o(1))n$ non-synchronizing ranks.

Conjecture

A primitive group of degree n has at most $O(\log n)$ non-synchronizing ranks, while a basic group has at most $O(\log \log n)$ non-synchronizing ranks.

The automorphism group of the Hamming scheme $H(r, m)$, namely $S_m \wr S_r$, has non-synchronizing ranks m^i for $i = 1, 2, \ldots, r-1$, and probably no others (work of Artur Schaefer).