Permutation groups and transformation semigroups

Peter J. Cameron
University of St Andrews

Groups St Andrews, August 2013

Groups and semigroups

How can group theory help the study of semigroups?
If a semigroup has a large group of units, we can apply group theory to it. But there may not be any units at all!
One area where our chances are better is the theory of transformation semigroups, i.e. semigroups of mappings $\Omega \to \Omega$ (subsemigroups of the full transformation semigroup $T(\Omega)$). In a transformation semigroup G, the units are the permutations; if there are any, they form a permutation group G. Even if there are no units, we have a group to play with, the normaliser of S in $\mathrm{Sym}(\Omega)$, the set of all permutations g such that $g^{-1}Sg = S$.

Acknowledgment

It was João Araújo who got me involved in this work, and all the work of mine I report below is joint with him and possibly others. I will refer to him as JA.

Levi–McFadden and McAlister

The following is the prototype for results of this kind. Let S_n and T_n denote the symmetric group and full transformation semigroup on $\{1, 2, \ldots, n\}$.

Theorem

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

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

In other words, semigroups of this form, with normaliser S_n, have *very nice* properties!

The general problem

Problem

- *Given a semigroup property P, for which pairs (a, G), with $a \in T_n \setminus S_n$ and $G \leq S_n$, does the semigroup $\langle g^{-1}ag : g \in G \rangle$ have property P?*
- *Given a semigroup property P, for which pairs (a, G) as above does the semigroup $\langle a, G \rangle \setminus G$ have property P?*
- *For which pairs (a, G) are the semigroups of the preceding parts equal?*

Further results

The following portmanteau theorem lists some previously known results.

Theorem

- *(Levi) For any $a \in T_n \setminus S_n$. the semigroups $\langle g^{-1}ag : g \in S_n \rangle$ and $\langle g^{-1}ag : g \in A_n \rangle$ are equal.*
- *(JA, Mitchell, Schneider) $\langle g^{-1}ag : g \in G \rangle$ 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.*
- *(JA, Mitchell, Schneider) $\langle g^{-1}ag : g \in G \rangle$ 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.*

Our first theorem

Theorem (JA, PJC)

Given k with $1 \leq k \leq n/2$, the following are equivalent for a subgroup G of S_n:

- *for all rank k transformations a, a is regular in $\langle a, G\rangle$;*
- *for all rank k transformations a, $\langle a, G\rangle$ is regular;*
- *for all rank k transformations a, a is regular in $\langle g^{-1}ag : g \in G\rangle$;*
- *for all rank k transformations a, $\langle g^{-1}ag : g \in G\rangle$ is regular.*

Moreover, we have a complete list of the possible groups G with these properties for $k \geq 5$, and partial results for smaller values.

The four equivalent properties above translate into a property of G which we call the k-universal transversal property.

Our second theorem

Theorem (André, JA, PJC)

We have a complete list (in terms of the rank and kernel type of a) for pairs (a, G) for which $\langle a, G\rangle \setminus G = \langle a, S_n\rangle \setminus S_n$.

As we saw, these semigroups have very nice properties. The hypotheses of the theorem are equivalent to "homogeneity" conditions on G: it should be transitive on unordered sets of size equal to the rank of a, and on unordered set partitions of shape equal to the kernel type of a, as we will see.

Our third theorem

Theorem (JA, PJC, Mitchell, Neunhöffer)

The semigroups $\langle a, G\rangle \setminus G$ and $\langle g^{-1}ag : g \in G\rangle$ are equal for all $a \in T_n \setminus S_n$ if and only if $G = S_n$, or $G = A_n$, or G is the trivial group, or G is one of five specific groups.

Problem

It would be good to have a more refined version of this where the hypothesis refers only to all maps of rank k, or just a single map a.

Homogeneity and transitivity

A permutation group G on Ω is k-homogeneous if it acts transitively on the set of k-element subsets of Ω, and is k-transitive if it acts transitively on the set of k-tuples of distinct elements of Ω.
It is clear that k-homogeneity is equivalent to $(n-k)$-homogeneity, where $|\Omega| = n$; so we may assume that $k \leq n/2$. It is also clear that k-transitivity implies k-homogeneity.
We say that G is set-transitive if it is k-homogeneous for all k with $0 \leq k \leq n$. The problem of determining the set-transitive groups was posed by von Neumann and Morgenstern in the context of game theory; they refer to an unpublished solution by Chevalley, but the published solution was by Beaumont and Peterson. The set-transitive groups are the symmetric and alternating groups, and four small exceptions with degrees $5, 6, 9, 9$.

