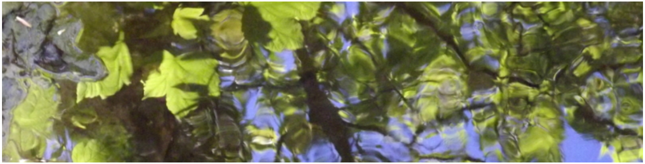
Permutation Groups and Transformation Semigroups
Lecture 2: Synchronization

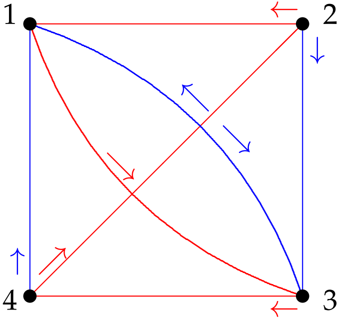
Peter J. Cameron
University of St Andrews



Shanghai Jiao Tong University
November 2017

The dungeon

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 death. You have a map of the dungeon, but you do not know where you are.



You can check that (Blue, Red, Blue) takes you to room 1 no matter where you start.

Automata

The diagram on the last page shows a finite-state deterministic automaton. This is a machine with a finite set of states, and a finite set of transitions, each transition being a map from the set of states to itself. The machine starts in an arbitrary state, and reads a word over an alphabet consisting of labels for the transitions (Red and Blue in the example); each time it reads a letter, it undergoes the corresponding transition.

A reset word is a word with the property that, if the automaton reads this word, it arrives at the same state, independent of its start state. An automaton which possesses a reset word is called synchronizing.

Not every finite automaton has a reset word. For example, if every transition is a permutation, then every word in the transitions evaluates to a permutation. How do we recognise when an automaton is synchronizing?

Automata and transformation semigroups

Combinatorially, an automaton is an edge-coloured digraph with one edge of each colour out of each vertex. Vertices are states, colours are transitions.

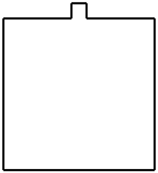
Algebraically, if $\Omega = \{1, \ldots, n\}$ is the set of states, then any transition is a map from Ω to itself. Reading a word composes the corresponding maps, so the set of maps corresponding to all words is a transformation semigroup on Ω.

So an automaton is a transformation semigroup with a distinguished generating set.

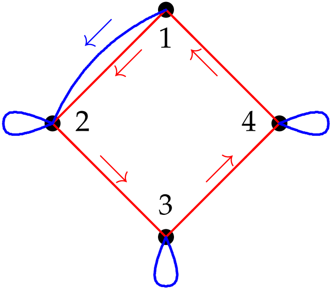
Industrial robotics

In a factory, parts are delivered by conveyor belt to a robot for assembly. Each part must be put on in the correct orientation. Assuming they arrive in random orientation, this is a job for a synchronizing automaton.

Suppose that the pieces are square, with a small projection on one side:



Suppose the conveyor has a square tray in which the pieces can lie in any orientation. Simple gadgets can be devised so that the first gadget rotates the square through 90° anticlockwise; the second rotates it only if it detects that the projection is pointing towards the top. The set-up can be represented by an automaton with four states and two transitions, see next slide.



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

The Černý conjecture

This is a special case of the Černý conjecture, made about fifty years ago and still open:

> *If an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.*

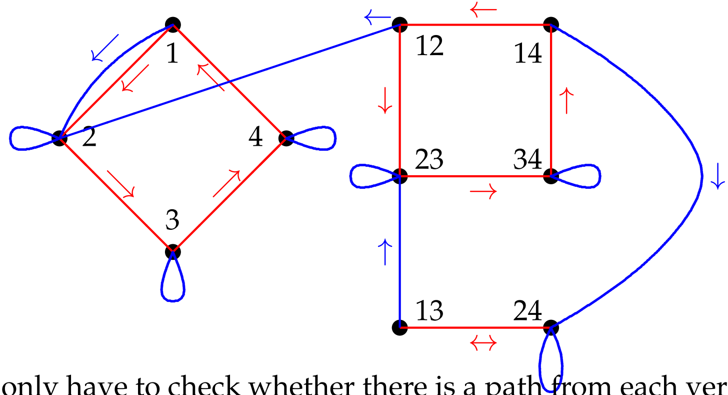
The above example and the obvious generalisation show that the conjecture, if true, is best possible.
The Černý conjecture has been proved in some cases, but the best general upper bound known is $O(n^3)$, due to Pin. Here is a proof of an $O(n^3)$ bound, which does not get the best constant, but illustrates a simple but important principle.

