Synchronization 2: Permutation groups

Peter J. Cameron

10-11 June 2010

Notation

Ω will denote a set (often the set $\{1,\ldots,n\}$).

The image of an element $v \in \Omega$ under a permutation g of Ω will be denoted by vg.

So if g and h are permutations, and we define composition by the rule that gh means "apply g, then h", then $v(gh) = (vg)h$.

With this operation, the set of permutations of Ω is a group. We use $\mathrm{Sym}(\Omega)$ for the group of all permutations of Ω. If $\Omega = \{1,\ldots,n\}$, then we write S_n for $\mathrm{Sym}(\Omega)$.

Permutation groups and group actions

A *permutation group* is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ of all permutations on Ω.

An *action* of a group G on a set Ω is a homomorphism ϕ from G to $\mathrm{Sym}(\Omega)$.

These are almost the same. The image of an action is a permutation group. The only difference is that an action may have a kernel. In particular, if G acts on Ω, we write vg rather than $v(g\phi)$.

Example 1. Let $G = S_4$. Then G acts on the set of three partitions of $\{1,2,3,4\}$ into two parts of size 2, namely $A = 12|34$, $B = 13|24$, $C = 14|23$. Then the element $(1,2,3)$ induces the permutation (A,C,B) of the set $\{A,B,C\}$. We have a homomorphism from S_4 to S_3; its image is S_3, and its kernel is the *Klein group*.

Orbits and transitivity

Let G act on Ω. Define a relation $\sim$ on Ω by:

$$v \sim w \Leftrightarrow (\exists g \in G)(vg = w).$$

This is an equivalence relation: the reflexive, symmetric and transitive laws come immediately from the identity, inverse and closure laws for G.

The equivalence classes are called *orbits*; and the action is *transitive* if there is only one orbit.

Now suppose that G is a permutation group on Ω. If $\Omega = \bigcup_{i\in I} \Omega_i$, where Ω_i are the orbits, then let G_i be the transitive permutation group induced by G on Ω_i; then G is embeddable in the Cartesian product $\prod_{i\in I} G_i$.

Thus we have our first reduction theorem:

Theorem 2.
- *A set on which G acts is a disjoint union of sets on which G acts transitively.*
- *Any permutation group is embeddable in the Cartesian product of transitive permutation groups.*

Note that the first part of the theorem, describing the structure of Ω, is more precise than the second part, describing the structure of G.

Transitive groups

Being a transitive permutation group is no restriction on the structure of a group, by Cayley's Theorem:

Theorem 3. *Every group is isomorphic to a transitive permutation group.*

Define a map ρ from G to $\mathrm{Sym}(G)$ (the *right regular action*) by the rule that $g\rho$ is the perutation $x \mapsto xg$.

Then ρ is an injective homomorphism; so its image is a subgroup of $\mathrm{Sym}(G)$ (a permutation group on G) isomorphic to G.

Imprimitivity

Suppose now that G acts transitively on Ω. A *congruence* on Ω is a G-invariant equivalence relation on Ω; the equivalence classes are called *blocks of imprimitivity* for G.

There are two trivial congruences (if $|\Omega| > 1$):

- the relation of *equality*, whose blocks are singletons;
- the *universal* relation, with a single block Ω.

The action is *imprimitive* if there is a non-trivial congruence, and is *primitive* if not.

The wreath product

Let H be a group, and K a permutation group on a set Δ. We define the *wreath product* H Wr K to be the semi-direct product of the "bottom group" B by the "top group" T, where

- B is the Cartesian product of $|\Delta|$ copies of H, which we may regard as the set of functions $f : \Delta \to H$ with componentwise product

$$(f_1 f_2)(d) = f_1(d) f_2(d) \text{ for } d \in \Delta;$$

- T is the group K, acting on B by permuting the factors of the Cartesian product in the same way that it permutes the elements of Δ:

$$(f^k)(d) = f(dk^{-1}) \text{ for } d \in \Delta.$$

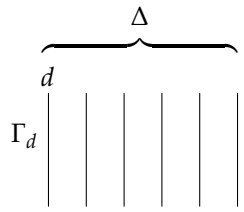
The inverse in the last formula is just a technicality to make the multiplication work correctly.