The Livingstone–Wagner Theorem

In an elegant paper in 1964, Livingstone and Wagner showed:

Theorem
Let G be k-homogeneous, where $2 \leq k \leq n/2$. Then

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

The k-homogeneous but not k-transitive groups for $k = 2, 3, 4$ were determined by Kantor. All this was pre-CFSG.
The k-transitive groups for $k > 1$ are known, but the classification uses CFSG.

The k-universal transversal property

Let $G \leq S_n$, and k an integer smaller than n.
The group G has the k-universal transversal property, or k-ut for short, if for every k-element subset S of $\{1, \ldots, n\}$ and every k-part partition P of $\{1, \ldots, n\}$, there exists $g \in G$ such that Sg is a transversal for P.

Theorem

For $k \leq n/2$, the following are equivalent for a permutation group $G \leq S_n$:

- *for all $a \in T_n \setminus S_n$ with rank k, a is regular in $\langle a, G \rangle$;*
- *G has the k-universal transversal property.*

A related property

In order to get the equivalence of "a is regular in $\langle a, G\rangle$" and "$\langle a, G\rangle$ is regular", we need to know that, for $k \leq n/2$, a group with the k-ut property also has the $(k-1)$-ut property. This is not at all obvious!

We go by way of a related property: G is $(k-1,k)$-homogeneous if, given any two subsets A and B of $\{1,\ldots,n\}$ with $|A| = k-1$ and $|B| = k$, there exists $g \in G$ with $Ag \subseteq B$.

Now the k-ut property implies $(k-1,k)$-homogeneity. (Take a partition with k parts, the singletons contained in A and all the rest. If Bg is a transversal for this partition, then $Bg \supseteq A$, so $Ag^{-1} \subseteq B$.)

$(k-1,k)$-homogeneous groups

The bulk of the argument involves these groups. We show that, if $3 \leq k \leq (n-1)/2$ and G is $(k-1,k)$-homogeneous, then either G is k-homogeneous, or G is one of four small exceptions (with $k = 3,4,5$ and $n = 2k-1$).

It is not too hard to show that such a group G must be transitive, and then primitive. Now careful consideration of the orbital graphs shows that G must be 2-homogeneous, at which point we invoke the classification of 2-homogeneous groups (a consequence of CFSG).

One simple observation: if G is $(k-1,k)$-homogeneous but not $(k-1)$-homogeneous of degree n, then colour one G-orbit of $(k-1)$-sets red and the others blue; by assumption, there is no monochromatic k-set, so n is bounded by the Ramsey number $R(k-1,k,2)$. The values $R(2,3,2) = 6$ and $R(3,4,2) = 13$ are useful here; $R(4,5,2)$ is unknown, and in any case too large for our purposes.

The k-ut property

The 2-ut property says that every orbit on pairs contains a pair crossing between parts of every 2-partition; that is, every orbital graph is connected. By Higman's Theorem, this is equivalent to primitivity.
For $2 < k < n/2$, we know that the k-ut property lies between $(k-1)$-homogeneity and k-homogeneity, with a few small exceptions. In fact k-ut is equivalent to k-homogeneous for $k \geq 6$; we classify all the exceptions for $k = 5$, but for $k = 3$ and $k = 4$ there are some groups we are unable to resolve (affine, projective and Suzuki groups).
For large k we have:

Theorem

For $n/2 < k < n$, the following are equivalent:

- *G has the k-universal transversal property;*
- *G is $(k-1,k)$-homogeneous;*
- *G is k-homogeneous.*

Without CFSG?

