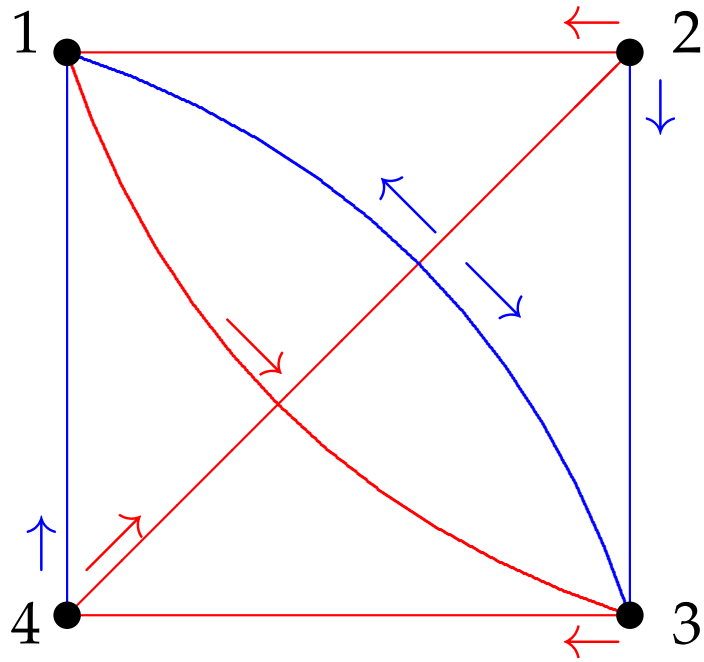
Diagonal groups, synchronization, and association schemes

Peter J. Cameron
University of St Andrews

London Algebra Colloquium
28 November 2019

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.

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.

Synchronization in the hierarchy

A permutation group G on Ω is primitive if it preserves no non-trivial equivalence relation on Ω; it is 2-homogeneous if it acts transitively on the 2-element subsets of Ω (equivalently, it preserves no non-trivial graph on the vertex set Ω). (Here a graph or equivalence relation is trivial if it is invariant under the full symmetric group.)

Theorem

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

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

The O'Nan–Scott Theorem

Here is a simple form of the O'Nan–Scott theorem which is adequate for our needs.

Theorem

Let G be a finite primitive permutation group on Ω. Then either

(a) *G preserves a Cartesian structure on Ω; or*

(b) *G is affine, diagonal or almost simple.*

I won't give all definitions. But type (a) preserve a Hamming graph, whose vertices are all words of length m over a finite alphabet of length A, two vertices joined if they differ in just one position.
This graph has clique number $|A|$: the set $\{(x, a_2, \ldots, a_m) : x \in A\}$ is a clique. It also has chromatic number $|A|$: take A to be an abelian group, and give $(a_1, \ldots, a_m)$ the colour $\sum a_i$. So type (a) are non-synchronizing.

O'Nan–Scott types

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 more difficult to define, so we'll approach them circumspectly.

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 $\{(g,g) : g \in S\}$) and the map $x \mapsto x^{-1}$. The result is the 2-factor diagonal group $D(T,2)$.
They noted that $|A_5| = 59+1$, $|\mathrm{PSL}(2,7)| = 167+1$, $|A_6| = 359+1$, $|\mathrm{PSL}(2,8)| = 503+1$, $|\mathrm{PSL}(2,11)| = 659+1$, ... (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.

The Classification of Finite Simple Groups

The biggest theorem in mathematics states:

Theorem

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, $n \geq 5$;*
- *a group of Lie type;*
- *a sporadic group (there are 26 of these).*

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.

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**

Three-factor diagonal groups

Recall the three classes of primitive groups not preserving a Cartesian structure in the O'Nan–Scott theorem: affine, diagonal and almost simple. 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. □

Diagonal groups with more socle factors

I didn't give you a definition of diagonal groups. But I did show you the two- and three-factor diagonal groups. The general case is an extension of this; the socle of a d-factor diagonal group is the direct product of d copies of a non-abelian finite simple group S, and it intersects the point stabiliser in the diagonal subgroup of S^d. The full diagonal group also contains the automorphism group of S, and the symmetric group S_d permuting the socle factors.

Theorem

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

A paper including Bray's final step in the proof of the Hall–Paige conjecture and this application to synchronization is to appear in the Sims memorial volume of the *Journal of Algebra*, hopefully next year.

