From synchronization, to permutation groups, to graphs

Pablo Spiga

pablo.spiga@unimib.it

10^{th} S♡nian conference on graph theory

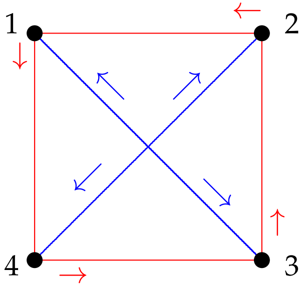
Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

We can force the machine to make any desired sequence of transitions (each transition being a mapping from the set of states to itself).

We can represent an automaton as an edge-coloured directed graph, where the vertices are the states, and the colours are the transitions. We require that the graph has exactly one edge of each colour leaving each vertex.

An example

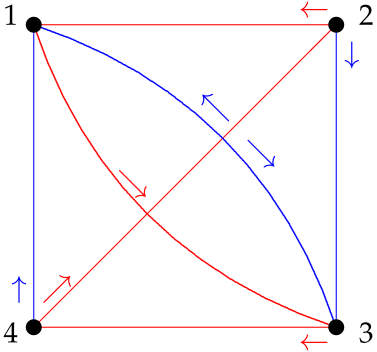


Synchronization

Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it.

A reset word is a sequence of transitions which take the automaton from any state into a known state; in other words, the composition of the corresponding transitions is a constant mapping.

An example

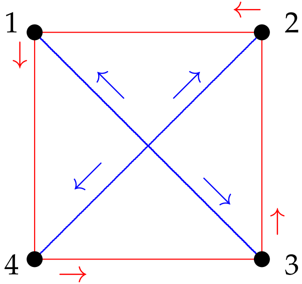


You can check that (Blue, Red, Blue, Blue) is a reset word which takes you to state 3 no matter where you start.

- $1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 3$
- $2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1 \longrightarrow 3$
- $3 \longrightarrow 1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 3$
- $4 \longrightarrow 1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 3$

This is not always possible!

For instance, here the two transitions *Blue* and *Red* are both permutations.



The road colouring problem

A directed graph with constant out-degree can be edge-coloured to produce an automaton.

Problem

Suppose that D is a directed graph in which all vertices have out-degree d. Then the edges of D can be coloured with d colours to produce an automaton with a reset word if and only if D is strongly connected and the greatest common divisor of the cycle lengths in D is 1.

This was the road colouring conjecture until it was proved by Avraham Trahtman in 2009.

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

Problem

Suppose that an n-vertex automaton has a reset word. Show that it has one of length at most $(n-1)^2$.

This is the Černý conjecture, and is still open. If true, the bound would be best possible.

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A permutation group G on a set Ω is said to be synchronizing if, whenever $f : \Omega \to \Omega$ is a mapping which is not a permutation, the semigroup generated by G and f contains a reset word (a constant mapping).

Which permutation groups are synchronizing?

Recap on permutation groups

Let G be a permutation group on a set Ω.

- G is transitive if the only subsets preserved by G are the empty set and the whole of Ω (that is, the trivial ones),
- G is primitive if the only partitions preserved by G are the partitions into singletons and the partition with only one part (that is, the trivial ones),
- G is 2-homogeneous if the only graphs preserved by G are complete graph and the empty graph (that is, the trivial ones),
- G is 2-transitive if the only directed graphs preserved by G are complete graph and the empty graph (that is, the trivial ones).

Synchronizing groups

Synchronization (for permutation groups) can be reformulated in more group-theoretic terms.

Proposition

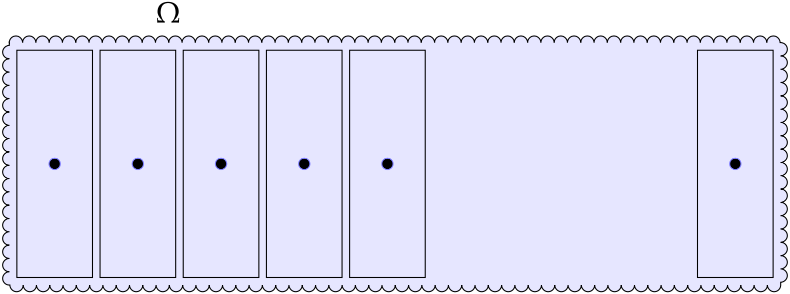
A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial partition π of Ω and a subset Δ of Ω such that, for all $g \in G$, Δg is a section (of transversal) of π.

In this case, the pair π, Δ is said to be a non-trivial section-regular partition for G.

Corollary

A synchronizing group is primitive.

For if there is a G-invariant partition π, then any section of π has the required property.



Equivalent definitions of synchronization

For a permutation group G on Ω, the following are equivalent

- G is non-synchronizing,
- G has a non-trivial section-regular partition,
- there is a non-trivial graph Γ having vertex set Ω, with G contained in its automorphism group, such that the clique number and chromatic number of Γ are equal.