In the spirit of Livingstone and Wagner, we could ask:

Problem

Without using CFSG, show any or all of the following implications:

- *k-ut implies $(k-1)$-ut for $k \leq n/2$;*
- *$(k-1,k)$-homogeneous implies $(k-2,k-1)$-homogeneous for $k \leq n/2$;*
- *k-ut (or $(k-1,k)$-homogeneous) implies $(k-1)$-homogeneous for $k \leq n/2$.*

Partition transitivity and homogeneity

Let λ be a partition of n (a non-increasing sequence of positive integers with sum n). A partition of $\{1,\ldots,n\}$ is said to have shape λ if the size of the ith part is the ith part of λ.
The group G is λ-transitive if, given any two (ordered) partitions of shape λ, there is an element of G mapping each part of the first to the corresponding part of the second. (This notion is due to Martin and Sagan.) Moreover, G is λ-homogeneous if there is an element of G mapping the first partition to the second (but not necessarily respecting the order of the parts).
Of course λ-transitivity implies λ-homogeneity, and the converse is true if all parts of λ are distinct.
If $\lambda = (n-t,1,\ldots,1)$, then λ-transitivity and λ-homogeneity are equivalent to t-transitivity and t-homogeneity.

Connection with semigroups

Let G be a permutation group, and $a \in T_n \setminus S_n$, where r is the rank of a, and λ the shape of the kernel partition.

Theorem

For $G \leq S_n$ and $a \in T_n \setminus S_n$, the following are equivalent:

- $\langle a, G\rangle \setminus G = \langle a, S_n\rangle \setminus S_n$;
- *G is r-homogeneous and λ-homogeneous.*

So we need to know the λ-homogeneous groups ...

λ-transitivity

If the largest part of λ is greater than $n/2$ (say $n-t$, where $t < n/2$), then G is λ-transitive if and only if it is t-homogeneous and the group H induced on a t-set by its setwise stabiliser is λ'-transitive, where λ' is λ with the part $n-t$ removed.
So if G is t-transitive, then it is λ-transitive for all such λ.
If G is t-homogeneous but not t-transitive, then $t \leq 4$, and examination of the groups in Kantor's list gives the possible λ' in each case.

So what remains is to show that, if G is λ-transitive but not S_n or A_n, then λ must have a part greater than $n/2$.
If $\lambda \neq (n), (n-1,1)$, then G is primitive.
If $n \geq 8$, then by Bertrand's Postulate, there is a prime p with $n/2 < p \leq n-3$. If there is no part of λ which is at least p, then the number of partitions of shape λ (and hence the order of G) is divisible by p. A theorem of Jordan now shows that G is symmetric or alternating.

λ-homogeneity

The classification of λ-homogeneous but not λ-transitive groups is a bit harder. We have to use

- a little character theory to show that either G fixes a point and is transitive on the rest, or G is transitive;
- the argument using Bertrand's postulate and Jordan's theorem as before;
- CFSG (to show that G cannot be more than 5-homogeneous if it is not S_n or A_n).

The outcome is a complete list of such groups.

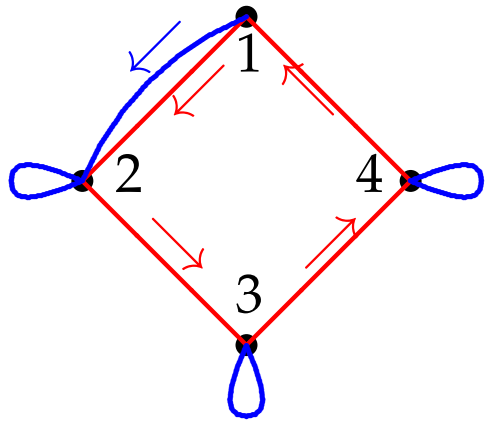
The third theorem

Our third theorem, the classification of groups G such that $\langle g^{-1}ag : g \in G\rangle = \langle a, G\rangle \setminus G$ for all $a \in T_n \setminus S_n$, is a little different; although permutation group techniques are essential in the proof, we didn't find a simple combinatorial condition on G which is equivalent to this property.
So I do not propose to discuss the proof here.

Synchronization

I will end the talk with a brief report on synchronization.
A (finite deterministic) automaton consists of a finite set Ω of states and a finite set of maps from Ω to Ω called transitions, which may be composed freely.
In other words, it is a transformation semigroup with a distinguished set of generators.
An automaton is synchronizing if there is a map of rank 1 (image of size 1) in the semigroup. A word in the generators expressing such a map is called a reset word.
I will also call a transformation semigroup synchronizing if it contains an element of rank 1.

