Combinatorics of transformation semigroups and synchronization

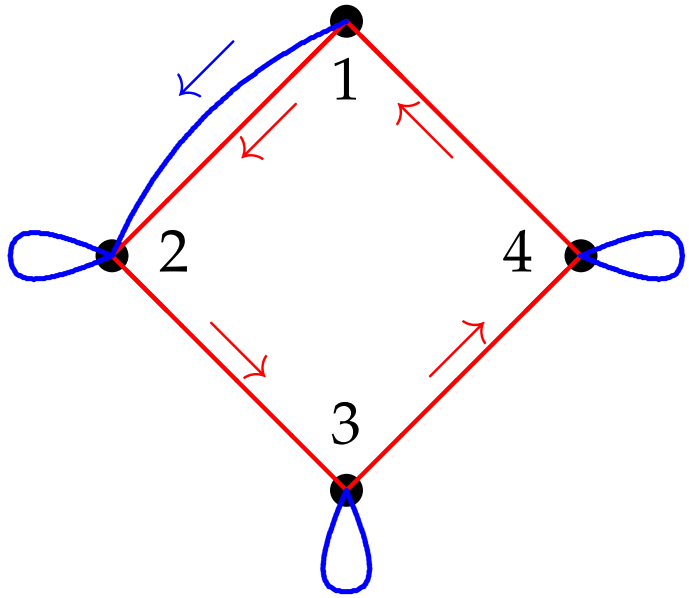
Peter J. Cameron
University of St Andrews

New Directions in Combinatorics
Institute for Mathematical Sciences
National University of Singapore
May 2016

NUS National University of Singapore

The dungeon

You are in a dungeon consisting of interconnecting caves. Each cave has two one-way exits, coloured red and blue; there is a third exit, which in one cave leads to freedom, and in the others to instant death. You have a map but don't know where you are.



You can check that the sequence BRRRBRRRB will bring you to room 2 from any starting point.

Automata

A (finite-state, deterministic) automaton is a black box with a finite number of internal states. If a symbol from an alphabet is input, it undergoes a state transition. (Imagine that there are red and blue buttons on the box.)

Our automata are very simple: they don't have "accept states", and so they don't recognise languages; you can start in any state.

An automaton can be represented combinatorially by a directed graph (whose vertices are the states) with edges labelled by symbols of the alphabet, so that there is exactly one edge with each label *leaving* each vertex, as in the preceding example.

Algebraically, a transition is a transformation on the set of states; since we may compose transitions, an automaton is a transformation monoid on the set of states, with a prescribed set of generators.

Synchronization

An automaton is said to be synchronizing if there is a sequence of inputs which brings it to a known state, regardless of its starting point. Such a sequence is called a reset word.
The example on the preceding slide had a reset word of length 9 (but none of shorter length).

Problem (The Černý conjecture)

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

Our example and the obvious generalisation shows that, if true, this bound is best possible. But the conjecture is still open after half a century!
We can test whether an automaton is synchronizing in polynomial time, but finding the shortest reset word is NP-hard.

Synchronization and graph endomorphisms

A transformation monoid is synchronizing if it contains a transformation of rank 1 (mapping the whole set to a single point).
There is a single obstruction to synchronization. An endomorphism of a (simple) graph is a map from the vertex set to itself which carries edges to edges.

Theorem

A monoid M is not synchronizing if and only if it is contained in the endomorphism monoid of a non-null simple graph whose clique number and chromatic number are equal.

One way round is clear; the other way, given a monoid M, define a graph where $v \sim w$ if and only if no element of M maps v and w to the same place, and check that this graph has the required property.

Synchronizing groups

With a few exceptions, all known examples meeting the Černý bound have monoids of the form $M = \langle G, a \rangle$, where G is a group of permutations, and a a transformation which is not a permutation. I will consider only this type in future.
Abusing notation, we call a permutation group G synchronizing if the monoid generated by G and a is synchronizing for all non-permutations a (on the set Ω of states).
Our question now is:

Question

Which permutation groups are synchronizing?

This turns out to include many problems of great interest from extremal combinatorics and finite geometry, as I shall show you.

Synchronizing groups, 2

From our earlier theorem, we see:

Theorem

A permutation group is non-synchronizing if and only if it is contained in the automorphism group of a non-trivial graph with clique number equal to chromatic number.

(The "trivial" graphs excluded are complete and null graphs.)