A graph is said to be weakly perfect if its clique number and chromatic number are equal; then G is synchronizing if it preserves no non-trivial weakly perfect graph on Ω.

Separating groups

Let G be transitive on Ω, with $|\Omega| = n$. Let Γ and Δ be subsets of Ω, with $|\Gamma| = k$, $|\Delta| = l$.

Lemma

If $kl < n$, then there exists $g \in G$ with $\Gamma \cap \Delta g = \emptyset$.

We say that G is separating if the same conclusion holds when $kl = n$.

Proposition

A separating group is synchronizing.

For if G is non-synchronizing, and Γ is a part of a partition π for which (π, Δ) witnesses the non-synchronization, then by assumption $|\Gamma \cap \Delta g| = 1$ for all $g \in G$.

- G is non-separating if and only if there is a non-trivial graph Γ having vertex set Ω with G contained in the automorphism group, such that the product of the clique number and independence number of Γ is equal to $|\Omega|$.

Separation and synchronization

Since synchronizing groups are primitive, the obvious first step is to check primitive groups of small degree (up to a few hundred) for these properties. MAGMA and GAP contain lists of these groups. But the checking is non-trivial.

In particular, we only know a tiny handful of permutation groups which are synchronizing but not separating; it would be interesting to find out why this property is so rare.

Some of the examples come from finite geometry (involving properties of ovoids and spreads in polar spaces), but all others appear to be "sporadic". [For instance the symmetric group of degree 10 acting on 4-sets shows a peculiar behaviour.]

Some examples: classical groups on polar spaces

We have a vector space V over $GF(q)$ on which there is a non-degenerate alternating bilinear, Hermitian, or quadratic form. The classical group is the group of isometries of the form.

The polar space associated with the form is the geometry whose points are the 1-dimensional subspaces of V and whose lines, planes, etc. are the 2-, 3-, etc.-dimensional subspaces on which the form vanishes.

A classical group is a rank 3 group on the polar space: the only two G-invariant graphs are the collinearity graph (in which two points are adjacent if they lie on a line of the polar space) and its complement.

An ovoid is a set of points which meets every maximal subspace in a single point, i.e. it is a coclique of maximum possible size in the collinearity graph.

A spread is a partition of the point set into maximal subspaces, i.e. it is a colouring of the complement of the collinearity graph.

Proposition

Let G be a classical group acting on the points of its polar space. Then G is non-synchronizing if and only if there exists an ovoid and a spread, or there exists a partition of the polar space into ovoids.

Deciding which polar spaces have ovoids and spreads has been studied by finite geometers for many years (the problem goes back to Segre), and it is far from a complete solution.

Groups of diagonal type

Understanding which primitive groups of diagonal type are synchronizing turns out to be equivalent to the Hall-Paige conjecture.

A complete mapping on a group G is a bijective function $\phi : G \to G$ such that the function $\psi : G \to G$ given by $\psi(g) = g\phi(g)$ is also a bijection. (A complete mapping is needed to construct a section of a suitable partition of the domain of a primitive group of diagonal type.)

The Hall–Paige conjecture asserts that a finite group has a complete mapping if and only if its Sylow subgroups are not cyclic.

The Hall-Paige conjecture has fallen silent for many years, but the connection to synchronizing groups has spurred some recent interest.

The k-universal transversal property

A permutation group G on Ω has the k-universal transversal property (or k-ut, for short) if the following holds: given any k-subset A of Ω, and any partition π of Ω with k parts, there is an element $g \in G$ such that A^g is a transversal for π.

A semigroup S is regular if, given any $a \in S$, there is an element $b \in S$ such that $aba = a$ and $bab = b$.

Proposition

Let G be a permutation group on Ω. The following are equivalent:

- *G has the k-ut property,*
- *if $f : \Omega \to \Omega$ is any map of rank k (that is, $|\mathrm{Im}(f)| = k$), then the monoid $\langle G, f \rangle$ is regular.*

The 2-ut property is equivalent to primitivity (via Higman's theorem). Therefore, 2-ut groups cannot be classified.

Reminiscent the Livingston-Wagner theorem, one can prove that k-ut implies $(k-1)$-ut for $n \geq 2k$. Moreover, k-ut implies the $(k-1)$-homogeneity. In particular, except for a few unresolved cases, using the classification of the 2-homogeneous groups, the groups satisfying the k-ut property are classified when $k \geq 3$.

The unresolved cases involve

- some affine linear groups, where the classification of k-ut groups is related to a number-theoretic question for affine linear groups,
- some projective special linear groups of rank 1 and
- the Suzuki groups.

The k-idemponent generation property

An idempotent of S of a semigroup is an element e satisfying $e^2 = e$.

