Permutation Groups and Transformation Semigroups
Lecture 3: Synchronization

Peter J. Cameron
Permutation Groups summer school, Marienheide
18–22 September 2017

The notion of synchronization arises in automata theory, but has very close links with transformation semigroups. The concept has had a lot of attention, partly because of the *Černý conjecture*; we begin with an account of this very addictive conjecture.

1 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 instant death. You have a schematic map of the dungeon (Figure 1), but you do not know where you are.

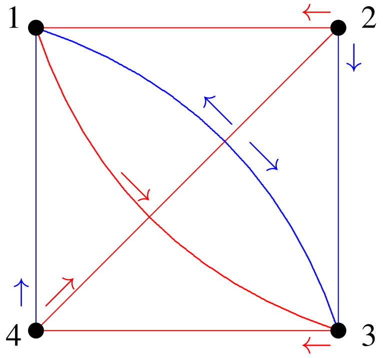


Figure 1: The dungeon

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

What Figure 1 shows is 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.

Our automata are particularly simple. There is no distinguished start state, no "accept state", no regular language, no nondeterminism.

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?

2 Synchronization

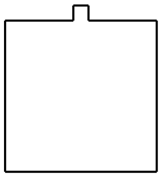
Combinatorially, an automaton is an edge-coloured digraph with one edge of each colour out of each vertex. Vertices are states, colours are transitions.

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 (indeed, a transformation monoid) on Ω.

We transfer the term "synchronizing" from the automaton to the semigroup. Thus, a transformation semigroup S is said to be *synchronizing* if it contains a map of rank 1.

The notion of synchronization arises in industrial robotics. Parts are delivered by conveyor belt to a robot which is assembling something. Each part must be put on in the correct orientation. One way to do this would be to equip the robot with sensors, information processing, and manipulators. An easier way involves synchronization.

Let us, for a simple case, 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, as in Figure 2.

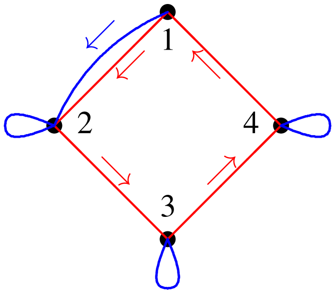


Figure 2: An industrial automaton

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

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 2.1 *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.*

Proof The forward implication is clear. So suppose the condition of the Proposition holds. Choose an element f of the monoid generated by the transitions which has smallest possible rank. If this rank is greater than 1, choose two points a and b in the image. By assumption, there is an element h which maps a and b to the same place; so the rank of fh is less than the rank of f, a contradiction.

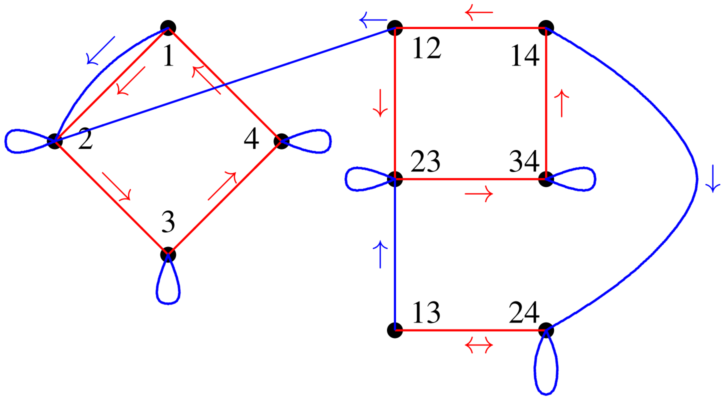


Figure 3: An extended diagram of an automaton

Now to obtain our bound, consider the diagram of the automaton extended to include pairs of states (shown for our industrial example in Figure 3).

According to the lemma, 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). The length of such a path is $O(n^2)$, and questions of connectedness can easily be checked. We only have to take such paths at most $n-1$ times. Moreover, checking this can be done in polynomial time, so we can test efficiently for the synchronization property. However, it is known that finding the shortest reset word is NP-hard.

