Synchronization update

Peter J. Cameron
University of St Andrews

CMS winter meeting, Vancouver, December 2018

Happy Birthday Robert!

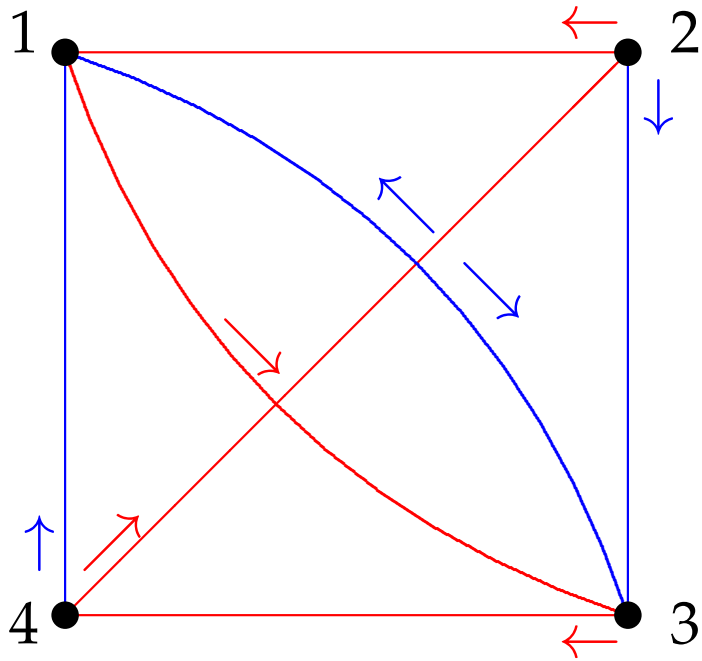
Synchronizing automata

Automata are very simple machines: they read a letter from an alphabet and change their state.
An automaton is synchronizing if there is a reset word in the input alphabet such that, when the automaton reads this word, it is in a fixed state, independent of its starting state.
We can regard an automaton as a transformation monoid on the set of states with a prescribed set of generators (the basic transitions corresponding to the letters in the alphabet). It is synchronizing if it contains a transformation of *rank* 1 (image of cardinality 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 death. You have a map of the dungeon,
but you do not know where you are.
Can you escape? In other words, is there a sequence of colours
such that, if you use the doors in this sequence from any
starting point, you will end in a known place?

An example



You can check that (Blue, Red, Blue) takes you to room 1 no matter where you start. So this is a picture of a synchronizing automaton.

Synchronizing permutation groups

A permutation group is a special transformation monoid, all of whose elements have full rank; so it is not synchronizing unless the domain has only one element. So we abuse language slightly in the following definition:

A permutation group G on Ω is synchronizing if, for any transformation t of Ω which is not a permutation, the monoid generated by G and t is synchronizing (as a transformation monoid).

We will see shortly that synchronizing groups are primitive, while 2-transitive groups are synchronizing.

Graph endomorphisms

All graphs here will be simple undirected graphs (no loops or multiple edges).
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.
An endomorphism of Γ is a homomorphism from Γ to itself.

Theorem

A transformation monoid M on Ω is non-synchronizing if and only if there is a non-null graph Γ on Ω, with clique number equal to chromatic number, such that $M \leq \mathrm{End}(\Gamma)$.

Corollary

A permutation group G on Ω is non-synchronizing if and only if there is a graph Γ on Ω, not complete or null, with clique number equal to chromatic number, such that $G \leq \mathrm{Aut}(\Gamma)$.

Synchronization in the hierarchy

We see from the preceding result that

- A 2-transitive group is synchronizing (for such a group preserves no non-trivial graph).
- A synchronizing group is primitive (for an imprimitive group preserves a disjoint union of complete graphs of the same size).

According to the O'Nan–Scott theorem, a primitive group either is contained in a wreath product with product action (and so preserves a Hamming graph and is non-synchronizing), or is of one of three types: affine, diagonal, or almost simple. So we see that a synchronizing group is of one of these three types. (The Hamming graphs have clique number equal to chromatic number.)

Separation

This related concept seems to have no interpretation in terms of automata. A transitive permutation group G is non-separating if it preserves a graph (not complete or null) with clique number times independence number equal to the number of vertices; it is separating otherwise.