Permutation group properties

I now turn to another place where diagonal groups arose.
It is possible to define many permutation properties in a uniform way. We say a structure on the set Ω is trivial if it is invariant under the symmetric group on Ω.
Now a permutation group is

- transitive if it preserves no non-trivial subset of Ω;
- primitive if (it is transitive and) it preserves no non-trivial partition of Ω;
- 2-homogeneous if it preserves no non-trivial (undirected) graph on Ω;
- 2-transitive if it preserves no non-trivial digraph on Ω
- synchronizing if it preserves no non-trivial graph on Ω with clique number equal to chromatic number.

You can take these as definitions; or, if you know other definitions, check that these statements agree with them.

Coherent configurations

A coherent configuration on a set Ω is a partition of $\Omega \times \Omega$ into classes whose relation matrices $A_1, \ldots, A_r$ satisfy the following conditions:

- $A_1 + \cdots + A_r = J$, the all-1 matrix;
- a subset of $A_1, \ldots, A_r$ sums to the identity I;
- $\{A_1, \ldots, A_r\}$ is closed under transposition;
- the span of $\{A_1, \ldots, A_r\}$ over $\mathbb{C}$ is closed under multiplication (that is, an algebra).

If G is a permutation group on Ω, then the partition of Ω^2 into G-orbits is a coherent configuration; the algebra mentioned in the fourth condition is the centraliser algebra of G.
The number r is the rank of the coherent configuration.

Association schemes

An association scheme is a coherent configuration in which the third condition in the definition is replaced by the stronger condition that all the matrices $A_1, \ldots, A_r$ are symmetric.
In this case it can be shown that the identity is one of the matrices A_i. So the pairs of distinct elements fall into $r-1$ classes; we speak of an $(r-1)$-class association scheme.
Note that "symmetrising" the matrices in a coherent configuration (replacing A_i and $A_i^\top$ by $A_i + A_i^\top$ if A_i is not symmetric) does *not* always produce an association scheme.
Association schemes arose in statistics, where statisticians deal with real data and covariance matrices are always symmetric.

Permutation groups

A coherent configuration or association scheme is trivial if $r = 2$, so that there are just two relations, equality and inequality.
Now, calling a permutation group CC-free if it preserves no non-trivial coherent configuration on Ω, we see that CC-freeness is equivalent to 2-transitivity.
However, the situation for association schemes is more complicated. We call the (transitive) permutation group G on Ω AS-free if the only G-invariant association scheme is trivial.
Thus, any 2-transitive (or even 2-homogeneous) permutation group is AS-free. But there are others.

Problem

Can the AS-free groups be classified?

Reductions

If G is transitive, a G-invariant partition gives rise to a divisible association scheme with two classes, "same part" and "different parts"; so an AS-free group must be primitive.
If G is non-basic, a G-invariant Cartesian structure gives rise to an association scheme, the Hamming scheme, where two points lie in the ith relation if their representing n-tuples disagree in exactly i positions. So a primitive AS-free group must be basic.
Thus a transitive AS-free group must be affine, diagonal or almost simple, by O'Nan–Scott.

AS-freeness

- Since affine groups have abelian transitive subgroups, it is easy to see that an affine group is AS-free if and only if it is 2-homogeneous.
- Diagonal groups with two socle factors preserve the conjugacy class association scheme on the simple factor, and so are not AS-free.
- With Sean Eberhard, I showed that diagonal groups with n socle factors ($n > 2$) are not AS-free either. But they have relatively large numbers of classes, typically one less than the number of paritions of n.The paper is published in the *Australasian Journal of Combinatorics*.
- As always, almost simple groups provide the mystery!

Almost simple groups

Based on computations by Faradžev, Klin and Muzichuk, we have the following.
The smallest almost simple AS-free group is the group $\mathrm{PSL}(3,3)$, acting on the right cosets of $\mathrm{PO}(3,3)$ (a subgroup isomorphic to S_4), with degree 234; this is also the smallest AS-free group which is not 2-homogeneous.
Other examples of almost simple AS-free groups are M_{12}, degree 1320; J_1, degree 1463, 1540 or 1596; and J_2, degree 1800.
The situation is not well understood! But with increased knowledge and computer power, it should be possible to explore this question further.

Bibliography

- 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; doi: 10.1016/j.jalgebra.2019.02.025
- P. J. Cameron and S. Eberhard, Association schemes for diagonal groups, *Australasian J. Combinatorics* **75** (2019), 357–364.