Corollary

- *A synchronizing group is transitive.*
- *A synchronizing group is primitive (preserves no non-trivial partition of Ω).*
- *A synchronizing group is basic (preserves no non-trivial Cartesian product structure on Ω).*

For example, if G preserves a partition with m parts each of size k, then it preserves a complete multipartite graph, which has clique number equal to chromatic number.

A necessary condition

A vertex colouring of a vertex-transitive graph with the smallest number of colours has the property that the colour classes all have the same size.
Hence a necessary condition for such a graph to have clique number equal to chromatic number is:

> The product of the clique number and the independence number of the graph is equal to the number of vertices.

So, for a given group G, we may consider G-invariant graphs and their complements in complementary pairs: if a graph fails this test then it and its complement do not need to be considered further.
This also shows that a transitive permutation group of prime degree is synchronizing.

The game

The game now is: Choose your favourite family of basic primitive permutation groups; try to decide whether or not the groups in the family are synchronizing.
I will give several examples:

- symmetic groups acting on k-sets;
- general linear groups acting on k-spaces;
- classical groups acting on polar spaces;
- some miscellaneous examples.

If G has r orbits on unordered pairs of points of Ω, then there are $2^r - 2$ non-trivial G-invariant graphs to check. (Each orbit may consist of edges or non-edges; and two trivial graphs must be excluded.)

S_n acting on k-subsets, $k = 2$

We consider the action of the symmetric group S_n on the set of k-subsets of $\{1, \ldots, n\}$. This group is primitive and basic if $n > 2k$.

We begin with the case $k = 2$. The two non-trivial graphs correspond to joining 2-sets if they intersect, or joining them if they are disjoint.

The first graph is the line graph of K_n: its clique number is $n - 1$, a maximal clique being all edges through a point. The second graph has clique number $\left\lfloor \frac{n}{2} \right\rfloor$.

The chromatic number of $L(K_n)$ is the chromatic index of K_n, which is $n - 1$ if n is even, or n if n is odd.

So S_n on 2-sets is synchronizing if and only if n is odd.

S_n acting on k-subsets, $k = 3$

The analogous result for S_n on the set of 3-subsets (for $n \geq 7$) is that it is synchronizing if and only if n is congruent to 2, 4 or 5 (mod 6) and $n > 8$. There are six invariant graphs; I will sketch the argument in two cases.

Consider the graph whose vertices are the 3-sets, two 3-sets joined if and only if they have non-empty intersection. The clique number is $\binom{n-1}{2}$, a maximum clique consisting of all the 3-sets through a point. The chromatic number is $\binom{n-1}{2}$ if n is divisible by 3 (take a Baranyai partition of the 3-sets), and greater otherwise.

Consider the graph whose vertices are the 3-sets, joined if and only if they intersect in at least two points. The clique number is $n-2$, a maximum clique consisting of all 3-sets containing two given points. The chromatic number is at least $n-2$; equality holds if and only if there is a large set of Steiner triple systems, a partition of the 3-sets into Steiner triple systems. These exist for all $n \equiv 1$ or 3 (mod 6) except for $n = 7$.

S_n acting on k-subsets, $k > 3$

The complete answer for larger values of k is not known.
It is clear from what is said above that it is going to involve ingredients like the Erdős–Ko–Rado theorem, Baranyai's theorem, Lovász's theorem on the chromatic number of Kneser graphs, the existence of t-designs and of large sets of t-designs for various parameters. Other considerations arise as well.
There is some beautiful combinatorics here, and I recommend the problem to anyone interested in a challenge!

$\mathrm{GL}(n,q)$ acting on k-spaces

An obvious analogue of the symmetric group acting on the set of k-subsets is the general linear group acting on the set of k-dimensional subspaces.

After Peter Keevash's beautiful theorem on the existence of designs, one of the most important problems for design theorists is to construct vector space analogues: given n, k, t, λ, we want collections $\mathcal{B}$ of k-dimensional subspaces of an n-dimensional vector space over the finite field $\mathrm{GF}(q)$, such that any t-dimensional subspace is contained in precisely λ members of $\mathcal{B}$. A few examples are known but there is no general existence result!

Hopefully it is clear from my remarks that testing synchronization for this class of groups will involve re-doing a lot of the combinatorics of sets and subspaces (including all the theorems mentioned earlier), in the setting of vector spaces and subspaces. Among this combinatorics, the existence of designs and large sets of designs will certainly feature prominently.

