Synchronization and semigroups, graphs and groups

Peter J. Cameron
University of St Andrews

G2S2, Sochi, 9 August 2021

Welcome to G2S2!

The G2 conferences are designed as summer schools as well as international conferences.

In this talk I will tell you a story covering the four topics of the meeting in reverse order, starting with synchronizing automata and ending with primitive permutation groups. To fit the "summer school" element, some of what I say is expository material aimed at students.

Please feel free to ask questions!

I have prepared a list of exercises and research problems, which is available on request.

Synchronizing automata

An automaton is a machine which has a set Ω of states, and can read symbols from an alphabet A. It is a very simple machine: all it does at a given time step is to read a symbol and change its state.

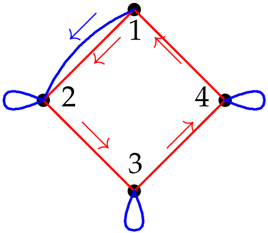
An automaton can read a word or sequence of symbols; each symbol causes a state change.

An automaton is synchronizing if there is a word, called a reset word, such that when the automaton reads this word, it ends up in a fixed state, no matter where it starts.

Reset words are useful to bring a machine into a known state before applying further transformations to it.

An infamous problem

Here is a synchronizing automaton.



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

Problem

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

This is the Černý conjecture, posed in the 1960s and still open.

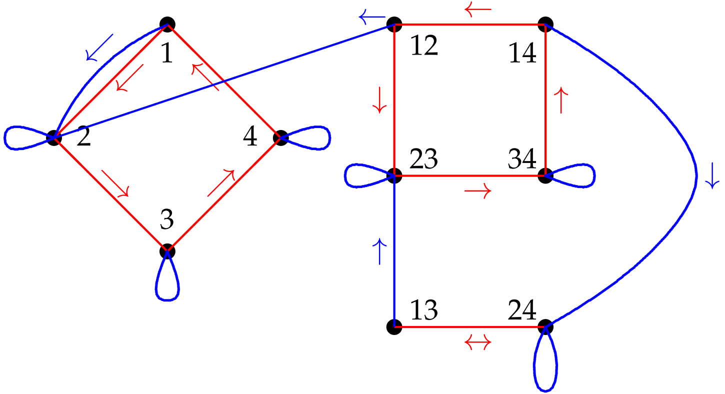
Decision is easy

Given a finite automaton, we can decide in polynomial time whether or not it is synchronizing.
This depends on the following observation:

> A finite automaton is synchronizing if and only if, for any two states s and t, there is a word $w = w_{s,t}$ in the input alphabet such that reading w from s or t takes the automaton to the same state.

For such a word reduces by (at least) one the number of reachable states. So after at most $n - 1$ such words we arrive at a single state.
Now the next slide shows how this can be tested.

The picture shows the earlier example, with the diagram extended to show all pairs of states.



Now it suffices to check that there is a path from any vertex on the right to some vertex on the left; this can clearly be done in polynomial time.

The resulting word has length $O(n^2)$, giving an $O(n^3)$ upper bound for the length of a reset word. The constant has been improved, but not the exponent 3.

Transformation monoids

The Černý conjecture seems to have nothing to do with either graphs or groups; but wait …

Each letter of the alphabet corresponds to a transition on the set Ω of states. Reading a word corresponds to composing the transitions. So the set of all possible transitions is closed under composition and contains the identity map (corresponding to the empty word): so

> An automaton can be represented as a transformation monoid on the set Ω of states, having a distinguished set of generators. The automaton is synchronizing if and only if the monoid contains an element of rank 1.

So the Černý conjecture is a question about transformation monoids, and semigroups enter the picture.

Graphs

An endomorphism of a graph is a map from the vertex set to itself which carries edges to edges. The action on nonedges is not specified; a nonedge may map to a nonedge, or to an edge, or collapse to a single vertex.

