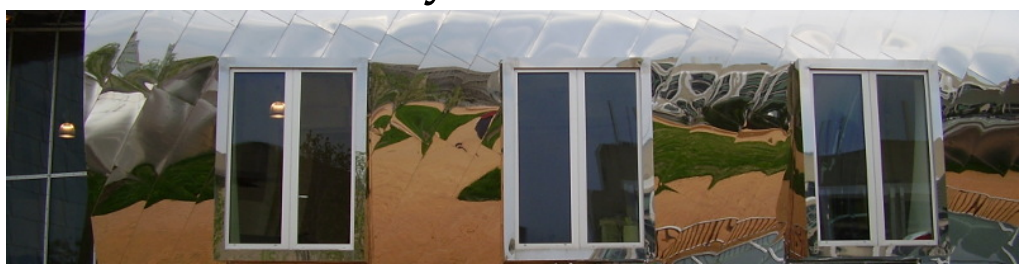
Synchronization

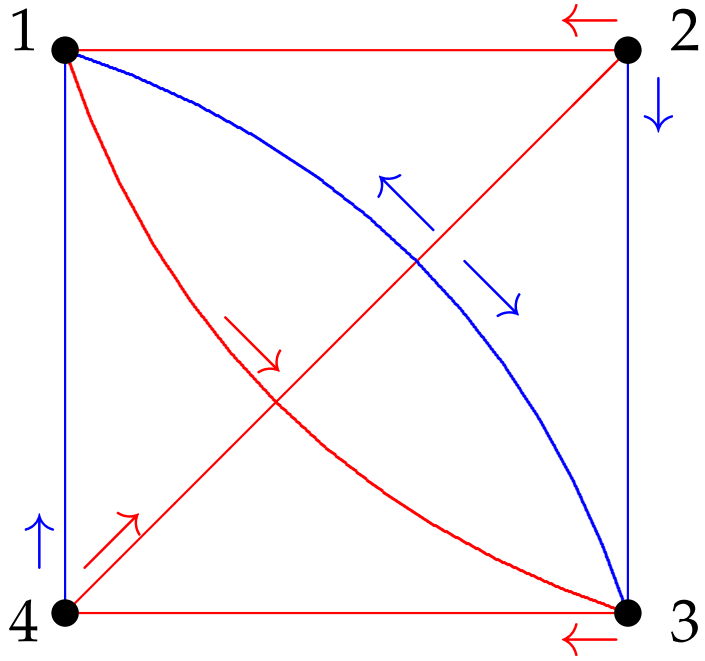
Peter J. Cameron
University of St Andrews



MIT Combinatorics Seminar
20 March 2019

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.

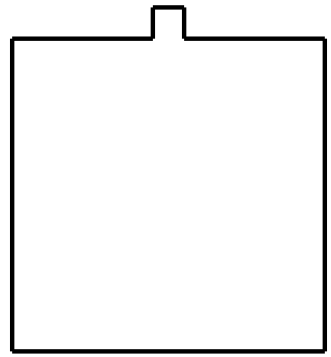
Not every finite automaton has a reset word. For example, if every transition is a permutation, then every word in the transitions evaluates to a permutation. How do we recognise when an automaton is synchronizing?

Automata and transformation semigroups

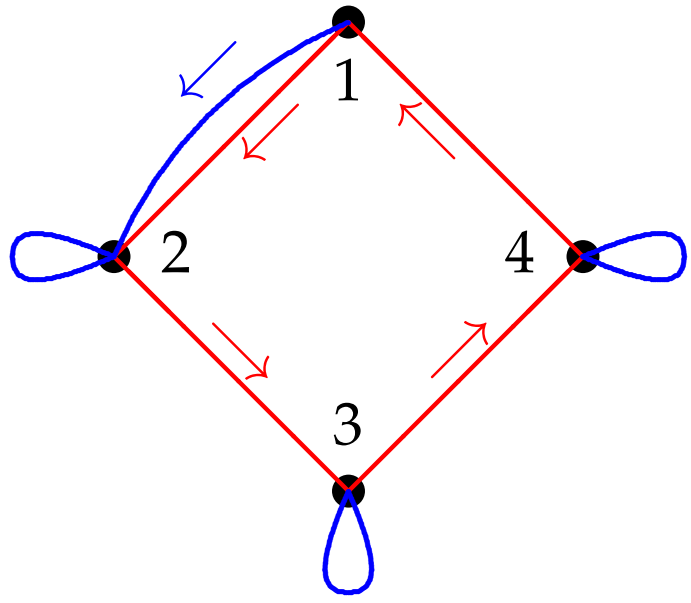
Combinatorially, an automaton is an edge-coloured digraph with one edge of each colour out of each vertex. Vertices are states, colours are transitions.
Algebraically, if $\Omega = \{1, \ldots, n\}$ is the set of states, then any transition is a map from Ω to itself. Reading a word composes the corresponding maps, so the set of maps corresponding to all words is a transformation semigroup on Ω. In fact it is a monoid, a semigroup with identity.
So an automaton is a transformation semigroup with a distinguished generating set.
The automaton is synchronizing if and only if there is an element of the semigroup which maps everything to a single point.