A simple counting argument shows that, in a vertex-transitive graph, the product of clique number and chromatic number is at most the number of vertices.

Thus, a separating group is synchronizing. (If Γ is vertex-transitive and has clique number equal to chromatic number, then the colour classes are independent sets.)

Is the converse true?

Synchronizing, not separating

Apart from one sporadic example, only one family of groups which are synchronizing but not separating is known. This depends on fairly recent results in finite geometry.
The 5-dimensional orthogonal groups over finite fields of odd characteristic, acting on the quadric in 4-dimensional projective space, preserve one complementary pair of graphs, the orthogonality graph with respect to the quadratic form and its complement. A maximal independent set in the orthogonality graph is an ovoid on the quadric, while a maximal clique is a maximal singular subspace; any two of these objects meet in a point, and the product of their sizes is the number of points. However, to fail synchronization, we would need a partition of the quadric either into singular subspaces, or into ovoids. Over fields of odd *prime* order, neither of these things exists. (This uses a fairly recent result of Ball, Govaerts and Storme that all the ovoids are quadrics.)

Synchronization and separation, continued

Theorem

A primitive group which is synchronizing but not separating is almost simple.

Here is a sketch of the proof. We consider groups G which have a regular subgroup H. Then we can identify the domain Ω with H. Any G-invariant graph is a Cayley graph for H.

Proposition

- *Suppose that $A, B \subseteq H$ witness non-separation. Then H has an exact factorisation by $A^{-1} = \{a^{-1} : a \in A\}$ and B.*
- *Suppose that A and B witness non-separation, and that H has an exact factorisation by A and B. Then G is non-synchronizing.*

Using this, it is possible to show that for affine groups, and diagonal groups with two simple factors in the socle, synchronization and separation are equivalent.

The Hall–Paige conjecture

Hall and Paige conjectured that, if G is a finite group whose Sylow 2-subgroups are non-cyclic (in particular, a finite simple group), then its Cayley table has an orthogonal mate.
This has been proved fairly recently by the combined efforts of Hall and Paige, Wilcox, Evans, and Bray.
Using this it is possible to show that diagonal groups with more than two factors are non-synchronizing.
For example, a diagonal group with socle T^3 (for T simple) preserves the Latin square graph associated with the Cayley table of T; the orthogonal mate gives a $|T|$-colouring of this graph.

S_m on k-sets

Important examples of primitive, almost simple groups, are the groups induced on k-sets by the symmetric group of degree m. If there exists a Steiner system $S(t,k,m)$ for some t with $1 \leq t \leq k-1$, then these groups are non-separating. (The blocks of the Steiner system form an independent set in the graph where k-sets are joined if they meet in at least t points; an Erdős–Ko–Rado set is a clique in this graph.)

Conjecture

There is a function F such that, if $m \geq F(k)$, then S_m on k-sets is non-separating if and only if a Steiner system $S(t,k,m)$ exists for some t with $1 \leq t \leq k-1$.

The fairly recent result of Peter Keevash shows that, for large m, this condition is equivalent to a collection of divisibility conditions, so easy to check.
The conjecture is true for $k \leq 5$ (the case $k = 5$ by Mohammed Aljohani, not yet published).

References

- M. Aljohani, J. Bamberg and P. J. Cameron, Synchronization and separation in the Johnson scheme, *Portugaliae Mathematica* **74** (2018), 213–232.
- J. Araújo, P. J. Cameron and B. Steinberg, Between primitive and 2-transitive: Synchronization and its friends, *Europ. Math. Soc. Surveys* **4** (2017), 101–184.
- S. Ball, P. Govaerts and L. Storme, On ovoids of parabolic quadrics, *Designs, Codes, Cryptography* **38** (2006), 131–145.
- J. N. Bray, Q. Cai, P. J. Cameron, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, preprint, arXiv `1811.12671`
- A. B. Evans, The admissibility of sporadic simple groups. *J. Algebra* **321** (2009), 105–116.
- S. Wilcox, Reduction of the Hall–Paige conjecture to sporadic simple groups. *J. Algebra* **321** (2009), 1407–1428.