Group theory problems from semigroups and automata

Peter J. Cameron
University of St Andrews

Groups, Geometry and Representations
Dan Segal and Aner Shalev birthday conference
Oxford, September 2018

A little (maybe biased) history

This is roughly the story as João Araújo told it to me.

In the early days of semigroup theory, the practitioners thought that the group of units of a semigroup would have a big influence on its structure. So they went along to their friendly neighbourhood group theorists with their questions.

“That’s much too hard,” said the group theorists.

So the semigroupists went away and played with idempotents instead.

But now we know rather more about groups (especially finite groups), so perhaps it is time to revisit some of these questions.

Permutation groups and transformation semigroups

I will only consider the finite case in this lecture.

Let Ω be a finite set. A transformation semigroup is a collection of maps from Ω to itself which is closed under composition. If it is also closed under inversion and contains the identity, then it is a permutation group.

We can always, without loss, assume that our transformation semigroup contains the identity (so that it is a transformation monoid. The invertible elements (units) in a transformation monoid form a permutation group.

Our goal is to relate the structure of the monoid to that of its group of units.

What if there are no permutations?

Perhaps our transformation semigroup S contains no permutations …

But the normaliser of S in the symmetric group is a permutation group:

$$G = N_{S_n}(S) = \{g \in S_n : g^{-1}Sg = S\}.$$

Now $\langle S, G\rangle = SG$ is a transformation semigroup containing G, and it is equal to the product SG if S contains a permutation, and $SG \cup G$ otherwise.

Now, S is regular (see below) if and only if $\langle S, G\rangle$ is regular. (The proof of this is not trivial.) So for regularity, we lose nothing by assuming that S contains a group of permutations. However, this can fail for other properties such as idempotent generation.

Semigroup properties

The semigroup property I am most interested in is regularity.
An element x of a semigroup S is regular if it has a “von Neumann inverse” or “generalised inverse” $y \in S$, and element satisfying $xyx = x$.
Note that, if y exists, then the element $z = yxy$ satisfies $xzx = x$ and $zxz = z$, so x and z are generalised inverses of each other.
The semigroup S is regular if each of its elements is regular.
Another property is idempotent generation. An element $e \in S$ is idempotent if $e^2 = e$. Many important types of semigroup are generated by their idempotents. However, the only idempotent in a group is the identity. So we ask whether, given a transformation semigroup S satisfying $S \cap S_n = G$, the sub-semigroup $S \setminus G$ is idempotent-generated.
To finish, I will say something about synchronization.

Regularity

It is clear that, if S is a transformation semigroup whose permutation group is G, then S is regular if and only if, for any element $t \in S \setminus G$, the semigroup $\langle G, t \rangle$ is regular.
So we pose our general question:

Problem

For which pairs (G, t), where G is a permutation group on Ω and t a transformation on Ω which is not a permutation, is it the case that $\langle G, t \rangle$ is regular?

This problem is not yet within reach. But over the last decade, substantial progress has been made on this problem, by João Araújo with various co-authors.

Classical results

The following result of Levi and McFadden in 1994 is the prototype for results of this kind. Let S_n and T_n denote the symmetric group and full transformation semigroup on $\Omega := \{1, 2, \ldots, n\}$.

Theorem

Let $t \in T_n \setminus S_n$, and let S be the semigroup generated by the conjugates $g^{-1}tg$ for $g \in S_n$. Then

- *S is idempotent-generated;*
- *S is regular;*
- *$S = \langle t, S_n \rangle \setminus S_n$.*

In other words, if $G = S_n$, then we are in the nicest possible situation!
An analogous result was also shown in the case where G is the alternating group A_n by Levi in 1996.

The first breach in the wall

In 2011, Araújo, Mitchell and Schneider showed:

Theorem

Let G be a subgroup of S_n.

