From automata to permutation groups

Peter J. Cameron, University of St Andrews

International Conference on Number Theory and Discrete Mathematics
RSET, Kochi, India, 12 December 2020
Marking 100 years since Srinivasa Ramanujan passed away

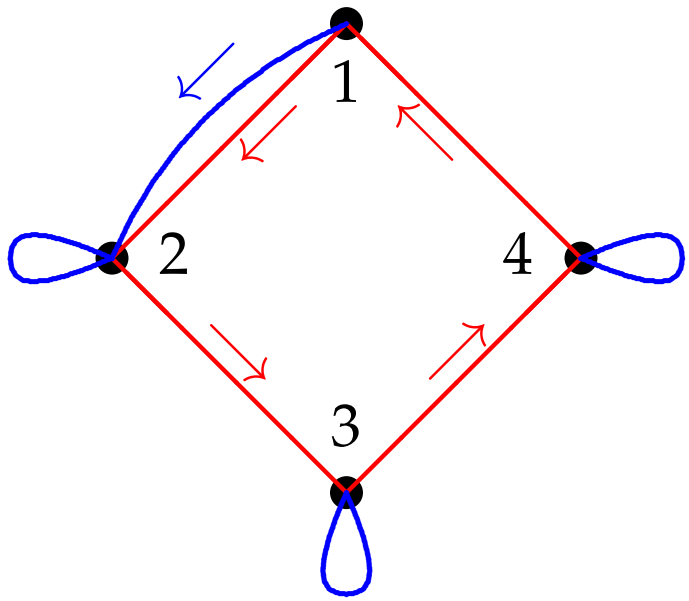
Outline

I intend to take you on a tour through some regions of discrete mathematics which, although very different, have deep interconnections. The talk will touch on

- automata and synchronization;
- permutation groups, primitive groups, O'Nan–Scott Theorem;
- partitions, characterisation of structures for products and diagonal groups;
- Latin squares, Cayley tables of groups, Hall–Paige conjecture and its proof;
- connections: synchronizing permutation groups, diagonal groups.

Automata

An automaton is a very simple machine. It has a set Ω of internal states; when it reads a letter from an alphabet A, it changes state according to a specified transition rule.
An automaton can be represented by an edge-coloured directed graph. The vertices are the states, the colours (RED and BLUE) the letters of the alphabet.



It is deterministic: one edge of each colour leaves each vertex.

Synchronization

An automaton can read a word (a sequence of letters) and undergo the composition of the corresponding transformations.
Algebraically we can regard an automaton as a transformation monoid (a set of transformations of Ω closed under composition and containing the identity) having a prescribed set of generators (the basic transitions).
An automaton is synchronizing if there is a word (called a reset word) such that reading this word brings us to the same state irrespective of the starting state.
In the preceding example, the word BRRRBRRRB is a reset word.

The Černý conjecture

One of the oldest open problems in automata theory (now half a century old) is the Černý conjecture:

Conjecture

If an n-state automaton is synchronizing, it has a reset word of length at most $(n-1)^2$.

Our example has four states and a reset word of length 9 (and none shorter). This example can be generalised to show that the conjecture is best possible for all n, replacing the square by an n-gon.
I am not going to show you a proof ...

Complexity

There is a simple polynomial-time algorithm to check whether an automaton A is synchronizing. We use the fact that A is synchronizing if and only if for any pair s, t of states, there is a word such that, on reading it from either s or t, the automaton ends in the same state.

This gives an upper bound of about cn^3 for the length of a reset word, with $c = 1/2$. The work of Frankl, Pin, and others has reduced the constant to about 0.1654, but the order of magnitude is still cubic.

There is no simple algorithm, as far as I know, to find the shortest reset word. Investigations show that automata needing long reset words are extremely rare; with finitely many exceptions, the only ones known to require length $(n-1)^2$ are those I showed earlier.

A characterization

The synchronization property of a monoid can be recognised graph-theoretically. Our graphs are now undirected simple graphs.

