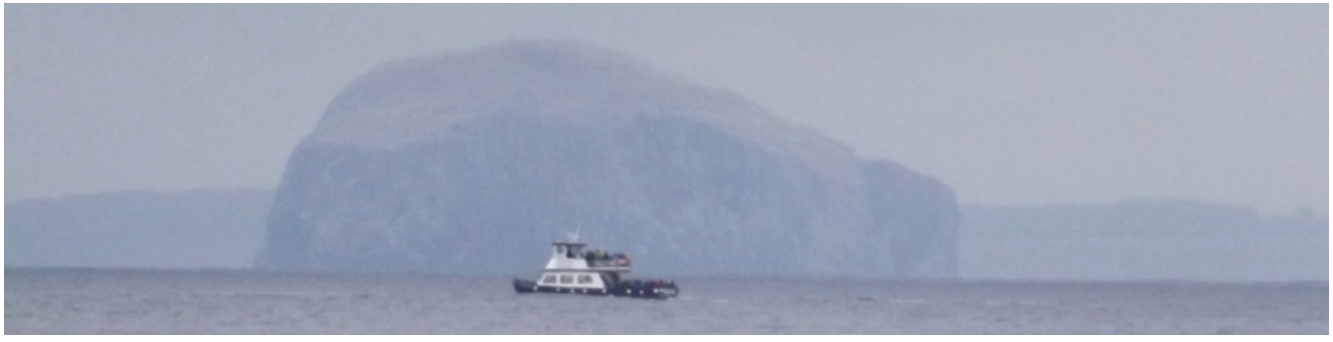
Synchronization and separation in the Johnson schemes

Peter J. Cameron
University of St Andrews

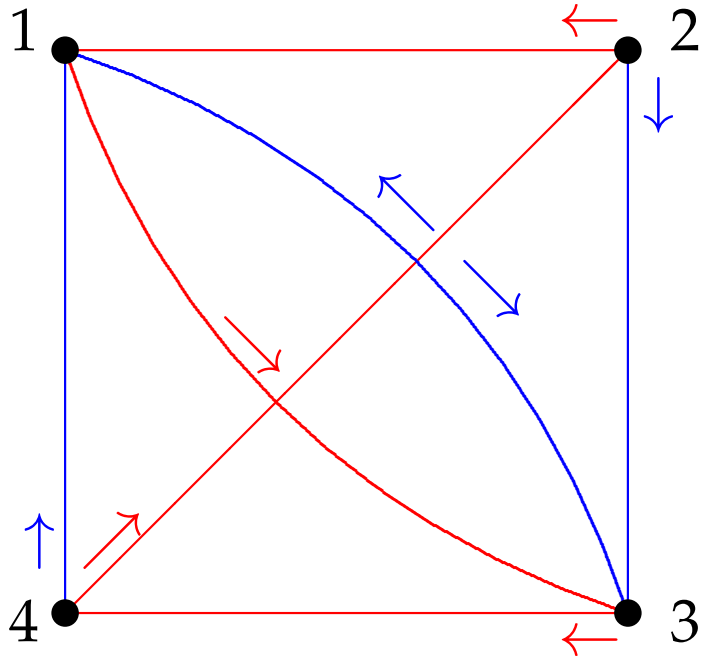


Bannai–Ito theory workshop
Hangzhou, 24 November 2017

(joint with Mohammed Aljohani and John Bamberg)

Synchronization

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. The Černý conjecture asserts that, if an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$. (If true, this would be best possible.) The conjecture is still open after half a century, and has motivated a lot of work on synchronization.

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.
An automaton is synchronizing if and only if the transformation semigroup contains a map of rank 1, that is, whose image has cardinality 1.

The obstruction to synchronizataion

Let Γ be a simple (undirected) graph on the vertex set Ω. An endomorphism of Γ is a map on Ω which takes edges of Γ to edges of Γ; there is no restriction to what it does to a non-edge (which can map to A non-edgs, or an edge, or collapse to a vertex).
The endomorphisms of Γ form a monoid, the endomorphism monoid of Γ, denoted by $\mathrm{End}(\Gamma)$.

Theorem

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

Permutation groups

João Araújo and Ben Steinberg considered semigroups of the form $\langle G, f \rangle$, where G is a permutation group and f a non-permutation. They made the following definition.
A permutation group G on Ω is synchronizing if, given any map $a : \Omega \to \Omega$ which is not a permutation, the semigroup $\langle G, a \rangle$ is synchronizing in the previous sense, that is, contains a rank 1 element.