Classical groups on polar spaces

Another important class of groups consists of the classical groups (the symplectic, orthogonal and unitary groups), acting on the points of their associated polar spaces. The geometry associated with such a group is a non-degenerate bilinear, Hermitian or quadratic form on a vector space over a finite field: the points and lines of the polar space are the 1-dimensional and 2-dimensional subspaces on which the form is identically zero. So two points are collinear if and only if they are orthogonal with respect to the form.
The automorphism groups are primitive and (except for the 4-dimensional orthogonal groups of split type acting on ruled quadrics) are also basic.

Ovoids and spreads

In a polar space,

- a spread is a partition of the point set into subspaces of maximum dimension which are totally isotropic (that is, on which the form is identically zero);
- an ovoid is a set of points meeting any maximum totally isotropic subspace in a single point.

Theorem

A classical group acting on its polar space is non-synchronizing if and only if there exist either

- *an ovoid and a spread; or*
- *a partition into ovoids.*

Despite a lot of attention from finite geometers, we still do not know which polar spaces possess ovoids and/or spreads. The study of partitions into ovoids is more recent, partly motivated by this application to synchronization.

Almost synchronizing groups

In the examples so far, the maps not synchronized by primitive groups are uniform: all non-empty inverse images of points of the domain have the same size. People wondered if this were necessarily the case, and a permutation group G was said to be almost synchronizing if it synchronizes all non-uniform maps. It was conjectured that primitive groups are almost synchronizing.

The conjecture is false, however. Recently we found counterexamples with a nice geometric structure. They are the automorphism groups of the Tutte–Coxeter and Biggs–Smith graphs, acting on the edge sets of these graphs. (Their line graphs have many non-uniform endomorphisms, and their endomorphism monoids have a rich structure worth investigating.)

Other connections with semigroups

If you want to read more about synchronization, there is a long preprint available by João Araújo, Ben Steinberg and me (arXiv 1511.03184).
There are many other questions about semigroups which look rather similar, and involve relating properties of the transformation monoid $\langle G, a\rangle$ for all maps a in some class with properties of the permutation group G. I will use what time remains to describe briefly one such connection.
The semigroup property we are interested in is idempotent generation; an idempotent is an element t satisfying $t^2 = t$.
It is easy to see that idempotent generation of $\langle G, a\rangle$ for all rank 2 maps a implies that G is primitive on Ω; so we have a question about primitive permutation groups.

Road closures

Given a transitive permutation group G on Ω, an *orbital graph* for G on Ω is the graph whose edge set is an orbit of G on unordered pairs of elements of Ω.
According to an old theorem of Higman, a permutation group G is primitive if and only if every orbital graph is connected.

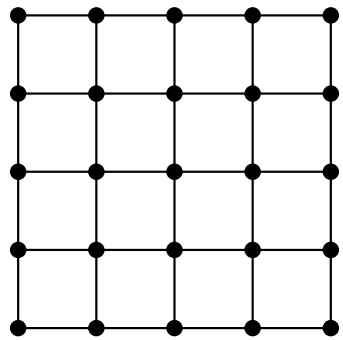
Theorem

Let G be a primitive permutation group on Ω. Then $\langle G, a\rangle$ is idempotent-generated for all rank 2 maps a if and only if G has the following property: for any orbital graph of G, with edge set E, and any block of imprimitivity B for the action of G on E, the graph with edge set $E \setminus B$ is connected.

In other words, thinking of the orbital graph as a road network, we cannot disconnect it by closing the roads in some block of imprimitivity for G.

Non-basic groups

First we observe that a group with the property of the theorem must be basic. The figure below shows why. There are two blocks of imprimitivity for the group acting on edges: the horizontal edges, and the vertical ones.



If workmen come and dig up all the vertical roads, then it is impossible to get from one row to another.

A conjecture

There are two kinds of basic examples for which the road closure condition fails. The first are a rich and varied class consisting of primitive groups which have imprimitive normal subgroups of index 2. The other form a very limited class based on the geometric phenomenon of triality.

Conjecture

Let G be a basic primitive permutation group. Suppose that G does not have an imprimitive normal subgroup of index 2, and is not one of the triality examples just mentioned. Then G has the 2-Hc property. Hence, for any rank 2 map a, the semigroup $\langle G, a\rangle \setminus G$ is idempotent-generated.

This conjecture has been checked computationally for all degrees up to 130 and many larger degrees. No counterexamples have been found.