Synchronization, diagonal structures, and the Hall–Paige conjecture

Peter J. Cameron
University of St Andrews

Rocky Mountain Algebraic Combinatorics Seminar
24 April 2020

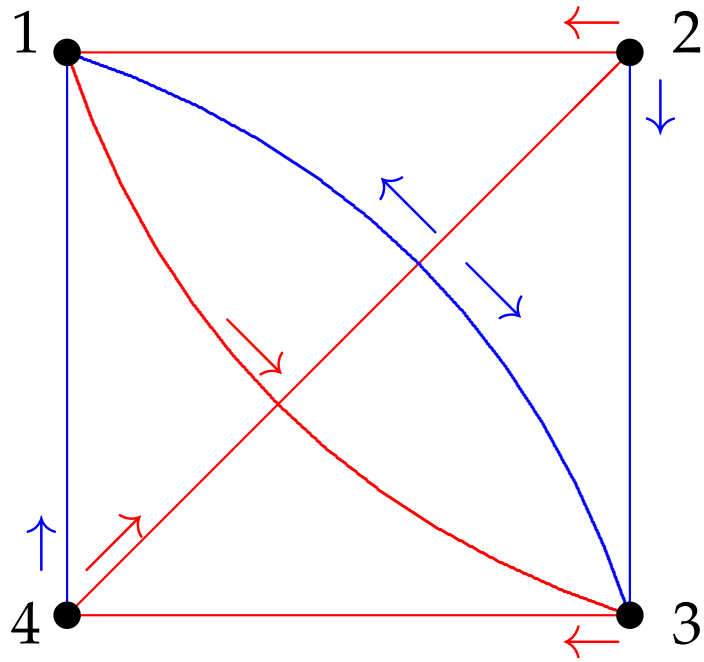
Welcome!

We live in strange times – I hope you are all surviving them! If things had been normal I would have given a talk rather like this one at the ALCOMA conference in Germany at the end of March.
But as it happens, things have moved on quite significantly since then!
The talk will be in three parts:

- a brief introduction to synchronization;
- a proof that one of the classes of primitive permutation groups, those of diagonal type with at least three factors, are non-synchronizing (this uses the truth of the Hall–Paige conjecture, which I will describe);
- a characterisation of the combinatorial structures preserved by the permutation groups of diagonal type (very recent, not written up yet!).

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.

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. The endomorphisms of a graph form a transformation monoid on the vertex set. If Γ is not a null graph, then $\mathrm{End}(\Gamma)$ is not synchronizing, since edges cannot be collapsed.

The obstruction to synchronization

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.

We saw that, if Γ has an edge, then $S \leq \mathrm{End}(\Gamma)$ is non-synchronizing.

Conversely, 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 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

If G is intransitive, then it preserves a complete graph on one of its orbits, which has clique number equal to chromatic number. So G is not synchronizing. Thus a synchronizing group is transitive.
A permutation group is imprimitive if it preserves a partition. Such a group preserves a disjoint union of complete graphs on the parts of the partition (which has clique number equal to chromatic number). So a synchronizing group is primitive.
A 2-homogeneous group preserves no non-trivial graph at all.

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.*
- *Neither of these implications reverses.*

The O'Nan–Scott Theorem

Here is a simplified form of the famous O'Nan–Scott Theorem.

Theorem

A primitive group is non-basic, affine, diagonal or almost simple.

Almost simple groups (those which have a unique minimal normal subgroup which is a non-abelian simple group) are the most mysterious. In the other three cases, we understand the maximal groups, not just as groups, but as permutation groups; I will describe them as we come to them.

Non-basic groups

Non-basic groups are contained in wreath products $S_q \wr S_n$, in their product action. The easiest way to specify the wreath product is as the automorphism group of the Hamming graph $H(n,q)$, as used in coding theory.

The vertices of $H(n,q)$ are all words of length n over an alphabet A of cardinality q, where $n, q > 1$. Two vertices are adjacent if they have Hamming distance 1. that is, they agree in all coordinates except one. (In coding theory, we would say that a single symbol error can transform one into the other.)

This graph has clique size q; the maximal cliques are the sets of words with fixed entries in all coordinates except the ith (for some i), and arbitrary entries in this coordinate.

Now assume that the alphabet A is an abelian group. Then the map taking a vertex $a_1 a_2 \ldots a_n$ to $a_1 + a_2 + \cdots + a_n$ is easily seen to be a proper colouring with q colours.

So non-basic groups are non-synchronizing.

Affine and almost simple groups

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.

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. The map ψ is an orthomorphism.
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, and ψ the corresponding orthomorphism.
Also, if ϕ and ψ are a complete mapping and corresponding orthomorphism, 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**

3-factor diagonal groups

We saw that 3-factor diagonal group $D(T,3)$ with T simple is the automorphism group of the Latin square graphs associated with Cayley table of T.