A permutation group G on Ω has the k-idempotent generation property (or k-id, for short) if the following holds: for any map $f : \Omega \to \Omega$ of rank k, the semigroup $\langle G, f\rangle \setminus G$ is generated by idempotents.

Since k-id implies k-ut, we have a nearly complete description of the groups satisfying the k-id property, when $k \geq 3$.

The case $k = 2$ has inspired, in my opinion, the most beautiful conjecture on primitive groups.

En route to the road closure conjecture

The following in taken from Peter Cameron's blog.

The University of St Andrews is installing a biomass boiler, to provide hot water to heat University buildings, on the old paper mill site at Guardbridge. The water has to be piped four miles to St Andrews, and this big job has involved a lot of road closures this year.

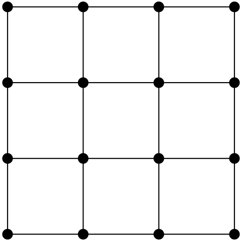
However, it was always possible to get through, by taking a sufficiently devious route.

This is a metaphor for the problem that Joao Araújo and I are thinking about at the moment.

Let G be a transitive permutation group on Ω. The orbital graphs for G are the graphs with vertex set Ω, whose edge sets are orbits of G on the set of 2-subsets of Ω. These graphs are vertex-transitive and edge-transitive. Moreover, if G acts primitively on the vertex set Ω, then every orbital graph is connected.

The action of G on the set $\mathcal{O}$ of edges of an orbital graph may or may not be primitive. For each maximal block of imprimitivity B in this action, consider the graph obtained by removing the edges in B from $\mathcal{O}$. This graph may or may not be connected.

Take G to be the automorphism group of the $m \times m$ grid (the graph with edges joining pairs of vertices in the same row or in the same column of the grid). Then G acts primitively on vertices, but not on edges; the edges fall into two blocks of imprimitivity, the horizontal edges and the vertical edges. If we dig up all the vertical edges, then it is not possible to travel from one row to another; the resulting graph is disconnected.



Let us say that a transitive permutation group G has the road closure property if, for every orbital graph $(\Omega, \mathcal{O})$ and every maximal block of imprimitivity for G acting on $\mathcal{O}$, the graph $(\Omega, \mathcal{O} \setminus B)$ is connected.

A group has the road closure property if and only if it has the 2-id property.

Which groups have this property?

If G is imprimitive, then it does not have the road closure property.

If G is primitive but not basic (this means that Ω has the structure of a Cartesian power which is preserved by G, so that G is embedded in a wreath product), then it does not have the road closure property.

If G is primitive and basic, but has an imprimitive normal subgroup of index 2, then it does not have the road closure property. This includes groups of automorphisms and dualities of various incidence structures, acting on the set of flags of the structure: such structures include points and hyperplanes (or points and complements of hyperplanes) in projective spaces, points and lines in some generalised polygons, points and blocks in some symmetric designs.

There is another class of examples, built using the wonderful geometric phenomenon of triality for the quadrics associated with split quadratic forms in 8-dimensional space. The smallest example is a primitive group of degree 14175.

There are further examples, a sporadic example arising from $\mathrm{PSU}_3(5)$, and an infinite family of examples arising from the Aschbacher class $\mathcal{S}$ embedding of $\Omega_8^+(2)$ in $\mathrm{P}\Omega_8^+(p)$, where $p \equiv \pm 3 \pmod 8$.

There are exponentially many maps of rank 2, since we have to choose an arbitrary subset of the domain to map to the first image point. The advantage of our characterisation of the road closure property in combinatorial terms is that the calculation involved is much smaller. There is at most a linear number of orbital graphs; the numbers of maximal blocks are hopefully not too large; and connectedness is very fast to check. Indeed, some of our intermediate results mean that certain classes of groups (non-basic groups, 2-homogeneous groups, groups of prime degree) don't even need to be checked.

Is the number of maximal blocks of imprimitivity through a point for a transitive group G of degree *n* bounded above by a polynomial of degree *n*? Find the best bound!

A special case of this problem has a long history. In 1961, Tim Wall conjectured that the number of maximal subgroups of a finite group of order n is not more than n. Now any group has a regular action (as in Cayley's theorem), which is transitive; the blocks of imprimitivity containing the identity are just the maximal subgroups. So Wall's conjecture is a special case of the problem above when the permutation group is regular. Wall's conjecture was disproved by the participants in an AIM workshop a few years ago, but it is thought to be very nearly true; in particular, Martin Liebeck, Laszlo Pyber and Aner Shalev showed that the number of maximal subgroups is bounded by a constant times the 3/2 power of the group order.

Theorem (Moscatiello, Lucchini, P.S)

A transitive permutation group of degree n has at most an $n^{3/2}$ maximal systems of imprimitivity.