- $\langle g^{-1}ag : g \in G\rangle$ *is regular for all* $a \in T_n \setminus S_n$ *if and only if* $G = S_n$ *or* $G = A_n$ *or* G *is one of eight specific groups of low degrees.*
- $\langle g^{-1}ag : g \in G\rangle$ *is idempotent-generated for all* $a \in T_n \setminus S_n$ *if and only if* $G = S_n$ *or* $G = A_n$ *or* G *is one of three specific groups of low degrees.*

When I learned about this theorem, I was reminded of a result in permutation group theory.

Set-transitive permutation groups

A permutation group $G \leq S_n$ is *k*-homogeneous or *k*-set transitive if it acts transitively on the set of *k*-element subsets of $\{1, \ldots, n\}$. The group G is set-transitive if it is *k*-set transitive for all k with $0 \leq k \leq n$.

In their 1944 book *Theory of Games and Economic Behavior*, von Neumann and Morgenstern asked the question: Which permutation groups are set-transitive? (An *n*-player game is obviously "fair" if its automorphism group is set-transitive – no collection of players can have an advantage over any equinumerous collection.)

The third edition of the book in 1953 carried a note that the problem had been solved by C. Chevalley. However, the first published solution was by Beaumont and Peterson in the *Canadian Journal of Mathematics* in 1955:

Theorem

The permutation group $G \leq S_n$ is set-transitive if and only if G is S_n or A_n or one of four other groups of small degrees.

Livingstone and Wagner

In 1964, Donald Livingstone and Ascher Wagner published a remarkable paper on k-homogeneous permutation groups. Noting that a subgroup of S_n is k-homogeneous if and only if it is $(n-k)$-homogeneous, there is no loss of generality in assuming that $k \leq n/2$. They showed:

Theorem

Let G be a k-homogeneous subgroup of S_n, with $2 \leq k \leq n/2$. Then

- *G is $(k-1)$-homogeneous;*
- *G is $(k-1)$-transitive;*
- *if $k \geq 5$, then G is k-transitive.*

Here a permutation group G is k-transitive if any k-set can be mapped to any other k-set, *in any possible order*, by some element of G. Clearly this is formally stronger than k-homogeneity, which only asks that we can map the first set to the second in some order.

Livingstone and Wagner

The first part of this theorem, that k-homogeneity implies $(k-1)$-homogeneity for $k \leq n/2$, is proved by a simple argument using character theory of the symmetric group. The argument can be translated into pure combinatorics and substantially generalised, and connects to many other topics such as graph reconstruction and Ramsey-type theorems, as well as having infinite versions.

Subsequently, Kantor determined the k-homogeneous but not k-transitive groups for $k = 2, 3, 4$. Moreover, from the Classification of Finite Simple Groups together with work by many authors, it is possible to give a complete list of the k-transitive groups for $k \geq 2$.

Regularity and the ut property

Suppose that t is a transformation of Ω. The kernel of t is the equivalence relation $\equiv$, where $x \equiv y$ if $xt = yt$, or the corresponding partition. The number of parts of the kernel is equal to the rank of t, the cardinality of the image.

Let g be a permutation which maps the image of t to a transversal for the kernel of t. Then gt permutes the image of t, and so $(gt)^m$ is an idempotent with image equal to that of t, for some m. Hence $t(gt)^m = t$, and t is regular in $\langle g, t \rangle$. The converse is also true.

We say that the permutation group G has the k-universal transversal property, or k-ut for short, if, for any k-set A and k-partition P, some element of G maps A to a transversal for P.

Thus, if G has the k-ut property, then if t is any rank k map, then t is regular in $\langle G, t \rangle$ – so any rank k map in this semigroup is regular.

The downward step

João Araújo and I showed the analogue of Livingstone and Wagner part 1:

Theorem

For $k \leq n/2$, if G has the k-ut property, then it has the $(k-1)$-ut property.

It follows that, if G has the k-ut property for $k \leq n/2$, and t is a map of rank k, then the semigroup $\langle G, t \rangle$ is regular. For we saw that all its rank k elements are regular; hence all the rank $k-1$ elements are regular, and so on down.

