Permutation Groups and Transformation Semigroups
Lecture 1: Introduction

Peter J. Cameron
University of St Andrews

Shanghai Jiao Tong University
14 November 2017

Permutation groups

For any set Ω, $\mathrm{Sym}(\Omega)$ denotes the symmetric group of all permutations of Ω, with the operation of composition.
If $|\Omega| = n$, we write $\mathrm{Sym}(\Omega)$ as S_n.
We write permutations to the right of their argument, and compose from left to right: that is, αg is the image of $\alpha \in \Omega$ under the permutation $g \in \mathrm{Sym}(\Omega)$, and

$$\alpha(g_1 g_2) = (\alpha g_1) g_2.$$

A permutation group on Ω is a subgroup of $\mathrm{Sym}(\Omega)$.
An action of a group G on Ω is a homomorphism from G to $\mathrm{Sym}(\Omega)$; its image is a permutation group on Ω. Whenever we define a property of a permutation group, we use the name for a property of the group action.

An example

Let G be the group of automorphisms of the cube, acting on the set Ω of vertices, edges and faces of the cube: $|\Omega| = 26$. The action is faithful, so G is a permutation group.

Automorphism groups of mathematical objects provide a rich supply of permutation groups. These objects can be of almost any kind.

Orbits and transitivity

Let G be a permutation group on Ω. Define a relation $\sim$ on Ω by the rule

$$\alpha \sim \beta \text{ if and only if there exists } g \in G \text{ such that } \alpha g = \beta.$$

$\sim$ is an equivalence relation on Ω. (The reflexive, symmetric and transitive laws correspond to the identity, inverse, and closure properties of G.)
The equivalence classes are called orbits; the group G is transitive if there is just one orbit. Thus, a permutation group has a transitive action on each of its orbits.
In the example, there are three orbits: the 8 vertices, the 12 edges, and the 6 faces.

Another way to say this

There is another way to describe transitivity, which will be useful for further properties.
We say that a mathematical structure built on the set Ω is trivial if it is invariant under $\mathrm{Sym}(\Omega)$, and non-trivial otherwise.
Thus,

- a subset of Ω is trivial if and only if it is either Ω or the empty set;
- a partition of Ω is trivial if and only if either it has a single part, or all parts are singletons (sets of size 1);
- a simple graph on Ω is trivial if and only if it is either the complete graph or the null graph.

So we can say:

> *A permutation group G on Ω is transitive if and only if there are no non-trivial G-invariant subsets.*

Transitive actions

Let G act on Ω, and take $\alpha \in \Omega$. The stabiliser of α in G is the set

$$\{g \in G : \alpha g = \alpha\}.$$

It is a subgroup of G.
If H is any subgroup of G, the (right) coset space of H in G is the set $G : H$ of right cosets Hx of H in G. There is a transitive action of G on $G : H$, given by the rule

$$(Hx)g = H(xg).$$

Now there is a notion of isomorphism of group actions, and the following theorem holds:

Theorem

- *Any transitive action of G on Ω is isomorphic to the action of G on the coset space $G : G_\alpha$, for $\alpha \in \Omega$.*
- *The actions of G on coset spaces $G : H$ and $G : K$ are isomorphic if and only if H and K are conjugate subgroups of G.*

Regular permutation groups and Cayley's Theorem

A permutation group G is regular on Ω if it is transitive and the stabiliser of a point is the identity subgroup.
The right cosets of the identity are naturally in bijection with the elements of G. So we can identify Ω with G so that the action of G is on itself by right multiplication. Thus we have Cayley's Theorem:

Theorem

Every group of order n is isomorphic to a subgroup of S_n.

In particular we see that asking a group G to be a transitive permutation group is no restriction on the abstract structure of G.

Primitivity

A transitive permutation group G on Ω is primitive if the only non-trivial G-invariant partitions are the trivial ones (the partition with one part and the partition into singletons).