The imprimitive action

Now suppose that H is itself a permutation group on a set Γ. There are two natural actions of H Wr K.

The first is the *imprimitive action* on the set $\Gamma \times \Delta$. We regard this as a covering of Δ with fibres indexed by Γ: that is,

$$\Gamma \times \Delta = \bigcup_{d \in \Delta} \Gamma_d, \quad \text{where} \quad \Gamma_d = \{(c, d) : c \in \Gamma\}.$$



Now $G = H$ Wr K acts as follows:

- Each factor H_d of B in the Cartesian product acts on the copy Γ_d of Γ:

$$(c, d) f = (cf(d), d).$$

- T permutes the fibres Γ_d like K acting on Δ:

$$(c, d)k = (c, dk).$$

The imprimitive action of the wreath product is (as the name suggests) imprimitive if $|\Gamma|, |\Delta| > 1$; the relation "belong to the same fibre Γ_d" is a congruence whose blocks are the fibres.

Imprimitive groups and wreath products

Wreath products embed imprimitive groups in a similar way that Cartesian products embed intransitive groups:

Theorem 4. *Let G be a transitive but imprimitive permutation group on Ω. Let Γ be a block of imprimitivity, and H the permutation group induced on Γ by its setwise stabiliser; let Δ be an index set for the set of blocks of imprimitivity, and let K be the permutation group induced on Δ by G.*

Then there is a bijection between Ω and $\Gamma \times \Delta$ under which G is embedded as a subgroup of H Wr K (with its imprimitive action).

The power action

Return to the situation where H and K are permutation groups on sets Γ and Δ respectively. Another important action of the wreath product H Wr K is the *power action*.

Let Γ^Δ be the set of functions $\phi : \Delta \to \Gamma$. Now

- The base group acts coordinatewise:

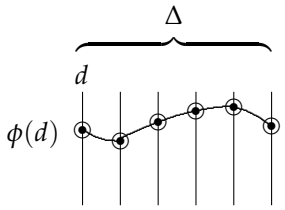
$$(\phi f)(d) = (\phi(d))f(d) \text{ for } d \in \Delta.$$

- The top group permutes the arguments:

$$(\phi k)(d) = \phi(dk^{-1}) \text{ for } d \in \Delta,$$

  where as before the inverse is required for technical reasons.

We can regard elements of Γ^Δ as *global sections* of the fibre space $\Gamma \times \Delta$: a function ϕ picks out one point $\phi(d)$ from each fibre Γ_d.



An example

Consider the wreath product S_2 Wr S_n, otherwise known as the *Weyl group* of type B_n. It has a normal subgroup S_2^n which is elementary abelian of order 2^n; the factor group is the symmetric group S_n.

The imprimitive action is on the vertices of the n-dimensional *cross-polytope* (or *hyperoctahedron*), vectors with ± 1 in one coordinate and 0 in all others. The ith factor of the base group changes the sign of the ith basis vector and fixes all others; the top group permutes the coordinates.

The power action is on the vertices of the n-dimensional *hypercube*, of the form $(\epsilon_1, \ldots, \epsilon_n)$, where $\epsilon_i = \pm 1$ for $i = 1, \ldots, n$. The base group changes signs, while the top group permutes the coordinates.

Note that the two actions are the same when regarded as acting on $\mathbb{R}^n$.

Primitive groups

We noted that every group is isomorphic to a transitive permutation group, by Cayley's Theorem. However, primitive groups are more special.

A permutation group G is *semiregular* if the stabiliser of any point is the identity, and is *regular* if it is transitive and semiregular. Any regular action of a group is just the *right regular action* ρ on itself by right multiplication:

$$x(g\rho) = xg.$$

There is also a *left regular action* λ:

$$x(g\lambda) = g^{-1}x.$$

The resulting permutation groups are isomorphic, but have an important property:

The centraliser of the right regular action of a group G is the left regular action.