We very much wanted a simple proof of this theorem along the lines of the Livingstone–Wagner proof. However, we failed to find this; our proof involves a near-classification of such permutation groups, and makes use of the Classification of Finite Simple Groups (CFSG).

Problem

Find a simpler proof!

Tools

Of course, we use results about permutation groups, and CFSG. We also use a variety of combinatorial tools, including

- Ramsey's theorem, and some specific Ramsey numbers;
- properties of vertex-transitive graphs, including Watkins' theorem on connectivity, and the result of Little, Grant and Holton on the existence of near 1-factors.

Typically the combinatorics excludes non-2-homogeneous groups, then the group theory takes over.

Regularity and k-ut

To summarise, our result is as follows:

Theorem

For a permutation group G of degree n and a positive integer $k \leq n/2$, the following are equivalent:

- *for all rank k maps t, t is regular in $\langle G, t\rangle$;*
- *for all rank k maps t, t is regular in $\langle g^{-1}tg : g \in G\rangle$;*
- *for all rank k maps t, $\langle G, t\rangle$ is regular;*
- *for all rank k maps t, $\langle g^{-1}tg : g \in G\rangle$ is regular;*
- *G has the k-ut property.*

We have a complete classification of these groups for $k \geq 5$, and nearly complete results for $k = 3, 4$.

The case $k = 2$

No such classification is possible for $k = 2$, for a simple reason:

> *the 2-ut property is equivalent to primitivity.*

For the images of a 2-set under G are the edges of an orbital graph for G; and 2-ut says that every orbital graph has an edge crossing every 2-partition, i.e. is connected.
But, as Donald Higman first observed, primitivity is equivalent to the connectivity of all orbital graphs.

The existential transversal property

We considered groups G for which $\langle G, t\rangle$ is regular for all rank k maps t. The next step towards our ultimate goal is to determine the groups G for which there exists a k-set A such that $\langle G, t\rangle$ is regular for all maps t with image A.

The permutation group G has the k-existential transversal property (for short, k-et) if there is a k-set A, the witnessing set, such that, for any k-partition P, there exists $g \in G$ such that Ag is a transversal for P.

If G has k-et, and the image of t is the witnessing set, then as before we find that all elements of rank k in $\langle G, t\rangle$ are regular.

The strategy

From the last observation, we obtain:

Theorem

Suppose that G satisfies k-et (with witnessing set A) and $(k-1)$-ut, where $k \leq n/2$. Then, for any map t with image A, $\langle G, t \rangle$ is regular.

Unfortunately, k-et does not imply $(k-1)$-ut, or even $(k-1)$-et. But, remarkably, the last implication fails for only two permutation groups: the group $\mathrm{AGL}(4,2) = 2^4 \colon A_8$ and its subgroup $2^4 \colon A_7$ satisfy k-et for $k \leq 4$ and for $k = 6$, but not for $k = 5$.

Results

João Araújo, Wolfram Bentz and I have a complete classification of groups which satisfy k-et for $4 \leq k \leq n/2$, with just a few undecided cases (none for $k \geq 6$ and only one for $k = 5$), together with a description of their witnessing sets.
Intransitive groups with k-et for $2 \leq k \leq n/2$ have just two orbits; if $k \geq 3$, one is a fixed point and the group is $(k-1)$-homogeneous on the other. The converse is also true.
We have examined these groups G and decided, in all but a few cases, whether it holds that $\langle G, t \rangle$ is regular for all maps t whose image is a witnessing set.
In particular, the only transitive groups satisfying k-et for $8 \leq k \leq n/2$ are the symmetric and alternating groups. The only 7-et group apart from S_n and A_n is the Mathieu group M_{24}.
Another interesting classification: the only primitive but not 2-homogeneous groups satisfying 4-et are the Higman–Sims group and its automorphism group.

Idempotents

An idempotent in a semigroup S is an element e satisfying $e^2 = e$. The semigroup is idempotent-generated if it is generated by its idempotents.