Proposition

An automaton is synchronizing if and only if, for any two states a, b, there is a word in the transitions which takes the automaton to the same place starting from either a or b.

A bound

Now to obtain our bound, consider the diagram of the automaton extended to include pairs of states.



We only have to check whether there is a path from each vertex on the right (a pair of states) to a vertex on the left (a single state). Such a path (if it exists) has length $O(n^2)$, and we only require $n-1$ "collapses" of pairs to synchronize.

Graph endomorphisms

Our graphs are simple (no directions, loops, or multiple edges).
The clique number $\omega(\Gamma)$ of a graph Γ is the number of vertices in its largest complete subgraph, and the chromatic number $\chi(\Gamma)$ is the smallest number of colours required for a vertex-colouring so that adjacent vertices get different colours.
Let Γ and Δ be graphs. A homomorphism from Γ to Δ is a map f from the vertex set of Γ to that of Δ with the property that, for any edge $\{v, w\}$ of Γ, the image $\{vf, wf\}$ is an edge of Δ.
An endomorphism of Γ is a homomorphism from Γ to itself.

Proposition

- *A homomorphism from K_m to Γ is an embedding of K_m into Γ; such a homomorphism exists if and only if $\omega(\Gamma) \geq m$.*
- *A homomorphism from Γ to K_m is a proper colouring of Γ with m colours; such a homomorphism exists if and only if $\chi(\Gamma) \leq m$.*
- *There are homomorphisms in both directions between Γ and K_m if and only if $\omega(\Gamma) = \chi(\Gamma) = m$.*

The obstruction to synchronization

The endomorphisms of a graph Γ form a transformation semigroup; if Γ is not a null graph, then $\mathrm{End}(\Gamma)$ is not synchronizing, since edges cannot be collapsed.

Theorem

Let S be a transformation monoid on Ω. Then S fails to be synchronizing if and only if there exists a non-null graph Γ on the vertex set Ω for which $S \leq \mathrm{End}(\Gamma)$. Moreover, we may assume that $\omega(\Gamma) = \chi(\Gamma)$.

Proof.

Given a transformation monoid S, we define a graph $\mathrm{Gr}(S)$ in which x and y are joined if and only if there is no element $s \in S$ with $xs = ys$. Show that $S \leq \mathrm{End}(\mathrm{Gr}(S))$, that $\mathrm{Gr}(S)$ has equal clique and chromatic number, and that S is synchronizing if and only if $\mathrm{Gr}(S)$ is null. □

Synchronizing groups

A permutation group is never synchronizing as a monoid, since no collapses at all occur.
We abuse language by making the following definition. A permutation group G on Ω is synchronizing if, for any map f on Ω which is not a permutation, the monoid $\langle G, f \rangle$ generated by G and f is synchronizing.

Theorem

A permutation group G on Ω is non-synchronizing if and only if there exists a G-invariant graph Γ, not complete or null, which has clique number equal to chromatic number.

The definition of synchronizing fits our paradigm for permutation group properties: G is synchronizing if and only if it preserves no non-trivial graph with equal clique and chromatic numbers.

Synchronization in the hierarchy

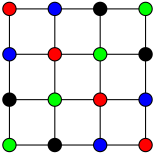
Theorem

Let G be a permutation group of degree $n > 2$.

- *If G is synchronizing, then it is transitive, primitive, and basic.*
- *If G is 2-homogeneous, then it is synchronizing.*

Proof.

If G fails to be transitive, primitive or basic, then it preserves a non-trivial graph with clique number equal to chromatic number (a Hamming graph in the non-basic case, see below). If G is 2-homogeneous it preserves no non-trivial graphs. □



An example

Let G be the group of degree $n = \binom{m}{2}$ induced by S_m acting on the 2-subsets of $\{1, \ldots, m\}$. Then G is primitive and basic, and not 2-homogeneous, for $m > 4$.