3 Graph endomorphisms

We now take a little detour to discuss graph endomorphisms. A *graph* has vertices and edges, each edge joining two vertices; we assume that the edge has no direction (no initial or terminal vertex). An edge is a *loop* if the two vertices are equal, a *link* otherwise. Two edges are *parallel* if they join the same two vertices. A graph is *simple* if it has no loops and no two parallel edges.

Let Γ and Δ be simple undirected graphs. A homomorphism from Γ to Δ should be a structure-preserving map. Since the structure of a graph is given by its edges, we make the definition as follows.

A *homomorphism* from graph Γ to graph 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.

Parallel edges make no difference to this concept. However, the existence of loops changes things enormously. In a loopless graph, the images of adjacent vertices must be distinct; but, if Δ had a loop on a vertex x, we could map the whole of Γ to x. Similarly, the existence of directions on the edges makes a difference. For us, graphs will always be simple.

Let K_n be a complete graph on n vertices: all pairs of vertices are joined by edges. Also, let $\omega(\Gamma)$ denote the *clique number* of Γ, the size of the largest complete subgraph of Γ; and let $\chi(\Gamma)$ be the *chromatic number* of Γ, the minimum number of colours required to colour the vertices so that adjacent vertices receive different colours (this is called a *proper colouring* of Γ). Note that $\omega(\Gamma) \leq \chi(\Gamma)$, since the vertices in a clique must all get different colours.

Proposition 3.1 *(a) A homomorphism from K_n to Γ is an embedding of K_n into Γ; such a homomorphism exists if and only if $\omega(\Gamma) \geq n$.*

(b) A homomorphism from Γ to K_n is a proper colouring of Γ with n colours; such a homomorphism exists if and only if $\chi(\Gamma) \leq n$.

(c) There are homomorphisms in both directions between Γ and K_n if and only if $\omega(\Gamma) = \chi(\Gamma) = n$.

An *endomorphism* of a graph Γ is a homomorphism from Γ to itself, and an *automorphism* is a bijective endomorphism. The set of all endomorphisms of a graph is a transformation monoid on the vertex set of the graph, and the set of automorphisms is a permutation group. [**Caution:** This definition of automorphism fails in the infinite case, where we must also assume that the inverse map is an endomorphism.]

Now the single obstruction to a semigroup S being synchronizing is the existence of a graph Γ such that $S \leq \mathrm{End}(\Gamma)$.

Theorem 3.2 *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 It is clear that the condition is sufficient, since endomorphisms cannot collapse edges. Conversely, 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. (The proof is an exercise.)

4 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.

We can assume that the map f has minimal possible rank in $\langle G, f\rangle$. Then, for any $g \in G$, $\mathrm{rank}(fgf) = \mathrm{rank}(f)$, from which it follows that $(\mathrm{Im}(f))g$ is a transversal for $\mathrm{Ker}(f)$. We say that a k-set A is a *G-transversal* for a k-partition P if, for any $g \in G$, Ag is a transversal for P. Thus a permutation group is non-synchronizing if there is a non-trivial partition which has a G-section. However, we can find a much more convenient equivalent condition, as follows.

Theorem 4.1 *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.*

So 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.

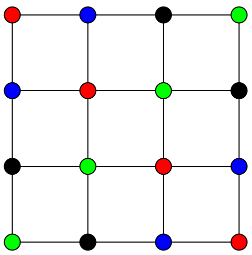
Corollary 4.2 *Let G be a permutation group of degree $n > 2$.*

(a) If G is synchronizing, then it is transitive, primitive, and basic.

(b) If G is 2-homogeneous, then it is synchronizing.

To see that synchronizing implies basic, note that the Hamming graph (whose vertex set is A^n, with two vertices joined if their Hamming distance is 1) has equal clique and chromatic number.

In the case of 2-dimensional Hamming graphs, a colouring with $|A|$ colours can be identified with a Latin square. This example uses the Klein group:



In higher dimensions, such colourings correspond to more complicated combinatorial objects.

So synchronizing groups form an interesting class lying between basic primitive groups and 2-homogeneous groups. We give an example to show that the containments are strict.

Example Let G be the group induced by S_m on the set of 2-element subsets of $\{1,\ldots,m\}$, where $m \geq 5$. Then G is primitive. (For $m = 4$, the relation "equal or disjoint" is a G-invariant equivalence relation on 2-sets.) It is clearly basic, and not 2-homogeneous for $m > 3$.

