Finite permutation groups: applications to transformation semigroups and synchronization

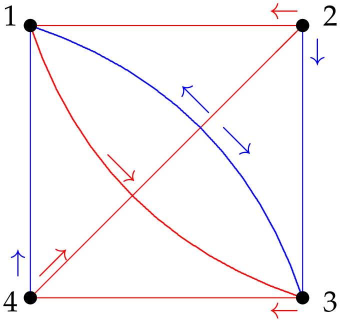
Peter J. Cameron
University of St Andrews

GRAW01, 10 January 2020

The dungeon

You are in a dungeon consisting of a number of rooms. Each room has two doors, coloured red and blue, which open into passages leading to another room (maybe the same one). Each room also 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?



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 monoids

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 monoid on Ω.

So an automaton is a transformation monoid with a distinguished generating set. It is synchronizing if it contains a map with rank 1.

The Černý conjecture

Much of the research on synchronization has been driven by the Černý conjecture, over 50 years old and still unsolved.

The conjecture is very simple. It states that if an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$. It is known that, if true, this would be best possible for all n.

This conjecture comes with a health warning. Despite its apparent simplicity, it does fight back!

What follows is not specifically a contribution to this conjecture, although these methods have allowed us to make small progress. See the paper by João Araújo, Ben Steinberg and me for more detail.

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 monoid; 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 by making the following definition. A permutation group G on Ω is 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.

So the definition of "synchronizing" exactly matches our previous template for permutation group properties: G is synchronizing if and only if there is no non-trivial G-invariant graph with clique number equal to chromatic number.

Synchronization in the hierarchy

An imprimitive group preserves a partition, and so a disjoint union of complete graphs of the same size (which clearly has clique number equal to chromatic number).

A non-basic group preserves a Hamming graph (two n-tuples adjacent if their Hamming distance is 1); this graph has clique number equal to chromatic number, both equal to the alphabet size.

A 2-homogeneous group preserves no non-trivial graph at all.

So we have:

Theorem

Let G be a permutation group of degree $n > 2$.

- *If G is synchronizing, then it is primitive and basic.*
- *If G is 2-homogeneous, then it is synchronizing.*
- *None of these implications reverses.*

The O'Nan–Scott Theorem

Recall that, by the O'Nan–Scott Theorem, a basic group is affine, diagonal or almost simple.

Affine groups have abelian normal subgroups. They have the form

$$\{x \mapsto xA + c : c \in V, A \in H\},$$

where V is a finite vector space and H an irreducible linear group on V. They may or may not be synchronizing.

Almost simple groups satisfy $T \leq G \leq \mathrm{Aut}(T)$, where T is a non-abelian finite simple group. The action is not specified. They may or may not be synchronizing.

Diagonal groups are considered below.

Counterexamples to a theorem of Cauchy

This was the wonderful title of a paper by Peter Neumann, Charles Sims and James Wiegold in 1968.

Cauchy "proved" that a primitive permutation group whose degree is one more than a prime must be doubly transitive.

Neumann, Sims and Wiegold noted that, if T is a finite simple group, then the group induced on T by left and right multiplication,

$$\{(g,h) : x \mapsto g^{-1}xh\}$$

is primitive. One can enlarge the group by adjoining automorphisms of S (the inner automorphisms are already included as the "diagonal" subgroup $\{(g,g) : g \in T\}$) and the map $x \mapsto x^{-1}$. The result is the 2-factor diagonal group $D(T,2)$.

They noted that $|A_5| = 59+1$, $|\mathrm{PSL}(2,7)| = 167+1$, $|A_6| = 359+1$, $|\mathrm{PSL}(2,8)| = 503+1$, $|\mathrm{PSL}(2,11)| = 659+1$, $\ldots$. (It is not known whether there are infinitely many counterexamples.)

Latin squares

A Latin square of order n is an $n \times n$ array with entries taken from an alphabet of size n, so that each letter in the alphabet occurs once in each row and once in each column.

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

This is not just any old Latin square: it is the Cayley table, or multiplication table, of the Klein group of order 4.

Latin square graphs

Given a Latin square L, we define a graph whose vertices are the n^2 cells of the square, two vertices adjacent if they lie in the same row or the same column or contain the same symbol. This is a Latin square graph.

If L is the Cayley table of a group T, the graph admits T^3 (acting on rows, columns and symbols), as well as automorphisms of T and the symmetric group permuting the three types of object. If T is simple, the group generated by all of these is primitive, and is a three-factor diagonal group $D(T, 3)$.

Latin square graphs are strongly regular, but almost all have only the trivial group of automorphisms.