Curiously, the commutative law of left and right actions is just a translation of the associative law for the group:

$$(x(g\rho))(h\lambda) = h^{-1}(xg) = (h^{-1}x)g = (x(h\lambda))(g\rho)$$

for all $x \in G$, so

$$(g\rho)(h\lambda) = (h\lambda)(g\rho)$$

for all $g, h \in G$.

We need one more observation:

A non-trivial normal subgroup of a primitive permutation group is transitive.

For the orbits of a normal sugroup of G form blocks of imprimitivity for G.

Theorem 5. *A primitive permutation group has at most two minimal normal subgroups. If it has two, then they are isomorphic and non-abelian.*

For distinct minimal normal subgroups of a group commute with each other. If there are two, they are the left and right regular actions of a (necessarily non-abelian) group; and then there cannot be a third.

The *socle* of a group is the product of its minimal normal subgroups. Any miminal normal subgroup of a finite group is itself a direct product of isomorphic finite simple groups. It follows from the theorem above that:

The socle of a primitive permutation group is the direct product of isomorphic simple groups.

An example

Here is an example of a primitive group with two minimal normal subgroups.

Example 6. Let S be a non-abelian simple group. Let $G = S \times S$ act on S by the rule that the first factor acts by left multiplication and the second by right multiplication: that is,

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

Any congruence for the second factor is the relation "same coset of T" for some subgroup T of S; and this congruence is preserved by the first factor if and only if T is a normal subgroup. So, since T is simple, G has only the trivial congruences.

Basic groups

A *Cartesian structure* or *power structure* on Ω is a bijection between Ω and the set Γ^Δ of functions from Δ to Γ, where $|\Gamma|, |\Delta| > 1$. This gives Ω the structure of an n-dimensional hypercube (where $n = |\Delta|$) whose sides have size $|\Gamma|$.

Let G act on Ω. We say that G is *non-basic* if it preserves a Cartesian structure on Ω, and *basic* otherwise.

A transitive non-basic group is embeddable in the wreath product of permutation groups on Γ and Δ in the power action. However, for primitive groups, we can make a stronger statement.

O'Nan–Scott I: Non-basic groups

Theorem 7. *Let G be a primitive but non-basic permutation group with socle N. Then G is embeddable in the wreath product G_0 Wr K, where G_0 is a basic primitive permutation group. Moreover, if K has degree n, then $N = N_0^n$, where N_0 is either the socle or a minimal normal subgroup of G_0.*

It turns out that the case where G_0 has two minimal normal subgroups, of which N_0 is one (the so-called *twisted wreath product* case, discovered by Aschbacher) will not concern us. The smallest twisted wreath product has degree $60^6 = 46656000000$.

Affine groups

Let V be a d-dimensional vector space over the field $\mathbb{F}_p$, where p is prime, and let H be a group of linear transformations of V. Then there is a corresponding *affine group*

$$G = \{x \mapsto x^h + v : h \in H, v \in V\}$$

of permutations of V, generated by the translations (which form a normal subgroup) and elements of H.

Theorem 8. *With the above notation,*

- *G is always transitive;*
- *G is primitive if and only if H acts irreducibly on V (that is, fixes no non-zero proper subspace of V);*
- *G is basic if and only if H acts primitively on V (that is, preserves no non-trivial direct sum decomposition of V).*

A primitive group is affine iff its socle (which is its unique minimal normal subgroup) is an elementary abelian p-group.

Diagonal groups

Let S be a non-abelian finite simple group. A *diagonal group* is one whose socle is S^n, acting on the cosets of a diagonal subgroup

$$\{(s, s, \ldots, s) : s \in S\}$$

of S^n.

For $n = 2$ we have the example of $S \times S$ acting by left and right multiplication we saw earlier.

A diagonal group may also contain

- automorphisms of S, acting in the same way on all factors;
- permutations of the factors.

If $n > 2$, we must have at least a transitive group of permutations of the factors in order for the diagonal group to be primitive.