This can be said another way. A block of imprimitivity is a subset B of Ω with the property that, for all $g \in G$, either $Bg = B$ or $Bg \cap B = \emptyset$. Then G is primitive if and only if the only blocks of imprimitivity are Ω, singletons, and the empty set..

Consider our example G, in its transitive action on the vertices of the cube. We see that G is imprimitive; indeed it preserves two non-trivial partitions:

- the partition into pairs of antipodal points (opposite ends of long diagonals;
- the partition into the vertex sets of two interlocking tetrahedra.

Primitive groups

Theorem

- *Let G be a transitive permutation group on Ω, where $|\Omega| > 1$. Then G is primitive if and only if the stabiliser of a point of Ω is a maximal proper subgroup of G.*
- *Let G be primitive on Ω. Then every non-trivial normal subgroup of G is transitive.*
- *Let G be primitive on Ω. Then G has at most two minimal normal subgroups; if there are two, then they are isomorphic and non-abelian, and each of them acts regularly.*

The last part shows that, unlike for transitivity, not every group is isomorphic to a primitive permutation group.

Basic groups

A Cartesian structure on Ω is an identification of Ω with A^d, where A is some set. We can regard A as an "alphabet", and A^d as the set of all words of length d over the alphabet A. Then A^d is a metric space, with the Hamming metric (used in the theory of error-correcting codes): the distance between two words is the number of positions in which they differ.

A Cartesian structure is non-trivial if $|A| > 1$ and $d > 1$.

Let G be a primitive permutation group on Ω. We say that G is basic if it preserves no non-trivial Cartesian structure on Ω.

Although this concept is only defined for primitive groups, we see that the imprimitive group we met earlier, the symmetry group of the cube acting on the vertices, does preserve a Cartesian structure. The automorphism group of a Cartesian structure over an alphabet of size 2 is necessarily imprimitive – generalise our argument for the cube to see this.

The O'Nan–Scott Theorem

A permutation group G is called

- affine if it acts on a vector space V and its elements are products of translations and invertible linear transformations of V, so that G contains all the translations;
- almost simple if $T \leq G \leq \mathrm{Aut}(T)$, where T is a non-abelian finite simple group, and $\mathrm{Aut}(T)$ its automorphism group (where T embeds into $\mathrm{Aut}(T)$ as the group of inner automorphisms or conjugations).

I won't define diagonal groups; here's an example. Let T be a finite simple group. Then $T \times T$, acting on T by the rule

$$x(g,h) = g^{-1}xh \text{ for all } x,g,h \in G,$$

is a diagonal group. (The stabiliser of the identity is the diagonal subgroup $\{(g,g) : g \in G\}$ of $G \times G$.)

Theorem

Let G be a finite basic primitive permutation group. Then G is affine, diagonal, or almost simple.

Multiple transitivity

If G acts on Ω, then it has induced actions on the set of t-element subsets of Ω, or the set of t-tuples of distinct elements of Ω, where $t \leq |\Omega|$.

We say that G is t-homogeneous if the first action above is transitive, and t-transitive if the second is.

A t-transitive group is t-homogeneous. The symmetric group S_n is t-transitive for all $t \leq n$, while the alternating group A_n is t-transitive for $t \leq n - 2$.

A 2-homogeneous group is primitive. (Exercise; proof later.)

For $t = 2$, these properties have graph-theoretic interpretations:

- G is 2-homogeneous if there are no non-trivial G-invariant undirected graphs on Ω;
- G is 2-transitive if and only if there are no non-trivial G-invariant directed graphs on Ω.

The Classification of Finite Simple Groups

A non-identity group is simple if its only normal subgroups are itself and the identity subgroup.
The Classification of Finite Simple Groups, or CFSG, does what its name suggests:

Theorem
A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type;*
- *one of 26 sporadic groups.*

This theorem has revolutionised finite permutation group theory. I will end with one of its consequences.

Multiply transitive groups

Theorem (CFSG)

All finite 2-transitive groups are explicitly known.

Corollary (CFSG)

The only finite 6-transitive groups are the symmetric and alternating groups.