Transversals and orthogonal mates

A *transversal* is a set of cells, one in each row, one in each column, and one containing each letter.

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

In this case we can partition the cells into transversals:

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

Regarding the colours as an alphabet we see a second Latin square which is orthogonal to the first square, in the sense that each combination of letter and colour occurs precisely once.

Not all Latin squares have transversals. Consider the following square:

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Given a set of cells, one from each row and one from each column, the sum of the row indices is $0 + 1 + 2 + 3 = 2 \pmod{4}$. Similarly for the columns. Since each entry is the sum of its row and column indices, the entries sum to $2 + 2 = 0 \pmod{4}$. Thus the entries cannot be $\{0, 1, 2, 3\}$.

More generally, the Cayley table of a cyclic group of even order has no transversal.

Complete mappings

Let G be a group. A complete mapping of G is a bijective map $\phi : G \to G$ such that the map ψ defined by $\psi(x) = x\phi(x)$ is also a bijection.

Given a transversal in the Cayley table of G, define ϕ and ψ by the rule that $\phi(g)$ and $\psi(g)$ are the column label and entry of the transversal cell in row g. Then ϕ is a complete mapping as above.

Also, if ϕ and ψ are as above, then the array with (g, h) entry $g\psi(h)$ is a Latin square, which is an orthogonal mate for the Cayley table.

Thus the following are equivalent:

- the Cayley table of G has a transversal;
- the Cayley table of G has an orthogonal mate;
- G has a complete mapping.

The Hall–Paige conjecture

In 1955, Marshall Hall Jr and Lowell J. Paige made the following conjecture:

Conjecture

A finite group G has a complete mapping if and only if the Sylow 2-subgroups of G are trivial or non-cyclic.

They proved the necessity of their condition, and its sufficiency in a number of cases, including soluble groups and symmetric and alternating groups.
Hall was a well known group theorist and combinatorialist.
Paige was much less well known: he was a student of Richard Bruck, had 6 students at UCLA, and has 18 papers (including his thesis on neofields) listed on MathSciNet.

Proof of the Hall–Paige conjecture

The Hall–Paige conjecture was proved in 2009 by Stuart Wilcox, Anthony Evans, and John Bray.

Wilcox showed that its truth for all groups follows from its truth for simple groups, and proved it for groups of Lie type, except for the Tits group ${}^2F_4(2)'$. (The first two types, cyclic and alternating, are covered by Hall and Paige.)

Evans dealt with the Tits group and 25 of the 26 sporadic groups.

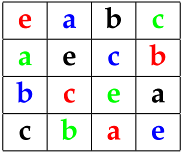
Bray dealt with the final group, the Janko group J_4.

The papers of Wilcox and Evans were published in the *Journal of Algebra* in 2009. But Bray's work has was not published at the time. (It has now appeared, together with the following discussion on synchronization, in the memorial issue of the *Journal of Algebra* for Charles Sims.)

Latin square graphs

Let L be a Latin square of order n, and Γ its Latin square graph. For $n > 2$, this graph has clique number n: any row, column or letter is a clique.

Also, the chromatic number is n if and only if A has an orthogonal mate:



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

Diagonal groups

We saw that 3-factor diagonal groups are automorphism groups of the Latin square graphs associated with Cayley tables of finite simple groups.

Proposition

The group $D(T, 3)$ is non-synchronizing.

Proof.

By Burnside's Transfer Theorem, a non-abelian simple group cannot have cyclic Sylow 2-subgroups. So by Hall–Paige, the Latin square graph of its Cayley table has clique number equal to chromatic number. □

With a little more effort, we have:

Theorem

The diagonal group $D(T, r)$ is non-synchronizing for $r \geq 3$.

Other properties

Knowledge of permutation groups has been used in studying other properties of transformation semigroups. Let S be a semigroup.

- an element $a \in S$ is regular if it has a quasi-inverse b, satisfying $aba = a$ (and, without loss of generality, also $bab = b$);
- S is regular if all its elements are regular;
- an element $e \in S$ is an idempotent if $e^2 = e$;
- S is idempotent-generated if all its elements are products of idempotents.

Transformation semigroups and permutation groups

A transformation semigroup S may have a permutation group G as its group of units; but whether or not this holds, it will have a permutation group G as its normaliser in the symmetric group.

Problem

How do properties of G influence S?

This problem goes back to the early days of semigroup theory. But little progress was made, because of lack of information about groups. The situation is different now. Here is a recent result I proved with João Araújo and Wolfram Bentz:

Theorem

Let S be a transformation monoid, G its normaliser in the symmetric group. If SG is regular, then S is regular.