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.

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 in the following definition, due to João Araújo and Benjamin Steinberg. A permutation group G on Ω is called 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.

Permutation group theory

A permutation group G on a set Ω is

- transitive if any point of Ω can be mapped to any other by some element of G;
- t-transitive if any t-tuple of distinct points of Ω can be mapped to any other by some element of G;
- primitive if it is transitive and the only partitions of Ω which are invariant under G are the trivial ones (the partition into singletons and the partition $\{\Omega\}$).
- basic if it is primitive and does not preserve a Cartesian structure on Ω (bijection with Δ^m for $m > 1$).

The notion of t-transitivity gets stronger as t increases (for $t \leq |\Omega|$). Also

$$2\text{-transitive} \Rightarrow \text{basic} \Rightarrow \text{primitive} \Rightarrow \text{transitive}.$$

Among the consequences of the Classification of Finite Simple Groups is the complete determination of all 2-transitive groups. But we are some way from a determination of primitive groups!

Synchronization in the hierarchy

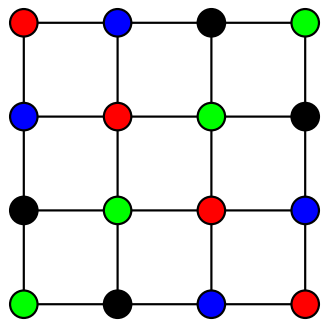
Theorem

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-transitive, 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-transitive 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-transitive, 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.

- $T(m)$ 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.

More generally . . .

An attempt to generalise the preceding has led to an interesting conjecture related to extremal set theory.
Consider the symmetric group S_m in its action on the set of k-element subsets of $\{1, \ldots, m\}$, for $k < m/2$. There is one general way in which such a group fails to be synchronizing.
A Steiner system $S(t, k, m)$ is a collection of k-sets (called blocks) of the set $\{1, \ldots, m\}$, such that any t-subset of $\{1, \ldots, m\}$ is contained in a unique block. A large set of Steiner systems is a partition of the set of all k-subsets of $\{1, \ldots, m\}$ into Steiner systems.

A conjecture

Conjecture

There is a function F such that, for $m > F(k)$, the group S_m acting on k-sets is non-synchronizing if and only if there is a large set of Steiner systems $S(t,k,m)$ for some t with $1 \leq t \leq k-1$.

The G-invariant graph on k-sets would make two k-sets adjacent if and only if they intersect in at least t points. Then an Erdős–Ko–Rado set (all k-sets containing a given t-set) is a clique, and the large set of Steiner systems a colouring, with the same cardinality.

Baranyai's theorem asserts that a large set of $S(1,k,m)$s exists if and only if $k \mid m$. The only other case to be settled is a theorem of Lu and Teirlinck: a large set of $S(2,3,m)$s exists if and only if m is an admissible order (congruent to 1 or 3 mod 6) and $m > 7$.

The O'Nan–Scott Theorem

In the last 40 years, many impressive results about primitive permutation groups have been proved with the help of two pieces of technology: the Classification of Finite Simple Groups, and the O'Nan–Scott Theorem. The latter divides the groups into a number of cases.
The theorem can be separated into two parts. The first concerns the group structure of non-basic primitive groups, and is not needed here since these groups are not synchronizing. The second asserts:

Theorem

Let G be a primitive basic permutation group. Then G is affine, diagonal, or almost simple.

Affine groups act as affine transformations on vector spaces over finite prime fields. Diagonal groups are a bit harder to describe, but I will say more later. Finally, a group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for some finite simple group T. In this case we do not specify the action of the group.

Three-factor diagonal groups

A Latin square is an $n \times n$ array whose cells contain entries from an alphabet of size k, such that each letter occurs once in each row and once in each column.
From a Latin square, we build a graph as follows: the vertices are the cells of the square, and two vertices are joined if and only if they lie in the same row or column or have the same entry.
The Cayley table of a group is a Latin square.
Now we can define a three-factor diagonal group to be the automorphism group of the Latin square graph of the Cayley table of a non-abelian finite simple group T. Its socle is $T \times T \times T$, and intersects the stabiliser of a cell in a diagonal subgroup of the direct product.

Transversals and orthogonal mates

A transversal in a Latin square of order n is a set of n cells, one from each row, one from each column, and one containing each entry. An orthogonal mate of the Latin square L is a Latin square M such that the positions of each letter of M form a transversal of L.

This picture shows three pairwise orthogonal Latin squares: can you spot them?