Indeed, there are only two 5-transitive groups which are not symmetric or alternating, the Mathieu groups M_{12} and M_{24}; and only two further 4-transitive groups, the Mathieu groups M_{11} and M_{23}.

Transformation semigroups

We recall the definitions.

- A semigroup is a set S with a binary operation $\circ$ satisfying the *associative law*:

$$a \circ (b \circ c) = (a \circ b) \circ c$$

  for all $a, b, c \in S$.
- A monoid is a semigroup with an *identity* 1, an element satisfying

$$a \circ 1 = 1 \circ a = a$$

  for all $a \in S$.
- A group is a monoid with *inverses*, that is, for all $a \in S$ there exists $b \in S$ such that

$$a \circ b = b \circ a = 1.$$

From now on we will write the operation as *juxtaposition*, that is, write ab instead of $a \circ b$, and a^{-1} for the inverse of a.

Mind the gap between semigroups and groups!

To any semigroup we can add an identity to produce a monoid of size one larger. Nothing like this is possible for groups!

Order	1	2	3	4	5	6	7	8
Groups	1	1	1	2	1	2	1	5
Monoids	1	2	7	35	228	2237	31559	1668997
Semigroups	1	5	24	188	1915	28634	1627672	3684030417

Note that the numbers of n-element semigroups and $(n+1)$-element monoids are fairly close; this is because we can add an identity to an n-element semigroup to form an $(n+1)$-element monoid. But numbers of groups are much smaller; the group axioms are much tighter!

Two analogues of $\mathrm{Sym}(\Omega)$

For a set Ω, let $T(\Omega)$ be the set of all the maps from Ω to itself, with the operation of composition. If $|\Omega| = n$, we write $T(\Omega)$ as T_n. Note that $T(\Omega)$ is a monoid; it contains $\mathrm{Sym}(\Omega)$, and $T(\Omega) \setminus \mathrm{Sym}(\Omega)$ is a semigroup. $T(\Omega)$ is the full transformation semigroup on Ω.
The order of T_n is n^n.

Also let $I(\Omega)$ denote the set of all partial bijections on Ω (bijections between subsets of Ω), with composition 'where possible': if f_i has domain A_i for $i = 1, 2$, then $f_1 f_2$ has domain $(A_1 f_1 \cap A_2) f_1^{-1}$ and range $(A_1 f_1 \cap A_2) f_2$. Again, if $|\Omega| = n$, we write I_n. This is the symmetric inverse semigroup.

The order of I_n is $\sum_{k=0}^{n} \binom{n}{k}^2 k!$; there is no closed form for this expression.

Regularity

An element a of a semigroup S is regular if there exists $x \in S$ such that $axa = a$. The semigroup S is regular if all its elements are regular. Note that a group is regular, since we may choose $x = a^{-1}$. The semigroup T_n is regular (exercise).
Regularity is equivalent to a condition which appears formally to be stronger:

Proposition

If $a \in S$ is regular, then there exists $b \in S$ such that $aba = a$ and $bab = b$.

Proof.

Choose x such that $axa = a$, and set $b = xax$. Then

$$\begin{aligned} aba &= axaxa = axa = a, \\ bab &= xaxaxax = xaxax = xax = b. \end{aligned}$$

□

Idempotents

An idempotent in a semigroup S is an element e such that $e^2 = e$. Note that, if $axa = a$, then ax and xa are idempotents. In a group, there is a unique idempotent, the identity. By contrast, it is possible for a non-trivial semigroup to be generated by its idempotents.

Proposition

Let S be a finite semigroup, and $a \in S$. Then some power of a is an idempotent.

Proof.

Since S is finite, the powers of a are not all distinct: suppose that $a^m = a^{m+r}$ for some $m, r > 0$. Then $a^i = a^{i+tr}$ for all $i \geq m$ and $t \geq 1$; choosing i to be a multiple of r which is at least m, we see that $a^i = a^{2i}$, so a^i is an idempotent. □

It follows that a finite monoid with a unique idempotent is a group. For the unique idempotent is the identity; and, if $a^i = 1$, then a has an inverse, namely a^{i-1}.