- The clique number $\omega(\Gamma)$ of a graph Γ is the size of the largest complete subgraph (all vertices adjacent).
- The chromatic number $\chi(\Gamma)$ is the minimum number of colours needed to colour the vertices so that adjacent vertices get different colours.
- An endomorphism of a graph is a map from vertices to vertices which carries edges to edges. The endomorphisms of a graph form a monoid.

Theorem

A transformation monoid S on Ω is non-synchronizing if and only if there is a non-null graph on Γ on Ω, with $\omega(\Gamma) = \chi(\Gamma)$, such that S is contained in the endomorphism monoid of Γ.

Permutation groups, transitivity, primitivity

A permutation group on a set Ω is a set G of permutations of Ω which is closed under composition and inversion and contains the identity permutation. The role of permutation groups in many parts of mathematics involving symmetry is well known.
A permutation group G is transitive on Ω if, given any two elements $\alpha, \beta \in \Omega$, there is an element of G which carries the first to the second. Said otherwise, G is transitive if there is no subset of Ω preserved by G apart from trivial cases, the empty set and the whole of Ω.
A transitive permutation group G is primitive on Ω if there is no partition of Ω preserved by G apart from trivial cases, the partition into singletons and the partition with a single part.
Many problems on permutation groups can be "reduced" to the study of primitive groups.

Double transitivity

A permutation group G on Ω is 2-transitive if, given two pairs of distinct elements of Ω, there is an element G which carries the first pair to the second. Said otherwise, G is 2-transitive if there is no G-invariant graph on Ω apart from the complete and null graphs.

2-transitive groups were the focus of much interest in the nineteenth century, when such remarkable objects as the Mathieu groups were discovered.

However, since the classification of finite simple groups (CFSG) was completed, early this century, we know the complete list of finite 2-transitive groups.

The O'Nan–Scott Theorem and CFSG

The celebrated O'Nan–Scott Theorem is the basis for applying CFSG to the study of (primitive) permutation groups. The terms in the theorem will be explained later.

Theorem

A finite primitive permutation group on Ω is contained in a group of one of the following types:

- *an affine group over a finite prime field;*
- *a wreath product in the product action;*
- *a diagonal group;*
- *an almost simple group.*

G is almost simple if $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S. Here is were knowledge of the simple groups is essential! This is provided by CFSG (which I will not state here) and much further work to understand these groups. Affine groups are groups of automorphisms of affine spaces.

Partitions

To understand the other two classes of primitive groups, we need to look at partitions. A partition of Ω is a set of pairwise disjoint non-empty subsets whose union is Ω.
The set $\mathbb{P}(\Omega)$ of all partitions of Ω is partially ordered by refinement: $P \preccurlyeq Q$ if every part of P is a subset of a part of Q.
With this order, $\mathbb{P}$ is a lattice: any two partitions P and Q have an infimum or meet $P \wedge Q$, whose parts are all non-empty intersections of a part of P and a part of Q, and a supremum or join $P \vee Q$, whose description I leave as an exercise.
A lattice of partitions is a set closed under meet and join and containing the two trivial partitions U (a single part) and E (parts are singletons). A join-semilattice is only required to be closed under join.

Structures for wreath product groups

Let A be an alphabet, and $\Omega = A^n$ the set of all words of length n over A. There is a map from the Boolean lattice of subsets of $\{1, \ldots, n\}$ to $\mathbb{P}(\Omega)$, which maps $I \subseteq \{1, \ldots, n\}$ to the partition in which a and b belong to the same part if and only if $a_j = b_j$ for all $j \notin I$. The image is a sublattice of $\mathbb{P}(\Omega)$ which we call a Cartesian lattice of dimension n.

The automorphism group of this lattice is the wreath product of the symmetric group on A with the symmetric group on $\{1, \ldots, n\}$, in its product action.