The first breach in the wall

Things began with a paper of Araújo, Mitchell and Schneider in 2011. Which permutation groups G on Ω have the property that, for any transformation a on Ω which is not a permutation, one of the semigroups $\langle G, f \rangle$, $\langle G, f \rangle \setminus G$, or $\langle f^g : g \in G \rangle$ is regular, or idempotent generated?
It turns out that the answer is the same for all three semigroups, except that $\langle G, f \rangle$ is not idempotent-generated for non-trivial G, since the only idempotent in G is the identity.
For "regular", the necessary and sufficient condition is that G is the symmetric or alternating group or one of nine specific groups with degrees from 5 to 9 inclusive. For "idempotent-generated", (excluding the semigroup $\langle G, f \rangle$), the condition is that G is the symmetric or alternating group or one of three specific groups of degrees 5 or 6.
These theorems are significant extensions of earlier results of Howie, Symons, Levi and McFadden.

Regularity

The image of a transformation is as usual; its kernel is the partition of Ω into inverse images of points in the image.

If b is a quasi-inverse of a, then b must map the image of a to a transversal for the kernel of a. If a is regular in $\langle G, a \rangle$, it can be shown that there must be an element of G mapping the image of a to a transversal for the kernel of a.

Accordingly, we say that a permutation group G on Ω has the k-universal transversal property, or k-ut for short, if for every k-subset A and k-partition P of Ω, there is an element of G mapping A to a transversal for P.

It follows from what is said above that every rank-k map f is regular in $\langle G, f \rangle$ if and only if G has the k-ut. But much more is true …

The k-ut property and regularity

João Araújo and I showed the following result.

Theorem

Let $n \geq 5$ and $2 \leq k \leq n/2$. If G is a permutation group of degree n with the k-ut property, then G has the $(k-1)$-ut property.

This resembles the result of Livingstone and Wagner stating that under the same conditions a k-homogeneous group of degree n is $(k-1)$-homogeneous. However the proof is rather more complicated than theirs.
The implication of this is:

Corollary

Let $n \geq 5$ and $2 \leq k \leq n/2$. Suppose that G has the k-ut property, and let f be a transformation of rank k. Then $\langle G, f\rangle$ is regular.

The earlier analysis shows that elements of rank k in $\langle G, f\rangle$ are regular. But by the theorem, for $l < k$, G also has the l-ut property, and so elements of smaller rank are also regular.

The case $k = 2$

For $2 < k < n/2$, the k-ut property implies $(k-1)$-homogeneity with known exceptions; these groups are known, and in principle a classification of groups with k-ut can be done (though significant difficulties remain). However,

Theorem

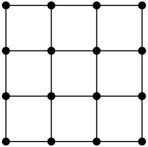
For $n > 2$, the 2-ut property is equivalent to primitivity.

For a G-orbit on 2-sets is the edge set of an (undirected) orbital graph; it contains a transversal to every 2-partition if and only if it is connected. Now G is primitive if and only if all orbital graphs are connected.

The Road Closure Conjecture

A primitive permutation group G on Ω has the road closure property if, given any orbit O of G on 2-sets, and any proper block of imprimitivity B for G in its action on O, the graph with vertex set Ω and edge set $O \setminus B$ is connected. In other words, if workmen dig up the edges in the block B, the orbital graph remains connected.

Non-basic primitive groups fail the to have the road closure property:



The automorphism group has two blocks of imprimitivity on edges, the horizontal and the vertical edges. If workers dig up all the vertical roads, the network becomes disconnected.

Idempotent generation

Idempotent generation of $\langle G, a\rangle \setminus G$ is stronger than regularity of $\langle G, a\rangle$. The case that has received most attention is $k = 2$. The connection is given by the following theorem.

Theorem

The permutation group G on Ω has the property that $\langle G, a\rangle \setminus G$ is idempotent-generated for any rank 2 map a if and only if G has the road closure property.

So we would like to know: which primitive groups have the road closure property?

The road closure property

Primitive groups with the road closure property must be basic. A primitive group which has an imprimitive normal subgroup of index 2 fails the road closure property. This accounts for most of the basic groups which fail to have the property. But there are others, known examples related to triality, and potential examples of almost simple groups with "novelty" maximal subgroups of certain types. Work to classify these is in progress. I hope it will be complete by the end of this INI programme.

References

J. Araújo and P. J. Cameron, Two generalizations of homogeneity in groups with applications to regular semigroups, *Trans. Amer. Math. Soc.* **368** (2016), 1159–1188.

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.

J. Araújo, J. D. Mitchell and C. Schneider, Groups that together with any transformation generate regular semigroups or idempotent generated semigroups, *J. Algebra* **343** (2011), 93–106.

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*, in press.