There are two non-trivial G-invariant graphs: the graph where two pairs are joined if they intersect (aka the triangular graph $T(m)$, or the line graph of K_m) and the graph where two pairs are joined if they are disjoint (the Kneser graph $K(m, 2)$). These are the two graphs in the triangular association scheme.

- $T(n)$ has clique number $m - 1$, a maximum clique consisting of all the pairs containing a fixed point. Its chromatic number is $m - 1$ if m is even, and m if m is odd.
- $K(m, 2)$ has clique number $\lfloor m/2 \rfloor$, and has chromatic number $m - 2$ by a theorem of Lovász.

Theorem

For $m \geq 5$, S_m acting on 2-sets is synchronizing if and only if m is odd.

Cores and pseudocores

A graph Γ is a core if all its endomorphisms are automorphisms.

It follows from the result above that a permutation group G is synchronizing if and only if every non-trivial G-invariant graph is a core.

A weaker notion is that of a pseudocore. A graph Γ is a pseudocore if every endomorphism is either an automorphism or a colouring (a map whose image is a clique and whose kernel is a proper colouring of Γ).

A graph Γ is strongly regular if there are numbers k, λ, μ such that the number of common neighbours of vertices v, w is k¡ λ or μ according as v and w are equal, adjacent, or non-adjacent.

David Roberson proved the following theorem:

Theorem

Every strongly regular graph (except the disjoint union of complete graphs and its complement) is a pseudocore.

Almost synchronizing groups

Suppose that the vertex-transitive graph Γ has clique number and chromatic number m. Then every proper m-colouring of Γ has all colour classes of the same size. (The proof is an exercise.)

A map f is uniform if all its kernel classes have the same size. We say that a permutation group G is almost synchronizing if, for any non-uniform map f, the semigroup $\langle G, f \rangle$ is synchronizing. Now from Roberson's theorem, we get the following, where the permutation rank of a permutation group G on Ω is the number of G-orbits on Ω^2 (so the groups of permutation rank 3 which have even order are automorphism groups of strongly regular graphs):

Theorem

A primitive permutation group of permutation rank 3 is almost synchronizing.

Not every primitive group is almost synchronizing. The smallest example is on 45 points, and was discovered by Araújo, Bentz, Cameron, Royle and Schaefer.

Non-synchronizing ranks

An integer m is a non-synchronizing rank for the permutation group G on Ω if there is a map f of rank m such that $\langle G, f \rangle$ is non-synchronizing.
It is not difficult to show that a transitive imprimitive permutation group of degree n has at least $(\frac{3}{4} - o(1))n$ non-synchronizing ranks.

Conjecture

A primitive permutation group of degree n has only $o(n)$ non-synchronizing ranks.

The greatest known number of non-synchronizing ranks for a primitive group of degree n is about $\sqrt{n}$, see the ABCRS paper. For basic primitive groups we think the value will be even smaller, maybe only $O(\log n)$.

A result about transitive groups

Proposition

Let G be a transitive permutation group on Ω. Suppose that A and B are subsets of Ω with $|A| \cdot |B| = |\Omega|$. Then the average value of $|Ag \cap B|$, over $g \in G$, is 1. In particular, either this intersection is always 1, or there exists $g \in G$ with $Ag \cap B = \emptyset$.

Proof.

Hint: Count triples (a, b, g) with $a \in A$, $b \in B$, $g \in G$, with $ag = b$. □

Corollary

If Γ is a vertex-transitive graph on n vertices, then

$$\omega(\Gamma) \cdot \alpha(\Gamma) \leq n.$$

Here $\alpha(\Gamma)$ is the independence number of Γ, the size of the largest null subgraph. (A complete subgraph and a null subgraph meet in at most one vertex.)

Separating groups

A transitive permutation group G on a set Ω is separating if, given any two subsets A and B of Ω with $|A| \cdot |B| = |\Omega|$ and $|A|, |B| > 1$, there exists $g \in G$ such that $Ag \cap B = \emptyset$: in other words, A and B can be "separated" by an element of G.

The argument in the previous proposition shows that, if sets A and B witness that G is non-separating, then $|Ag \cap B| = 1$ for all $g \in G$.