This can be viewed another way. The Hamming graph, familiar from coding theory, is the graph with vertex set Ω, in which words a and b are joined if they differ in exactly one coordinate. The minimal non-trivial elements of the Cartesian lattice coincide exactly with the maximal cliques of the Hamming graph, in which all but one coordinate is fixed and the remaining coordinate takes all values in A.

Counterexamples to a theorem of Cauchy

This was the title of a paper published by Neumann, Sims and Wiegold in the 1960s. Cauchy "proved" in the 19th century that a primitive permutation group whose degree is a prime number plus one is 2-transitive.
Neumann *et al.* noted that, if S is a non-abelian finite simple group, then the group $G = S \times S$, acting on S by the rule

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

is primitive but not doubly transitive. Now there are simple groups of orders $59+1, 167+1, 359+1, \ldots$
G is an example of a diagonal group.
Here is a challenge to the number theorists:

Question

Are there infinitely many counterexamples to Cauchy's Theorem of this form?

Latin squares: a first look

A Latin square of order n is usually regarded as an $n \times n$ array with entries from an alphabet of size n, such that each element of A 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**

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Ignore the second square for now

The Cayley table of a group G is an example: rows, columns and letters are indexed by elements of G, with the entry in row x and column y equal to the product xy. The square on the left is the Cayley table of the Klein group V_4.

There are huge numbers of Latin squares (at least $(n/c)^{n^2}$).

Almost all of them have trivial automorphism group.

Latin squares as partitions and graphs

Instead, we will regard a Latin square as a lattice of partitions. We take Ω to be the set of cells of the array; as well as E and U, there are three partitions R, C, L, into rows, columns and letters respectively. Note that any two of R, C, L generate a 2-dimensional Cartesian lattice.

In our previous example, if we number the squares from 1 to 16 in the usual way, the three partitions are

R: $\{1,2,3,4\}, \{5,6,7,8\}, \{9,10,11,12\}, \{13,14,15,16\}$;

C: $\{1,5,9,13\}, \{2,6,10,14\}, \{3,7,11,15\}, \{4,8,12,16\}$;

L: $\{1,6,11,16\}, \{2,5,12,15\}, \{3,8,9,14\}, \{4,7,10,13\}$.

We can construct a graph from a Latin square: the vertices are the cells, two vertices are adjacent if they lie in the same row or column or contain the same letter. This gives a prolific family of strongly regular graphs.

Here I pause to pay tribute to Sharadchandra Shankar Shrikhande, a mathematician who achieved much in this area, and who died earlier this year.

Diagonal groups

The definition of a diagonal group is a bit technical, so I will not give it here. For each choice of positive integer m and group T (finite or infinite) there is a diagonal group $D(T, m)$, of dimension m.

The groups we saw in the disproof of Cauchy's "theorem" are (more or less) diagonal groups with $m = 1$. I will not consider these further because, as in many geometric situations, the 1-dimensional case has no interesting geometry.

In the case $m = 2$, although most Latin squares have trivial automorphism group, the Cayley tables of groups have interesting automorphisms: in fact the automorphism group of one of these (or of its graph) is the diagonal group $D(T, 2)$.

On the next slide I give a higher-dimensional analogue, proved recently with Rosemary Bailey, Cheryl Praeger and Csaba Schneider. As often happens in geometry, there is a plethora of 2-dimensional examples (the Latin squares), but for higher dimensions an algebraic structure (a group) emerges naturally.

Characterization of diagonal structures

Here is the main theorem:

Theorem

Let m be an integer greater than 1. Let $Q_0, Q_1, \ldots, Q_m$ be a set of $m+1$ partitions of a set Ω, with the property that any m of them are the minimal elements of an m-dimensional Cartesian lattice. Let S be the join-semilattice generated by $Q_0, \ldots, Q_m$.

