Hall–Paige and synchronization

Peter J. Cameron
University of St Andrews

BCC, Birmingham
30 July 2019

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.

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. Bray's work is in a paper in the same journal this year, in the memorial volume for Charles Sims.

Synchronization

A finite deterministic automaton A is synchronizing if there is a word w (called a reset word) such that, when A reads w, its final state is always the same no matter where it started.
The transformations of the state set generated by reading all possible words form a monoid (a semigroup with identity), and A is synchronizing if and only if this monoid contains a transformation of rank 1 (that is, with image of size 1).
An endomorphism of a graph Γ is a transformation on the vertex set of Γ which maps edges to edges.
It is known that a monoid M is not produced by any synchronizing automaton if and only if there is no non-null graph Γ such that $M \leq \mathrm{End}(\Gamma)$. Moreover, we can assume that the clique number and chromatic number of Γ are equal.

Synchronizing permutation groups

A permutation group G on Ω is said to be synchronizing if, for any transformation f of Ω which is not a permutation, the monoid $\langle G, f \rangle$ contains a map of rank 1.

By the previous result, a permutation group G is non-synchronizing if and only if it is contained in the automorphism group of a non-trivial (that is, not complete or null) graph with clique number equal to chromatic number.

It is known that a synchronizing permutation group must be primitive (that is, preserve no non-trivial partition of Ω) and basic (that is, preserve no non-trivial Cartesian structure – or Hamming graph – on Ω).

Which basic primitive groups are synchronizing?

Latin square graphs

Let L be a Latin square. The associated Latin square graph has vertex set the set of cells of L, two vertices joined if they lie in the same row, or in the same column, or contain the same letter. If G ias a group, the automorphism group of the Cayley table of G is generated by the group $G \times G \times G$ (the factors acting on rows, columns and symbols), automorphisms of G (acting in the same way on all three sets of labels), and transformations permuting the sets of rows, columns, and symbols among themselves.

It can be shown that this automorphism group is primitive and basic if and only if G is a non-abelian simple group. Moreover, by the truth of the Hall–Paige conjecture, in this case the group is non-synchronizing. (The Sylow 2-subgroups of a non-abelian simple group cannot be cyclic, by a theorem of Burnside.)

The wider context

According to the O'Nan–Scott Theorem, there are three types of basic primitive groups, which I will not describe in detail:

- affine groups, groups of automorphisms of affine spaces;
- diagonal groups, of which the automorphism group of the Latin square graph treated above is an example;
- almost simple groups.

Using an extension of the arguments above, it can be shown that any diagonal group whose minimal normal subgroup is G^n with $n \geq 3$ and G simple is non-synchronizing. So one of the three cases is almost completely dealt with!