The endomorphisms of a graph form a transformation monoid. Moreover, as long as the graph has at least one edge, its endomorphism monoid is not synchronizing, since that edge cannot be collapsed by any endomorphism.

Synchronization and endomorphisms

Now we have a pleasant surprise:

Theorem

A transformation monoid M is non-synchronizing if and only if there is a non-trivial graph Γ on the domain such that M is contained in the endomorphism monoid of Γ. Moreover, we can assume that the clique number and chromatic number of Γ are equal.

A graph is trivial if it is complete (all possible edges) or null (no edges at all). The clique number is the number of vertices in the largest complete subgraph, while the chromatic number is the number of colours required to colour the vertices so that adjacent vertices get different colours.

Sketch proof

Since endomorphisms cannot collapse edges, it is clear that the endomorphism monoid of a non-trivial graph must be non-synchronizing.

For the converse, let M be a transformation monoid on Ω. We define a graph $\mathrm{Gr}(M)$ as follows: the vertex set is Ω; there is an edge joining s and t if and only if there is no element $m \in M$ with $sm = tm$. Now

- $\mathrm{Gr}(M)$ is non-trivial if and only if M is non-synchronizing;
- $M \leq \mathrm{End}(\mathrm{Gr}(M))$;
- $\mathrm{Gr}(M)$ has clique number equal to chromatic number.

The first point is clear; I will outline the second. If it fails, then some element $m \in M$ maps an edge $\{s, t\}$ to either a single vertex or a non-edge. The first case contradicts the definition; in the second case, there is $m' \in M$ with $(sm)m' = (tm)m'$, so mm' maps s and t to the same place.

For the last point, take an element $m \in M$ of minimal rank; then m is a colouring of the graph and its image is a clique.

Does this help?

We seem to have replaced an easy problem (deciding whether an automaton is synchronizing) by a much harder problem (deciding whether the graph has clique number equal to chromatic number).

However, the advantage is that we can potentially show that whole classes of automata are synchronizing, or non-synchronizing.

In our introductory example, one of the basic transitions of the automaton was a permutation (generating a cyclic group of order 4), while the other was not. We now turn to automata with the property that all but one of their transitions are permutations.

Groups

A permutation group is a transformation monoid in which every element is a bijection. Permutation groups form the oldest part of group theory, going back to the work of Galois or earlier.

Here are some basic definitions related to permutation groups. If you have seen these before, my definitions may look a little different, but you should be able to see that they are equivalent. If you haven't seen them, then you can take these as the definitions.

Let Ω be a set. I will call a structure on Ω trivial if it is invariant under the symmetric group, the group of all permutations of Ω. Many important permutation group properties can be defined saying that a permutation group G on Ω (a subgroup of $\mathrm{Sym}(\Omega)$) has property P if it preserves no non-trivial structure of type X on Ω.

Permutation group properties

- A permutation group G on Ω is transitive if it preserves no non-trivial subset of Ω. (The trivial subsets are the whole of Ω and the empty set.)
- A permutation group G on Ω is primitive if it is transitive and preserves no non-trivial partition of Ω. (The trivial partitions are the partition into singletons and the partition with a single part Ω.)
- A permutation group G on Ω is 2-homogeneous if it preserves no non-trivial graph on Ω. (The trivial graphs are the complete and null graphs.)

Now we can add one further property:

- A permutation group G on Ω is synchronizing if it preserves no no-trivial graph with clique number equal to chromatic number on Ω.

Note on terminology

A permutation group cannot be synchronizing as a transformation monoid (unless the domain has just one point). So we hijack the word for a different use, as described on the preceding slide.

Theorem

The permutation group G on Ω is synchronizing if and only if, for every non-permutation f of Ω, the transformation monoid $\langle G, f \rangle$ generated by G and f is synchronizing.

Sketch proof: If G preserves a non-trivial graph with clique number equal to chromatic number, then this graph has an endomorphism f which is not an automorphism; so $\langle G, f \rangle$ preserves the graph, and is not synchronizing.