Inverse semigroups

The semigroup S is an inverse semigroup if for each $a \in S$ there exists a unique $b \in S$ such that $aba = a$ and $bab = b$. We say that b is the (von Neumann) inverse of a.
The symmetric inverse semigroup $I(\Omega)$ is an inverse semigroup.
In an inverse semigroup, the idempotents commute, and they form a semilattice under the order relation $e \leq f$ if $ef = fe = f$.
In $I(\Omega)$, the semilattice of idempotents is isomorphic to the Boolean lattice of all subsets of Ω.

Analogues of Cayley's Theorem

Theorem

An n-element semigroup is isomorphic to a sub-semigroup of T_{n+1}.

In Cayley's theorem, we let the group act as the group of right multiplications of itself. For a semigroup, this action may not be faithful. So first we add an identity e to form a monoid. Now $ea = eb$ implies $a = b$ and all is well.

A similar but slightly harder theorem holds for inverse semigroups:

Theorem (Vagner–Preston Theorem)

An n-element inverse semigroup is isomorphic to a sub-semigroup of I_n.

Basics of transformation semigroups

Any map $f : \Omega \to \Omega$ has an image

$$\mathrm{Im}(f) = \{xf : x \in \Omega\},$$

and a kernel, the equivalence relation $\equiv_f$ defined by

$$x \equiv_f y \Leftrightarrow xf = yf,$$

or the corresponding partition of Ω. (We usually refer to the partition when we speak about the kernel of f, which is denoted $\mathrm{Ker}(f)$.) The rank $\mathrm{rank}(f)$ of f is the cardinality of the image, or the number of parts of the kernel.
Under composition, we clearly have

$$\mathrm{rank}(f_1 f_2) \leq \min\{\mathrm{rank}(f_1), \mathrm{rank}(f_2)\},$$

and so the set $S_m = \{f \in S : \mathrm{rank}(f) \leq m\}$ of elements of a transformation semigroup which have rank at most m is itself a transformation semigroup.

Idempotents in transformation semigroups

Suppose that f_1 and f_2 are transformations of rank r. The rank of $f_1 f_2$ is at most r. Equality holds if and only if $\mathrm{Im}(f_1)$ is a transversal for $\mathrm{Ker}(f_2)$, in the sense that it contains exactly one point from each part of the partition $\mathrm{Ker}(f_2)$. This combinatorial relation between subsets and partitions is crucial for what follows. Here is one simple consequence.

Proposition

Let f be a transformation of Ω, and suppose that $\mathrm{Im}(f)$ is a transversal for $\mathrm{Ker}(f)$. Then some power of f is an idempotent with rank equal to that of f.

For the restriction of f to its image is a permutation, and some power of this permutation is the identity.

Permutation groups and transformation semigroups

Let S be a transformation semigroup whose intersection with the symmetric group is a permutation group G. How do properties of G influence properties of S. In particular, what can we say if $S = \langle G, a \rangle$ for some non-permutation a?

Here is a sample theorem due to Araújo, Mitchell and Schneider.

Theorem

Let G be a permutation group on Ω, with $|\Omega| = n$. Suppose that, for any map f on Ω which is not a permutation, the semigroup $\langle G, f \rangle$ is regular. Then either G is the symmetric or alternating group on Ω, or one of the following occurs:

- $n = 5$, $G = C_5$, $C_5 \rtimes C_2$, *or* $C_5 \rtimes C_4$;
- $n = 6$, $G = \mathrm{PSL}(2,5)$ *or* $\mathrm{PGL}(2,5)$;
- $n = 7$, $G = \mathrm{AGL}(1,7)$;
- $n = 8$, $G = \mathrm{PGL}(2,7)$;
- $n = 9$, $G = \mathrm{PGL}(2,8)$ *or* $\mathrm{P\Gamma L}(2,8)$.