An example



It can be checked easily that BRRRBRRRB is a reset word of length 9. In fact, this is the shortest reset word.

The Černý Conjecture asserts that if an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$. The above example, with the square replaced by an n-gon, shows that this would be best possible. The problem has been open for about 45 years. The best known bound is cubic.

It is known that testing whether an automaton is synchronizing is in P, but finding the length of the shortest reset word is NP-hard.

Graph homomorphisms

All graphs here are undirected simple graphs (no loops or multiple edges).

A homomorphism from a graph X to a graph Y is a map f from the vertex set of X to the vertex set of Y which carries edges to edges. (We don't specify what happens to a non-edge; it may map to a non-edge, or to an edge, or collapse to a vertex.) An endomorphism of a graph X is a homomorphism from X to itself.

Let K_r be the complete graph with r vertices. The clique number $\omega(X)$ of X is the size of the largest complete subgraph, and the chromatic number $\chi(X)$ is the least number of colours required for a proper colouring of the vertices (adjacent vertices getting different colours).

- There is a homomorphism from K_r to X if and only if $\omega(X) \geq r$.
- There is a homomorphism from X to K_r if and only if $\chi(X) \leq r$.

Graphs and transformation semigroups

There are correspondences in both directions between these objects (not quite functorial, or a Galois correspondence, sadly!) First, any graph X has an endomorphism semigroup $\mathrm{End}(X)$. In the other direction, given a transformation semigroup S on Ω, its graph $\mathrm{Gr}(S)$ has Ω as vertex set, two vertices v and w being joined if and only if there is no element of S which maps v and w to the same place.

- $\mathrm{Gr}(S)$ is complete if and only if $S \leq S_n$;
- $\mathrm{Gr}(S)$ is null if and only if S is synchronizing;
- $S \leq \mathrm{End}(\mathrm{Gr}(S))$ for any $S \leq T_n$;
- $\omega(\mathrm{Gr}(S)) = \chi(\mathrm{Gr}(S))$; this is equal to the minimum rank of an element of S.

The main theorem

Theorem

A transformation semigroup S on Ω is non-synchronizing if and only if there is a non-null graph X on the vertex set Ω with $\omega(X) = \chi(X)$ and $S \leq \mathrm{End}(X)$.

In the reverse direction, the endomorphism semigroup of a non-null graph cannot be synchronizing, since edges can't be collapsed. In the forward direction, take $X = \mathrm{Gr}(S)$; there is some straightforward verification to do.

Maps synchronized by groups

Let $G \leq S_n$ and $a \in T_n \setminus S_n$. We say that G synchronizes a if $\langle a, G \rangle$ is synchronizing.
By abuse of language, we say that G is synchronizing if it synchronizes every element of $T_n \setminus S_n$.
Our main problem is to determine the synchronizing groups.
From the theorem, we see that G is non-synchronizing if and only if there is a G-invariant graph whose clique number and chromatic number are equal.

Primitivity

Rystsov showed:

Theorem
A permutation group G of degree n is primitive if and only if it synchronizes every map of rank $n-1$.

So a synchronizing group must be primitive.
JA and I have recently improved this: a primitive group synchronizes every map of rank $n-2$. The key tool in the proof is graph endomorphisms.

Synchronizing groups

Recall that G is synchronizing if it synchronizes every element of $T_n \setminus S_n$.

A 2-homogeneous group is synchronizing, and a synchronizing group is primitive (indeed, is basic in the O'Nan–Scott classification, i.e. does not preserve a Cartesian power structure, i.e. is not contained in a wreath product with the product action). So it is affine, diagonal or almost simple.

Neither of these implications reverses.

Also, G is synchronizing if and only if there is no G-invariant graph, not complete or null, with clique number equal to chromatic number.

We are a long way from a classification of synchronizing groups. The attempts to classify them lead to some interesting and difficult problems in extremal combinatorics, finite geometry, computation, etc. But that is another talk!

Araújo's conjecture

The biggest open problem in this area is the following. A map $a \in T_n$ is non-uniform if its kernel classes are not all of the same size.

Conjecture

A primitive permutation group synchronizes every non-uniform map.

We have some small results about this but are far from a proof!