Conversely, if there exists f such that $\langle G, f \rangle$ is not synchronizing, then this monoid is contained in $\mathrm{End}(\Gamma)$, where Γ is a non-trivial graph with clique number equal to chromatic number; clearly $G \leq \mathrm{Aut}(\Gamma)$.

Which permutation groups are synchronizing?

A long-running project aims to answer this question. Here is a summary of what we know.

- A synchronizing group is transitive. For if G preserves a non-trivial subset Δ of Ω, then the complete graph on Δ is a non-trivial G-invariant graph with clique number equal to chromatic number.
- A synchronizing group is primitive. For if G is transitive and preserves a non-trivial partition P of Ω, then all parts of P have the same size, and the disjoint union of complete graphs on the parts of P is G-invariant and has clique number equal to chromatic number.

The O'Nan–Scott Theorem

The structure of finite primitive permutation groups is given by this theorem, which was proved independently by Michael O'Nan and Leonard Scott in 1979. However, much of the theorem, including what we need, was in Camille Jordan's *Traité des Substitutions* a hundred years earlier. The groups in the theorem will be explained on the next few slides.

Theorem

A finite primitive permutation group G on Ω satisfies one of the following:

- *G is contained in a wreath product with product action;*
- *G is affine;*
- *G is contained in a group of simple diagonal type;*
- *G is almost simple.*

Non-basic groups

Let A be a finite alphabet and m an integer greater than 1. The Hamming graph $H(m, A)$ has vertex set A^m (the set of words of length m over the alphabet A); two vertices are joined if they have Hamming distance 1 (that is, they agree in all positions except one).

The wreath products in the first part of the O'Nan–Scott Theorem preserve Hamming graphs. We call these non-basic; a permutation group is basic if it preserves no Hamming graph.

- A synchronizing group is basic.

For this we need to show that Hamming graphs have clique number equal to chromatic number. Let $|A| = n$. The set of vertices with arbitrary entry in the first position and all other entries equal is a clique of size n. But, if we take A to be an abelian group of order n, then the function mapping $a_1 a_2 \ldots a_m$ to $a_1 + a_2 + \cdots + a_m$ is a colouring with n colours.

Affine and almost simple groups

A permutation group G on Ω is affine if Ω can be identified with a vector space over a prime field F so that elements of G have the form $v \mapsto vM + c$ for some matrix M and vector c. Affine groups may or may not be synchronizing.

A group G is almost simple if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian finite simple group G. Note that the action as a permutation group is not specified, and is completely arbitrary. Almost simple groups may or may not be synchronizing.

Diagonal groups

I will not describe the groups of simple diagonal type in detail. I will just say that diagonal groups in much greater generality are studied in a recent paper with Rosemary Bailey, Cheryl Praeger and Csaba Schneider.

The diagonal group $D(G, m)$ of dimension m over a group G is a permutation group of degree $|G|^m$ containing G^m as a regular subgroup.

If G is a non-abelian simple group, we have a simple diagonal group; these are the groups in the O'Nan–Scott theorem. However, the construction of these groups does not require G to be simple, or even finite.

Diagonal groups with dimension at least 2 preserve a graph known as a diagonal graph. Based on the proof in 2009 of the Hall–Paige conjecture, it is possible to show that a diagonal graph over a finite simple group has clique number equal to chromatic number. Hence permutation groups of simple diagonal type with dimension at least 2 are non-synchronizing. There remain the simple diagonal groups of dimension 1. These contain the group $G \times G$, acting on G by left and right multiplication, together with possibly inversion and automorphisms of G. A recent result of John Bamberg, Michael Giudici, Jesse Lansdown and Gordon Royle shows that these groups may or may not be synchronizing.

Latin squares

I will end with some words about Latin squares, which provide a connection with diagonal groups, and explain the relevance of the Hall–Paige conjecture. Rosemary will tell you more about diagonal graphs in her lecture on Friday.