The Hall–Paige conjecture

In general, having an orthogonal mate is a much more restrictive condition than having a transversal. But, for Cayley tables of groups, it is not too hard to see that these conditions are equivalent, and are also equivalent to the group having what is known as a complete mapping.
Marshall Hall Jr and Lowell Paige conjectured in 1955 that a finite group G has a complete mapping (that is, has the property that its Cayley table has an orthogonal mate) if and only if the Sylow 2-subgroups of G are either trivial or non-cyclic.

Proof of the conjecture

The conjecture was proved in 2009:

- Stuart Wilcox reduced it to the case of simple groups, and dealt with the simple groups of Lie type (except the Tits group). The alternating groups had already been dealt with by Hall and Paige.
- Anthony Evans dealt with the Tits group and all the sporadic simple groups except the Janko group J_4.
- John Bray handled the remaining case, which involved computing with a permutation action of degree roughly 2×10^9.

The papers of Wilcox and Evans were published in the *Journal of Algebra* in 2009. Bray's work is yet unpublished, but has been accepted for publication as part of a paper on the work described here.

Diagonal groups

The Hall–Paige conjecture enables us to deal with one of the three O'Nan–Scott classes, the diagonal groups.
We saw that a three-factor diagonal group preserves a Latin square graph; such a graph has clique number n, and chromatic number n if and only if the Cayley table of the simple group has an orthogonal mate. But by Burnside's transfer theorem, the Sylow 2-subgroups of a simple group cannot be cyclic, so Hall–Paige applies: the Latin square graph has clique number equal to chromatic number, so the group is non-synchronizing.
The argument can be modified to show that diagonal groups with more than two factors are non-synchronizing.
The 2-factor case depends on some subtle questions about factorisations of simple groups and is yet unsolved.

Affine and almost simple groups

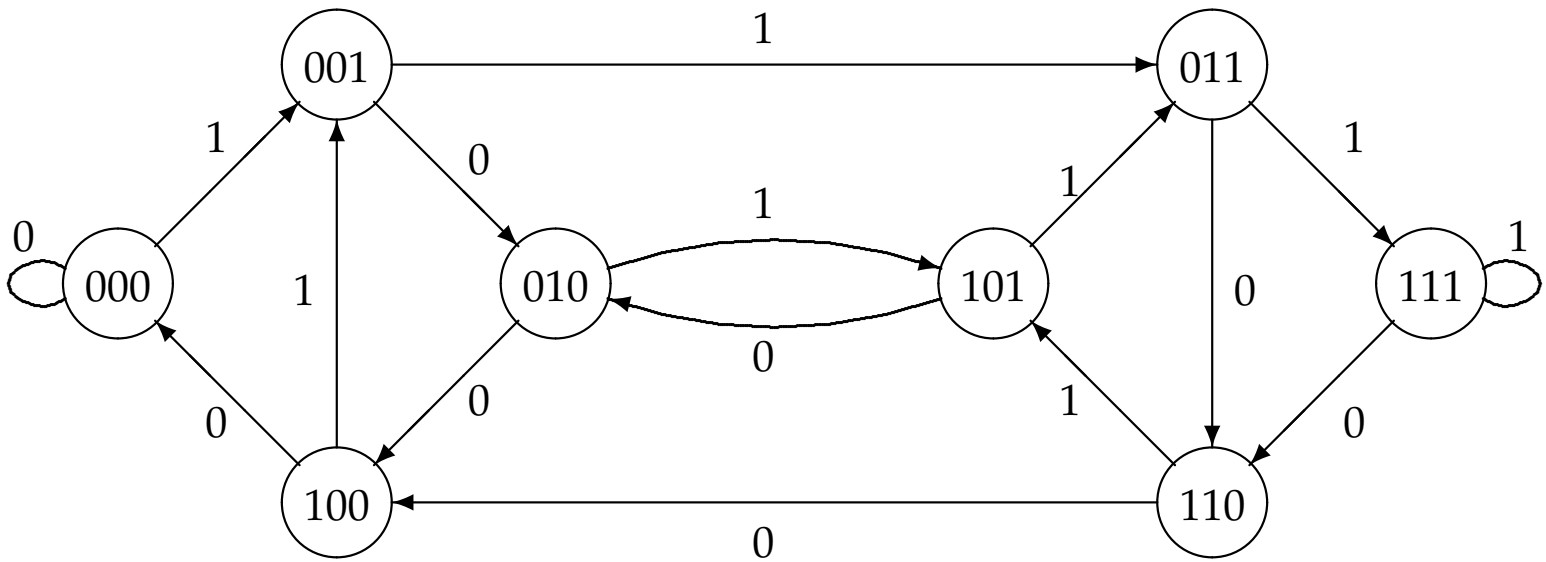
Synchronization for the other O'Nan–Scott classes almost always leads to interesting but difficult problelms in extremal combinatorics and finite geometry.
Earlier, I mentioned S_m acting on k-sets, where we have to invoke Erdős–Ko–Rado, Baranyai, and the existence of Steiner systems and large sets.
Baranyai's theorem also arises in the case of S_n acting on regular partitions, as do Hadamard matrices.
For the classical groups acting on their polar spaces, the argument turns on the existence of ovoids, spreads, and partitions into ovoids. Despite fifty years of effort by finite geometers, many of these problems are still open.