- *If $m = 2$, then S is the lattice form of a Latin square, unique up to "isotopism"; conversely, any Latin square arises in this way.*
- *If $m > 2$, there is a group T, unique up to isomorphism, so that the automorphism group of S is the diagonal group $D(T, m)$; every diagonal group arises in this way.*

We call S in the second part the diagonal semilattice of dimension m defined by G, denoted $\mathcal{D}(T, m)$.

The diagonal graph

Just as a Cartesian lattice is associated with a Hamming graph, so there is a graph associated with a diagonal structure, the diagonal graph $\Gamma_D(T, m)$, with the same automorphism group $D(T, m)$.
The vertex set is Ω, and we join two vertices if they lie in a part of one of the partitions Q_i.
Apart from a few small cases, the graph is like the Hamming graph in that the parts of the Q_i are maximal cliques in the graph; so the graph and the semilattice determine each other.
Two cases are familiar:

- for $m = 2$, the diagonal graph is the Latin square graph we met earlier.
- for $T = C_2$, the graph is the folded cube: take the 1-skeleton of the m-dimensional cube, and add edges joining antipodal vertices.

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.

The Hall–Paige conjecture

Proposition

The following are equivalent for a finite group G:

- *the Cayley table of G has a transversal;*
- *the Cayley table of G has an orthogonal mate;*
- *G has a complete mapping, a bijection $\phi : G \to G$ such that the map $\psi : G \to G$ given by $\psi(G) = g \cdot \phi(G)$ is also a bijection.*

In 1955, Hall and Paige conjectured the following, and proved the necessity, and the sufficiency in some cases. The proof was completed in 2009 by Wilcox, Evans and Bray using CFSG.

Theorem

A group G has a complete mapping if and only if either the order of G is odd, or the Sylow 2-subgroups of G are not cyclic.

Since a non-abelian finite simple group has even order and non-cyclic Sylow 2-subgroups, any such group has a complete mapping.

Synchronization of permutation groups

I now return to the problem of synchronization. Recall that a transformation semigroup S on Ω is synchronizing if it contains an element whose image is a single point of Ω. We saw that S is non-synchronizing if and only if it is contained in the endomorphism monoid of a non-trivial graph with clique number equal to chromatic number.

A permutation group can never be synchronizing in this sense, so we redefine the concept: a permutation group G on Ω is synchronizing if, for any map $f : \Omega \to \Omega$ which is not a permutation, the transformation monoid S generated by G and f is synchronizing in the earlier sense.

It can be shown that G is non-synchronizing if and only if it is contained in the automorphism group of a non-trivial graph with clique number equal to chromatic number. Hence:

Theorem

Every 2-transitive group is synchronizing; and every synchronizing group is primitive.

Which primitive groups are synchronizing?

Recall the O'Nan–Scott theorem: a primitive group is contained in a group which is affine, wreath product, diagonal or almost simple.
Affine and almost simple groups may or may not be synchronizing; work is still ongoing. However, for the other two classes, we are in good shape:

- A wreath product is non-synchronizing, since the Hamming graph Γ has $\omega(\Gamma) = \chi(\Gamma)$.
- The diagonal graph $\Gamma_D(T, m)$ has clique number equal to chromatic number if m is odd or if T satisfies the conditions of the Hall–Paige conjecture (i.e. odd order or non-cyclic Sylow subgroups). In particular, for every non-abelian simple group T and $m > 1$, the diagonal group $D(T, m)$ is non-synchronizing. Since these are the only primitive diagonal groups, this class is settled, apart from the case $m = 1$, where hard problems remain.

How hard is testing synchronization?

We saw that the class of synchronizing permutation groups lies between the well-known classes of primitive and 2-transitive groups. Members of both these classes can be recognised in polynomial time.

Question

Is there a polynomial-time algorithm to test whether a permutation group is synchronizing?

Since our current test involves clique numbers and chromatic numbers of graphs, both hard problems, no such algorithm is currently known. But it may be that, with the help of CFSG and the O'Nan–Scott Theorem, such a test can be found.

. . . for your attention.