Theorem

The permutation group G is non-synchronizing if and only if there is a non-trivial G-invariant graph Γ with clique number equal to chromatic number.

Separation

There is a closely related property, which can be phrased in terms of graphs as follows (this was not the original form). The transitive permutation group G is non-separating if there is a non-trivial G-invariant graph for which the product of clique number and independence number is equal to the number of vertices. (For a vertex-transitive graph, the product of clique number and independence number cannot exceed the number of vertices.)
If no such graph exists, then G is separating.
Note that, if a vertex-transitive graph has clique number equal to chromatic number, then all the colour classes in a minimal colouring have the same size, so the product of clique and independence numbers is equal to the number of vertices.

The big problem

Theorem

2-*homogeneous* $\Rightarrow$ *separating* $\Rightarrow$ *synchronizing* $\Rightarrow$ *primitive. None of these implications reverses.*

The big problem is:

Question

Determine the synchronizing (or separating) permutation groups.

For more details about the status of this problem, and related concepts on permutation groups derived from semigroups, see J. Araújo, P. J. Cameron and B. Steinberg, "Between primitive and 2-transitive: synchronization and its friends", *European Math. Soc. Surveys* **4** (2017), 101–184.

S_n on k-sets: the Johnson scheme

One important family, which I will talk about here, consists of the symmetric group S_n acting on k-sets, for $k < n/2$.
In this case, the orbital graphs (the minimal non-trivial G-invariant graphs) are defined by joining two k-sets if the cardinality of their intersection is i, for some fixed i with $0 \leq i \leq k-1$. These are the associate classes in the Johnson association scheme.
So any G-invariant graph is defined by a subset I of $\{0, \ldots, k-1\}$, with two k-sets joined if their intersection belongs to I. Let us call this graph $\Gamma_I(n,k)$.
We have to decide whether such graphs can have clique number equal to chromatic number, or product of clique number and independence number equal to $\binom{n}{k}$.

Erdős–Ko–Rado theorem

The Erdős–Ko–Rado theorem (proved 1938, published 1961) says that, for n sufficiently large in terms of k and t, the largest size of a family of t-intersecting k-subsets of $\{1,\ldots,n\}$ is $\binom{n-t}{k-t}$, and is realised by the family of k-sets containing a fixed t-set. How large is large enough? This was worked out by Wilson.

Steiner systems

This problem led us to a conjecture which would be a wide extension of part of Peter Keevash's existence theorem for t-designs.

A Steiner system $S(t,k,n)$ is a collection of k-subsets (called blocks) of a set of n points with the property that any t points lie in a unique block.

If such a system exists, then S_n acting on k-sets is not separating: the blocks of the system form a clique in the graph in which two k-sets are joined if they meet in at most $t-1$ points, and the k-sets containing a fixed t-set form an independent set (of Erdős–Ko–Rado type, or EKR type), and the product of the sizes of these sets is $\binom{n}{k}$.

The conjecture

Conjecture

There is a function F such that, if $n > F(k)$, then S_n acting on k-sets is non-separating if and only if a Steiner system $S(t,k,n)$ exists for some t with $0 < t < k$.

In other words, out of all the graphs $\Gamma_I(n,k)$, the only ones that matter for large n are those with $I = \{0,\ldots,t-1\}$ or $I = \{t,\ldots,k-1\}$.

There are well-known divisibility conditions which are necessary for the existence of a Steiner system: $\binom{k-i}{t-i}$ must divide $\binom{n-i}{t-i}$ for $i = 0,\ldots,t-1$. Keevash showed that, for n sufficiently large, these conditions are also sufficient.

So the conjecture can be re-phrased: for $n > G(k)$, S_n on k-sets is non-separating if and only if the divisibility conditions hold for some t with $0 < t < k$.

And what about synchronizing?

There is a similar conjecture. A large set of Steiner systems $S(t,k,n)$ is a partition of the set of k-subsets of an n-set into Steiner systems. If a large set exists, then S_n on k-sets is not synchronizing.

Conjecture

There is a function H such that, for $n > H(k)$, S_n acting on k-sets is non-synchronizing if and only if a large set of Steiner systems $S(t,k,n)$ exists for some t with $0 < t < k$.