We show that G is synchronizing if and only if m is odd.

There are two 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 complementary graph where two pairs are joined if they are disjoint (the *Kneser graph* $K(m,2)$).

- The triangular graph has clique number $m-1$, a maximum clique consisting of all pairs containing one given point of the m-set. Its chromatic number is the *chromatic index* or edge-chromatic number) of K_m, which is well known to be $m-1$ if m is even, or m if m is odd. (Indeed, if m is odd, a set of pairwise disjoint pairs has size at most $(m-1)/2$, so the chromatic number is at least m.)
- The clique number of the Kneser graph is $m/2$ if m is even, and $(m-1)/2$ if m is odd (by the argument just given). It is elementary to see that the chromatic number is strictly larger; in fact, a celebrated theorem of Lovász shows that the chromatic number is $m-2$.

So our claim follows.

5 Separating groups

Separation is a concept which implies synchronization but in turn is implied by 2-homogeneity. It has no obvious connection with automata but is defined analogously to our graph-theoretic characterisation of synchronization.

We begin with the following general result.

Proposition 5.1 *Let G be a transitive permutation group on Ω. Suppose that A and B are subsets of Ω with the property that, for all $g \in G$, we have $|Ag \cap B| \leq 1$. Then $|A| \cdot |B| \leq |\Omega|$.*

Proof Count triples (a, b, g) with $a \in A$, $b \in B$, $g \in G$, and $ag = b$.

On the one hand, there are $|A|$ choices of a and $|B|$ choices of b; then the set of elements of G mapping a to b is a coset of the stabiliser of a, and so there are $|G|/|\Omega|$ such elements, by the Orbit-Stabiliser Theorem. So the number of triples is $|A| \cdot |B| \cdot |G|/|\Omega|$.

On the other hand, for each $g \in G$, we have $|Ag \cap B| \leq 1$, so there is at most one choice of a and b. So there are at most $|G|$ such triples.

The argument shows that, if equality holds, then $|Ag \cap B| = 1$ for all $g \in G$.

Note that the hypothesis of the proposition is satisfied if A is a clique and B an independent set in a vertex-transitive graph. Let $\alpha(\Gamma)$ be the *independence number* of Γ (the size of the largest independent set of Γ, in other words, the clique number of the complementary graph. Then we have:

Corollary 5.2 *If Γ is a vertex-transitive graph on n vertices, then*

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

We say that 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 5.3 *A separating group is synchronizing.*

For, if G is non-synchronizing, let P be a partition of Ω and A a G-transversal for P; let B be a part of P. Then $|A| \cdot |B| = |\Omega|$ and $|Ag \cap B| = 1$ for all $g \in G$.

Theorem 5.4 *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*

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

Proof If such a graph Γ exists, we can take A and B to be a clique and an independent set of maximum size in Γ to witness non-separation.

Conversely, suppose that G is non-separating, and let A and B be sets witnessing this property. No element of G can map a 2-subset of A to a 2-subset of B. So form a graph whose edges are the images under G of the 2-subsets of A; the graph is G-invariant, and A is a clique and B an independent set. Since the product of their cardinalities is $|\Omega|$, they are both of maximum size.

This theorem shows that we can test whether a group is separating by computing clique numbers of all G-invariant graphs. To test for the synchronizing property, we first test separation; if this fails, we must look further, and face the harder problem of finding chromatic numbers. If it were the case that "synchronizing" and "separating" were equivalent, then the step involving finding chromatic number could be omitted, and the algorithm would only need to find clique numbers of graphs. This is not so, but one has to look quite far to find an example of a group which is synchronizing but not separating.

Examples of such groups can be found as follows.

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. It can be shown that there is a choice of basis such that in coordinates, after possibly multiplying by a non-zero scalar,

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

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. It can be shown that 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.

Let Γ be the graph in which two points are joined if they are orthogonal. Then it is known that

- 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.

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; it is a standard fact that 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. It was shown by Ball, Govaerts and Storme that, for fields F of odd prime order, the only ovoids on this quadric are hyperplane sections (elliptic 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 an infinite family of groups which are synchronizing but not separating. (The classification of ovoids over non-prime fields is unknown.)

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