Proposition

A separating group is synchronizing.

For, if G is non-synchronizing, let f be a map not synchronized by G, with minimal rank; let A be a part of $\mathrm{Ker}(f)$, and $B = \mathrm{Im}(f)$. Then $|A| \cdot |B| = |\Omega|$ and $|Ag \cap B| = 1$ for all $g \in G$.

Theorem

The transitive group G on Ω is non-separating if and only if there exists a G-invariant graph Γ on Ω, not complete or null, such that

$$\omega(\Gamma) \cdot \alpha(\Gamma) = |\Omega|.$$

Separation in the hierarchy

We see that a separating group is synchronizing: for if G is not synchronizing, and every image of A is a transversal for P, then taking B to be a part of P we see that separation fails.

Furthermore, since non-separation requires a non-trivial G-invariant graph, a 2-homogeneous group is separating.

There are separating groups which are not 2-homogeneous: our argument above showed that S_n on 2-sets is separating if and only if it is synchronizing.

It is harder to find examples of groups which are synchronizing but not separating: we end with an example.

Quadrics

Let V be a 5-dimensional vector space over a finite field F of odd characteristic, and Q a non-singular quadratic form on V. There is a choice of basis such that, in coordinates,

$$Q(x_1, \ldots, x_5) = x_1x_2 + x_3x_4 + x_5^2.$$

The quadric associated with Q is the set of points in the projective space based on V (that is, 1-dimensional subspaces of V) on which Q vanishes. The number of points on the quadric is $(q+1)(q^2+1)$.

The associated orthogonal group $O_5(F)$ acts on the quadric; it is transitive on the points, and has just two orbits on pairs of points, corresponding to orthogonality and non-orthogonality with respect to the associated bilinear form.

The orthogonality graph

Let Γ be the graph in which two points are joined if they are orthogonal.

- the clique number of Γ is $(q+1)$, and the cliques of maximal size are totally singular lines on the quadric (the point sets of 2-dimensional subspaces on which the form vanishes identically – the span of the first and third basis vectors is an example);
- the independence number of Γ is q^2+1, and the independent sets of maximal size are ovoids of the quadric, sets of points meeting every line in exactly one point.

Synchronizing but not separating

We see from this that $O_5(q)$ is not separating. Is it synchronizing?

A colouring of the complement of Γ with $q^2 + 1$ colours would be a spread, a partition of the quadric into totally singular lines; no such partition can exist.

A colouring of Γ with $q + 1$ colours, on the other hand, is a partition of the quadric into $q + 1$ ovoids. Now, for $|F|$ an odd prime, it has been proved that the only ovoids on this quadric are hyperplane sections (quadrics in 3-dimensional projective space). Any two hyperplanes intersect in a plane, and the corresponding quadrics meet in a conic in the plane; so there are no two disjoint ovoids, and *a fortiori* no partitions into ovoids, in this case. So we have a family of groups which are synchronizing but not separating.

Note how this simple question in synchronization theory leads to the frontiers of knowledge in finite geometry!

Towards the Černý conjecture?

How could we use these ideas to prove some cases of the Černý conjecture?
First note that the conjecture has been proved in the case where none of the transitions of the automaton are permutations; so we may assume that the transitions include both permutations and non-permutations, and it would be enough to deal with the case where there is a single non-permutation, that is, $S = \langle G, f \rangle$.
Now there exist x and y such that $xf = yf$. So we can reduce the rank of an element $s \in S$ by postmultiplying it by gf, where g maps two points in the image of s to x and y. At most $n - 1$ steps of this kind are required.

Now if we could show that

- the only occurrences of members of G in a synchronizing word are used as described above; and
- any such element of G is a product of at most $n-1$ generators,

we would be done, since $(n-1)+(n-2)(n-1)=(n-1)^2$. This is not possible in general, but there are stronger conditions on the group G which guarantee the first condition, and there are powerful results about the diameters of Cayley graphs for permutation groups.

And finally . . .

A survey paper “Between primitive and 2-transitive: synchronization and its friends” by J. Araújo, P. J. Cameron, and B. Steinberg, will appear in the next issue of the *European Mathematical Society Surveys*, due out soon!