Less is known about the existence of large sets, and we do not feel confident enough to conjecture an analogue of Keevash's theorem for them.

Results

The separation conjecture is true for $k \leq 4$:

Theorem

- *For $n \geq 5$, S_n acting on 2-sets is synchronizing if and only if it is separating; this occurs if and only if n is odd.*
- *For $n \geq 7$, S_n on 3-sets is synchronizing if and only if it is separating; this occurs if and only if $n \equiv 2$, 4 or 5 (mod 6) and $n > 8$.*
- *For $n \geq 9$, S_n on 4-sets is synchronizing if and only if it is separating; this occurs if and only if $n \equiv 3, 5, 6, 7, 9$ or 11 (mod 12) and $n > 9$.*

These agree with the conjecture. e.g. for $k = 4$, by results of Hanani, the necessary and sufficient conditions for the existence of $S(t, 4, n)$ are $n \equiv 0 \pmod 4$ for $t = 1$, $n \equiv 1$ or 4 (mod 12) for $t = 2$, and $n \equiv 2$ or 4 (mod 6) for $t = 3$.

Proof tools

The main tool is a theorem of Delsarte:

Theorem

Let $\mathcal{A}$ be an association scheme on v vertices and let Γ be the union of some of the graphs in the scheme. If C is a clique and S is an coclique in Γ, then $|C| \cdot |S| \leq v$. If equality holds and x and y are the respective characteristic vectors of C and S, then $(xE_jx^\top)(yE_jy^\top) = 0$ for all $j > 0$, where $E_0, E_1, \ldots$ are the minimal idempotents in the Bose–Mesner algebra of the scheme.

In order to apply this, we need expressions for the minimal idempotents in terms of the basis matrices of the algebra. These are given by the Q-matrix of the scheme.
For the Johnson scheme, the entries of the Q-matrix are expressed in terms of the Eberlein polynomials. This can also be found in Delsarte's thesis.

Exceptions

We saw in the theorem earlier that there are exceptions for $k = 3, n = 7, 8$, and for $k = 4, n = 9$.
For $k = 3, n = 8$, the Fano plane $S(2, 3, 7)$ is a 7-clique in the graph corresponding to intersection 1. A 7-colouring of this graph is given by the extension $S(3, 4, 8)$: for each of the 7 parallel classes of blocks, give a colour to the 3-subsets of the two blocks in this class.
A similar construction works for $k = 3, n = 7$: the Fano plane is a 7-clique; for each of its lines, that line together with the four 3-sets disjoint from it form a colour class in a 7-colouring.

For $k = 4$, $n = 9$, there is an overlarge set of $S(3, 4, 8)$ systems on 9 points, a partition of the 4-sets into 9 such systems, each omitting one point, found by Breach and Street. This is a 9-colouring of the graph on 4-sets corresponding to intersections 1 and 3. It is straightforward to find a 9-clique in this graph.

Breach and Street found computationally that there are just two overlarge sets up to isomorphism, each admitting a doubly transitive automorphism group. Praeger and I found a more conceptual proof, using the geometric phenomenon of triality on the hyperbolic quadric in $\mathrm{PG}(7, 2)$.

So small exceptions are often very beautiful configurations! The pattern continues, since examples arising from $S(4, 5, 11)$ give exceptions to the conjecture in the case $k = 5$, $n = 11$ or $n = 12$.

Other association schemes

Hamming schemes: Since the Hamming graph $H(n,q)$ has clique number and chromatic number q, it is non-synchronizing. (Indeed, primitive groups which are non-basic (that is, contained in a wreath product with the product action) are non-synchronizing.

q-Johnson schemes: Here similar considerations apply to the Johnson schemes. But the theory of Steiner systems in q-Johnson schemes is in its infancy, the first nontrivial example having been found by Michael Braun, Tuvi Etzion, Patric R. J. Östergård and Alexander Vardy in 2016. There are hard open problems here!

Polar spaces: Only the case of points has been studied. A classical polar space is non-synchronizing if and only if it has either an ovoid and a spread, or a partition into ovoids; it is non-separating if it has an ovoid. The complete solution to which polar spaces have these properties is not yet known despite many decades of research.

Others: Pick your favourite family of permutation groups or association schemes. Which ones are synchronizing, which are separating? The answer is probably not known! (The synchronization property is closed under coarsening, and a synchronizing scheme is primitive – that is, all relations are connected.)

. . . for your attention!