If S is a transformation semigroup and G a permutation group normalising S, then according to a theorem of McAlister, the semigroups $\langle G, S\rangle$ and $\langle g^{-1}sg : g \in G\rangle$ contain the same idempotents. So we might ask when one or other of these semigroups is generated by its idempotents.

This is a harder question, and I will speak only of the case $\langle G, t\rangle$, where t is a rank 2 map.

The Road Closure Property

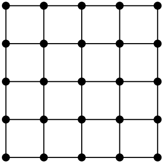
Last year, there was a long season of road closures in the neighbourhood of St Andrews.

Let G be a transitive permutation group on Ω. By Donald Higman's result, G is primitive if and only if, for every orbit O of G on the set of 2-element subsets of Ω, the orbital graph with vertex set Ω and edge set O is connected.

We say that G has the road closure property if, given any orbit O of G on 2-sets and any (maximal) block of imprimitivity for the action of G on O, the graph $(\Omega, O \setminus B)$ is connected.

An example

Consider the automorphism group of a $m \times m$ grid: two points are joined if they lie in the same row or column. The automorphism group is the wreath product $S_m \wr S_2$ in its product action on m^2 points.



The edges fall into two blocks of imprimitivity under the automorphism group: horizontal and vertical.
If workmen come and dig up all the vertical roads, then it is impossible to get from one row to another. So this primitive group fails to have the road closure property.

The Road Closure Conjecture

In the same way, we see that if G is primitive and non-basic (that is, preserves a Cartesian structure on Ω), then G does not have the road closure property.

Similarly, if G is primitive and has an imprimitive normal subgroup of index 2, then G does not have the road closure property.

We know one more family of groups, arising from $\mathrm{P}\Omega^{+}(8,q):S_3$ on the cosets of the parabolic subgroup corresponding to the three leaves of the D_4 diagram.

Problem

True or false: if G is a basic primitive group, not having an imprimitive subgroup of index 2, and not one of the above examples from triality, then G has the road closure property.

Connection with semigroups

Here is the connection with idempotent-generated semigroups.

Theorem

Let G be a transitive permutation group on Ω. Then the following conditions on G are equivalent:

- *for every rank 2 map t on Ω, the semigroup*

$$\langle G, t \rangle \setminus G$$

  is idempotent-generated;
- *G has the road closure property.*

So the conjecture would give the complete classification of such groups.

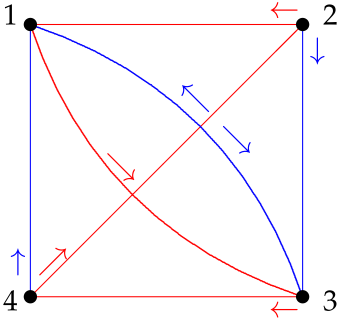
Synchronization

To conclude, a very brief account of synchronization …

You are in a dungeon consisting of a number of rooms. Passages are marked with coloured arrows. Each room 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?

The dungeon



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 semigroups

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 semigroup on Ω.

So an automaton is a transformation semigroup with a distinguished generating set.

The obstruction to synchronization

From now on our graphs are simple and undirected. An endomorphism of a graph is a map from the graph to itself which takes edges to edges.
The endomorphisms of a graph Γ form a transformation semigroup; 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 $\omega(\Gamma) = \chi(\Gamma)$.

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 t on Ω which is not a permutation, the monoid $\langle G, t\rangle$ generated by G and t 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

Theorem

- *A synchronizing group is primitive and basic.*
- *A* 2*-homogeneous group is synchronizing.*

There are polynomial-time tests to decide if a permutation group is transitive, primitive, basic, or 2-homogeneous.

Problem

How to decide whether a permutation group is synchronizing?

Here is a test:

- List all the non-trivial G-invariant graphs ($2^r - 2$ of them, where r is the number of G-orbits on 2-sets).
- Find the clique number and chromatic number of each graph. If we find one where they are equal, then G is not synchronizing; otherwise it is.

Very inefficient, but no known algorithm does much better …