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. □

Partitions

To give our main theorem about the geometry of diagonal structures, it is necessary to work with partitions.
The set of all partitions of a set Ω is partially ordered by refinement: $P \leq Q$ if every part of P is contained in a part of Q.
With this ordering, partitions form a lattice:

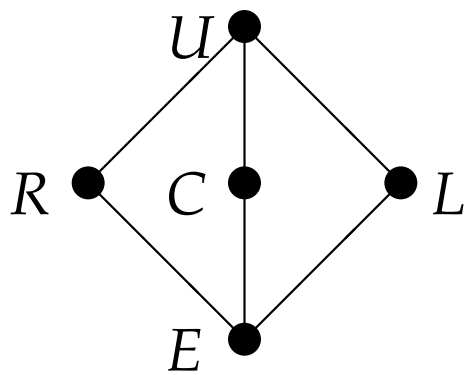
- the meet $P \wedge Q$ is the partition whose parts are all non-empty intersections of a part of P and a part of Q;
- the join $P \vee Q$ is the partition into connected components of the graph in which $a, b \in \Omega$ are joined if they lie in the same part of P or of Q.

Cartesian lattices

Let Ω be the set of all words of length n over an alphabet A.
For $I \subseteq \{1, \ldots, n\}$, let P_I be the partition of Ω into parts, in each of which the entries in coordinates in I take all possible values while the entries in the other coordinates are fixed.
The minimal (non-trivial) partitions have $|I| = 1$; their parts are the maximal cliques in the Hamming graph $H(n, A)$.
The map $I \mapsto P_I$ is an isomorphism from the Boolean lattice of subsets of $\{1, \ldots, n\}$ to a sublattice of the partition lattice on Ω.
We will call such a sublattice a Cartesian lattice. Its least and greatest elements are E and U.
In their book, Praeger and Schneider axiomatise Cartesian structures in terms of their maximal partitions; they call this a Cartesian decomposition of Ω.

Latin squares revisited

Latin squares can be interpreted in the following way. Let Ω be the set of cells of the square array. Then we have three partitions R, C, L of Ω corresponding to rows, columns, and letters of the Latin square. These, together with the universal partition U and the partition E into singletons, form a sublattice of the partition lattice. Its Hasse diagram looks like this:



Note the following important property: Any two of R, C, L generate a lattice which is a Cartesian lattice on Ω with $n = 2$ (a square grid).

Diagonal groups and their structures

I will briefly describe diagonal groups, leaving out details. Let m be an integer greater than 1, and T a group. Let $\Omega = T^m$, and define $m+1$ subgroups $T_0, \ldots, T_m$ as follows:

- For $1 \leq i \leq m$, T_i consists of m-tuples with the identity in all coordinates except the ith;
- T_0 is the diagonal subgroup consisting of elements with all coordinates equal.

Let Q_i be the partition into right cosets of T_i, for $0 \leq i \leq m$. The definition seems to give T_0 a special role, but it can be shown that the subgroups are all equivalent, and can be permuted arbitrarily by symmetries of the structure.

Any m of the partitions defined above are the minimal partitions in a Cartesian lattice. (This is clear for $Q_1, \ldots, Q_m$; for other choices it follows by symmetry.)
The diagonal structure is the union of these $m+1$ Cartesian lattices. It is not in general a lattice, but it is a join-semilattice, that is, closed under taking joins. Indeed, it is generated as join-semilattice by $Q_0, \ldots, Q_m$.
We call it a diagonal semilattice, and denote it $\mathcal{D}(T, m)$.
I now come to the main theorem, a very recent result of Rosemary Bailey, Cheryl Praeger, Csaba Schneider and me.

The main theorem

Theorem

Let m be an integer greater than 1. Let Ω be a set, and $Q_0, \ldots, Q_m$ partitions of Ω.
Suppose that any m of the $m+1$ partitions $Q_0, \ldots, Q_m$ are the minimal non-trivial partitions in a Cartesian lattice.

- *If $m = 2$, then the three partitions together with U and E form a Latin square on Ω.*
- *If $m > 2$, then there is a group T such that $Q_0, \ldots, Q_m$ are the minimal partitions in a diagonal semilattice $\mathcal{D}(T, m)$.*

Note that the group T emerges naturally from simple combinatorial assumptions! This is like the situation in projective geometry, where planes are "wild" but higher-dimensional spaces are coordinatised by skew fields.

A very brief sketch

For $m = 2$, we have a Latin square, as noted earlier; there is nothing more to be said, since any Latin square gives an example.

The main job is to prove the theorem for $m = 3$. Here we have four Latin squares, and we have to show that they are all isotopic to the Cayley table of the same group. The main tool is an old theorem of Frolov (1890): Any two rows and two columns of a Latin square define four entries. Suppose it happens that if, for two such choices, three of the four letters agree, then the fourth letter also agrees. Then the Latin square is isotopic to the Cayley table of a group.

The remainder of the proof goes by induction. We build smaller-dimensional quotients, show they satisfy the hypotheses of the theorem, and patch them together to give the result.

The diagonal graph

Given a diagonal structure $\mathcal{D}(T, m)$, we can define a graph $\Gamma(T, m)$ in which two vertices are adjacent if they lie in the same part of one of the minimal partitions Q_i.

For $m = 2$, this is the Latin square graph associated with the Latin square.

For higher values of m, it can be shown (again using the truth of Hall–Paige for m even) that it has clique number equal to chromatic number, and hence that the corresponding diagonal group is non-synchronizing.

These diagonal graphs may be of wider interest. In the case $|A| = 2$, they are the folded cubes, and are distance-transitive. They are surely worth further study ...

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
- C. E. Praeger and C. Schneider, *Permutation Groups and Cartesian Decompositions*, London Math. Soc. Lecture Notes **449**, Cambridge Univ. Press 2018; doi: 10.1017/9781139194006