A Latin square is a square array of size $n \times n$ filled with letters from an alphabet of size n, so that each letter occurs once in each row and column.

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

Latin squares exist in great profusion. There are more than $\exp(n^2)$ Latin squares of order n; exact numbers are only known up to $n = 11$.

Latin square graphs

The Cayley table of a group is a Latin square. (The Latin square on the preceding slide is the Cayley table of the Klein group V_4.) These Latin squares are better behaved: the automorphism group (or paratopism group, as it is called) of the Cayley table based on G is the 2-dimensional diagonal group over G.

The Latin square graph $\Gamma(L)$ has as vertices the n^2 cells of L, two vertices adjacent if the cells are in the same row or same column or contain the same letter. Latin square graphs are strongly regular, and indeed form a very prolific family of strongly regular graphs.

Transversals

Let L be an $n \times n$ Latin square. A transversal of L is a collection of n cells, one in each row, one in each column, and one containing each symbol.

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Orthogonal mates

An orthogonal mate of L is a $n \times n$ Latin square M with the property that, for any (a, b), where a is in the alphabet of L and b in the alphabet of M, there is a unique cell in which L contains the letter a and M contains the letter b. The letters of M partition the cells of L into transversals.

e	**a**	**b**	**c**
a	**e**	**c**	**b**
b	**c**	**e**	**a**
c	**b**	**a**	**e**

Cayley tables

For arbitrary Latin squares, the existence of a transversal and an orthogonal mate are far from equivalent; but for Cayley tables of groups, we have:

Theorem

For the Cayley table L of a group G of order n, the following are equivalent:

- *L has a transversal;*
- *L has an orthogonal mate;*
- *the Latin square graph $\Gamma(L)$ has chromatic number n.*

Marshall Hall Jr and Lowell Paige conjectured in 1955 that a finite group G satisfies the three equivalent conditions of the preceding theorem if and only if either G has odd order or the Sylow 2-subgroups of G are non-cyclic.

The Hall–Paige conjecture

The conjecture was proved by Stewart Wilcox, Tony Evans and John Bray in 2009.

Wilcox reduced the problem to the case of non-abelian simple groups, and handled the groups of Lie type except for the Tits group ${}^2F_4(2)'$ (the alternating groups had been done by Hall and Paige); Evans dealt with the Tits group and all the sporadic simple groups except for the Janko group J_4; and Bray did J_4, although his proof was not published until 2020.

Diagonal groups of dimension 2 are non-synchronizing

The diagonal group $D(G, 2)$ of dimension 2 over G preserves the Latin square graph of the Cayley table of G. (Indeed, with a few small exceptions, it is the automorphism group of the Latin square graph.)

If the diagonal group is primitive, then G must be simple. Since the Sylow subgroups of finite simple groups are non-trivial and non-cyclic, the Latin square graphs of their Cayley tables have clique number equal to chromatic number. So the 2-dimensional simple diagonal groups are non-synchronizing.

Higher dimensions

Using graph homomorphisms it is possible to extend this result to all higher dimensions.
It can be shown that, over a given group G, there is a homomorphism from the m-dimensional diagonal graph to the $(m-2)$-dimensional diagonal graph.
Now homomorphisms do not increase chromatic number; the 1-dimensional diagonal graph is complete on $|G|$ vertices; and the 2-dimensional case is handled by the Hall–Paige conjecture.
So $D(G, m)$ is non-synchronizing for all non-abelian simple groups G and all $m \geq 2$.

References

- 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; doi: `10.4171/EMSS/4-2-1`
- J. N. Bray, Q. Cai, P. J. Cameron, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra* **545** (2020), 27–42; doi: `10.1016/j.jalgebra.2019.02.025`
- R. A. Bailey, P. J. Cameron, C. E. Praeger and Cs. Schneider, The geometry of diagonal groups, *Trans. Amer. Math. Soc.*, in press; doi: `10.1090/tran/8507`