Almost simple groups

A group G is *almost simple* if its socle is simple. Such a group is an extension of a simple group by a subgroup of its automorphism group; in other

words, there is a simple group S such that $S \leq G \leq \mathrm{Aut}(S)$.

For example, the symmetric group S_n is almost simple for $n \geq 5$. (It is affine for $n \leq 4$.)

The almost simple primitive groups are the largest and least understood class.

O'Nan–Scott II: Basic groups

Theorem 9. *Let G be a basic primitive permutation group. Then G is affine, or diagonal, or almost simple.*

This theorem opened the way to the application of the Classification of Finite Simple Groups to permutation group theory, which has been done very successfully since the Classification was first announced in 1980.

2-transitive and 2-set transitive groups

A permutation group G on Ω is 2-*transitive* if, given any two ordered pairs of distinct elements of Ω, there is an element of G which carries the first pair to the second.

The symmetric group S_n is 2-transitive for any $n \geq 2$.

A permutation group G on Ω is 2-*set transitive* if, given any two unordered pairs of distinct elements of Ω, there is an element of G which carries the first pair to the second.

Theorem 10.

- *A 2-transitive group is 2-set transitive.*
- *A 2-set transitive group is primitive (and basic).*

The first statement is obvious. For the second, note that if G is 2-set transitive, then there are only four G-invariant *symmetric* relations: the empty relation, equality, inequality, and the universal relation. So the only G-invariant equivalence relations are equality and the universal relation.

The power structure on Γ^n can be specified by a collection of symmetric binary relations $R_0, R_1, \ldots, R_n$, where two n-tuples $\underline{v}$ and $\underline{w}$ satisfy $(\underline{v}, \underline{w}) \in R_i$ if they differ in exactly i coordinates. So no such structure can be preserved by a 2-set transitive group.

Neither implication in the previous theorem reverses.

Example 11. Let G be the cyclic group of prime order p, in its regular action.

- If $p = 2$, then G is 2-transitive.
- If $p = 3$, then G is 2-set transitive but not 2-transitive.
- If $p \geq 5$, then G is primitive (and basic) but not 2-set transitive.

CFSG

The *Classification of Finite Simple Groups*, or *CFSG* for short, is the major theorem announced in 1980 and now, perhaps, finally proved. It asserts the following.

Theorem 12. *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.*

The groups of Lie type are essentially matrix groups, and are divided into classical (special linear, symplectic, unitary and orthogonal groups) and exceptional (associated with the exceptional simple Lie algebras of types G_2, F_4, E_6, E_7 and E_8, and with exceptional graph automorphisms of other Lie algebras.

The sporadic simple groups range from the Mathieu group M_{11} (of order 7920) to the Fischer–Griess Monster $\mathbb{M}$ (of order roughly 10^{54}).

Classification of 2-transitive groups

A 2-transitive group is basic, and so must be affine, diagonal, or almost simple. It is not hard to show that it cannot be diagonal.

The affine 2-transitive groups (these are just the ones where the linear group H acts transitively on non-zero vectors) are all known, thanks to work of Hering and Liebeck. The almost simple 2-transitive groups have also been classified, by a combination of work by many authors.

Hence it is possible to write down a list of all the 2-transitive groups. Such a list can be found in my book *Permutation Groups* (Cambridge, 1990).

Classification of 2-set transitive groups

A permutation group which is 2-set transitive but not 2-transitive necessarily has odd order. (For a group of even order contains an element of order 2, which must swap some pair of points; in a 2-set transitive group, this means every pair of points can be swapped, and the group is 2-transitive.)

By the *Feit–Thompson Theorem*, such a group is soluble; so its socle is abelian, and it must be an affine group.

A result proved by several authors classifies these groups: they are permutation groups of a field $\mathbb{F}_q$, where $q \equiv 3 \bmod 4$, of the form

$$\{x \mapsto ax^\sigma + c : a \in (\mathbb{F}_q^\times)^2, c \in \mathbb{F}_q, \sigma \in S\},$$

where S is a subgroup of the automorphism group of $\mathbb{F}_q$.