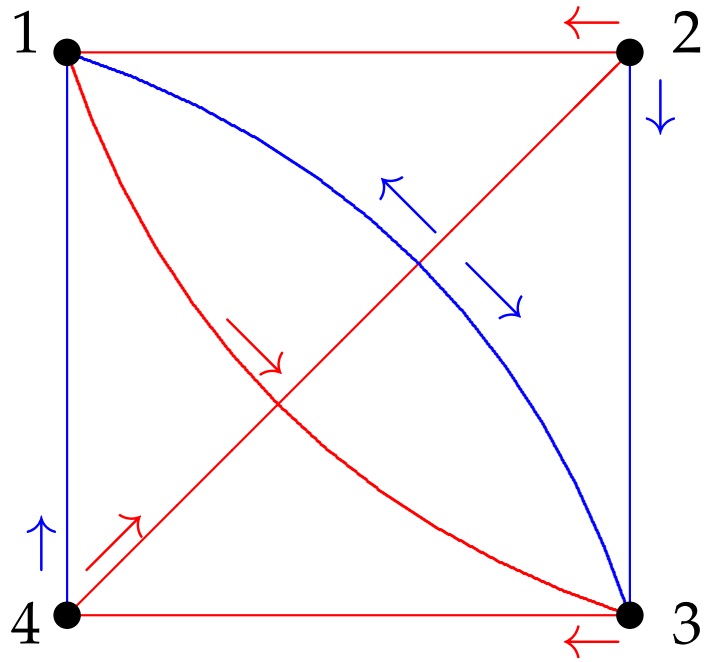
The Hall–Paige conjecture and an application

Peter J. Cameron
University of St Andrews

Algebra and Combinatorics seminar
30 January 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 I will postpone this. No diagonal group is known to be synchronizing (as far as I know).

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.

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 never been published.
So there is no proof of the conjecture in the literature.

Latin square graphs

Let A be a Latin square of order n. The corresponding Latin square graph Γ_A has vertices the cells of A, two vertices joined if they lie in the same row or column or contain the same entry in A.

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

Recall the three classes of primitive groups not preserving a Cartesian structure in the O'Nan–Scott theorem: affine, diagonal and almost simple. I didn't give you a definition of diagonal groups. Here is a non-standard definition of a subclass.

Let T be a non-abelian finite simple group. The diagonal group $D(T,3)$ is the automorphism group of Γ_A, where A is the Cayley table of T. It has socle T^3 (the factors acting on rows, columns and letters), and the quotient is the direct product of the outer automorphism group of T and the symmetric group S_3.

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

The diagonal groups $D(T,r)$ with larger numbers of socle factors are a little more difficult to define. But by a modification of the above argument, we obtain:

Theorem

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

I proved this in China last October. Armed with this, I talked to John Bray and persuaded him to send me his proof and to be an author of the paper. It is now available as arXiv 1811.12671. (It also contains results on $D(T,2)$ and on affine groups.)
I should add that John took the opportunity to make a thorough check on his earlier computations. At several points in the argument, different computations have been done so as to provide some checks.

John Bray's proof

I will finish by saying something about the computations. They depend on the following result of Wilcox:

Theorem

Let H be a subgroup of a finite group G. Suppose that

- *H has a complete mapping;*
- *there are bijections Φ, Ψ on the set $\mathcal{D}$ of double cosets HxH of H in G such that, for all $D \in \mathcal{D}$, $\Psi(D) \subseteq D\Phi(D)$.*

Then G has a complete mapping.

In particular, if there is a set of double coset representatives for H in G such that all (except possibly the representative of H) have order 3, then Wilcox's theorem applies, with $\Phi(D) = D$ and $\Psi(D) = D^{-1}$. (For, if $t^3 = 1$, then $t^{-1} = t^2 \in HtHtH$.)

The group $G = \mathrm{J}_4$ has order around 10^{20}. The smallest index of a proper subgroup is more than 10^8: rather large for the usual permutation group computations!
Several things work in our favour:

- J_4 has a matrix representation of degree 112 over the field of two elements, small enough for explicit calculations with elements;
- there is a permutation representation (on the set of 2A involutions) with degree a few billion, but if we identify the points with involutions, there are four dimensions of related subspaces in the 112-dimensional module which give complete invariants for the orbits on pairs (the orbital graphs);

- the rank of the permutation representation is 20; the two collapsed adjacency matrices for the orbital graphs of smallest degree can be calculated, and generate the entire adjacency algebra.

From the collapsed adjacency matrices we can verify Wilcox's hypothesis. But at an even earlier stage in the computation, double coset representatives are found which are all (except the identity) conjugates of a particular element of order 3.