De Bruijn graphs

I will now turn to a recent development of synchronization in a different direction.

Let n be a positive integer and A a finite alphabet. The de Bruijn graph $G(n, A)$ has vertex set A^n. For $a \in A$, $w \in A^n$, the target of the edge labelled a with source w is obtained by removing the first letter of w and appending a.

Here is $G(3, \{0, 1\})$:



Strong synchronization

An automaton is said to be strongly synchronizing at level n if *every* word of length n is a reset word.
Clearly the de Bruijn graph $G(n, A)$ is synchronizing at level n: when it reads $w \in A^n$, it ends up in the state labelled w.
Moreover, it is universal with this property, in the sense that any strongly connected automaton which is strongly synchronizing at level n is obtained by folding $G(n, A)$, that is, taking the quotient by an equivalence relation $\equiv$ with the property that, if two states v and w are equivalent, then the states reached by reading a letter a from these two states are also equivalent.

Counting foldings

Question

How many foldings does $G(n, A)$ have?

For $n = 1$, the number of foldings is just the Bell number $B(|A|)$.
We have a formula for $n = 2$. Let

$$R(s,t) = \sum_{\pi} (-1)^{|\pi|-1} (|\pi| - 1)! \prod_{i=1}^{|\pi|} B(a_i s),$$

where π runs over all partitions of $\{1, \ldots, t\}$, $|\pi|$ is the number of parts of π, and a_i is the size of the ith part.
You may recognise the Möbius function of the lattice of set partitions here.

Theorem

The number of foldings of the de Bruijn graph with word length 2 *over an alphabet of cardinality n is*

$$\sum_{\pi} \prod_{i=1}^{s} R(s, a_i),$$

where π runs over all partitions of the alphabet, s is the number of parts of π, and a_i is the cardinality of the ith part for $i = 1, \ldots, s$.

Here $R(s,t)$ is the number defined on the preceding slide.
The numbers are easy to compute, but grow rather rapidly: for $|A| = 2, 3, \ldots, 7$, we obtain

$$5, 192, 78721, 519338423, 82833228599906, 429768478195109381814.$$

Transducers

A transducer is an automaton which can write as well as read. That is, if it is in state s and reads a symbol a, it writes a (possibly empty) string $\lambda(s,a)$ and moves as usual along the directed edge labelled a.
A transducer can potentially read an infinite string: I will always make the assumption that, if it does so, it writes an infinite string. Such a transducer induces a continuous map on the Cantor space of all infinite strings over the alphabet.
The maps induced by invertible transducers are thus homeomorphisms of the Cantor space. The collection of such maps is a group, the rational group, introduced by Grigorchuk, Nekrashevich, and Sushchanskiĭ.

The Higman–Thompson groups

The first infinite finitely presented group known was discovered by Richard Thompson in the 1960s; this is now called Thompson's group V.
Shortly afterwards, Graham Higman found an infinite family of such groups, denoted $G_{n,r}$, with $n \geq 2$ and $1 \leq r \leq n-1$.
Thompson's group V is $G_{2,1}$.
These groups are subgroups of the rational group, although they were not initially presented in this way. They are defined by prefix replacement on infinite strings.

Automorphisms of $G_{n,r}$

In recent work with Collin Bleak, Yonah Maissel, Andrés Navas and Shayo Olukoya, we have given a description of the outer automorphism group of $G_{n,r}$. Outer automorphisms are given by core (that is, strongly connected) invertible transducers for which the automata describing the transducer and its inverse are both strongly synchronizing.
However, the arguments are rather lengthy ...

References

- M. Aljohani, J. Bamberg and P. Cameron, Synchronization and separation in the Johnson scheme, *Portugaliae Mathematica* **74** (2018), 213–232.
- J. Araújo, P. Cameron and B. Steinberg, Between primitive and 2-transitive: Synchronization and its friends, *Europ. Math. Soc. Surveys* **4** (2017), 101–184.
- C. Bleak, P. Cameron, Y. Maissel, A. Navas, and F. Olukoya, The further chameleon groups of Richard Thompson and Graham Higman: Automorphisms via dynamics for the Higman groups $G_{n,r}$, arXiv 1605.09302
- J. Bray, Q. Cai, P. Cameron, P. Spiga and H. Zhang, The Hall-Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra*, in press; arXiv 1811.12671