Primitivity

Peter J. Cameron

Combinatorics, Algebra and More
8 July 2013

Before I begin, I'd like to say sincere thanks to

- my colleagues and students at Queen Mary, past and present, who have made this such a great place to work for the last 27 years;
- Leonard, David, Karen, and all who have helped organise this great conference;
- everyone here, speakers and listeners, for coming along.

I have learned a huge amount from you!

> … the university's purpose … is not to maximize revenue but to serve the common good through teaching and research. It is true that teaching and research are expensive, and universities devote much effort to fund-raising. But when the goal of money making predominates … the university has strayed far from the scholarly and civic goods that are its primary reason for being.
>
> Michael Sandel, *Justice*

Successive governments and administrators are turning education and research from a civic good to a private one, and students into customers for this private good. We have a lot to do to maintain Sandel's university.

Reduction

One of mathematicians' favourite tools is some form of reduction. Ideally the process should have three features:

- a procedure to tell whether an object is reducible or not;
- for reducible objects, a method to get information about them from "smaller" objects;
- for irreducible objects, a restriction on what they can look like (ideally a classification);
- if possible, a procedure for reconstructing an object from its building blocks (extension theory).

In the case of primitivity of permutation groups, we have the bonus that there are connections with many other things, in combinatorics, automata theory, and several other areas.

Primitivity was invented by Galois in his *Second Mémoire*; I will say a bit more about this later.

First definition

I will take you through eight definitions of primitivity. Here is the first.
Let G be a permutation group on Ω.
We say that G is imprimitive if there is a partition π of Ω, which is neither the partition into singletons nor the partition with a single part, which is preserved by G (in the sense that G permutes the parts of π among themselves.)
Then G is primitive if it is not imprimitive.
This is typical of many negative definitions of this type, where something is "irreducible" if it is not "reducible".

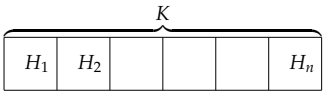
First digression

Consider the trivial group G, acting on a set Ω with two elements. Is G primitive?
Yes, according to the definition I just gave. For the partition into singletons and the partition with a single part are the only partitions of Ω.
This simple problem has ramifications that go very deep, see the next slide. But I will dodge these problems by ignoring this case. In any other case, a primitive group (as defined) must be transitive.
In future, this is part of the definition!

A particular kind of diagonal group is a transitive permutation group G whose socle N is a direct power of a non-abelian finite simple group S, such that the intersection of N with a point stabiliser is a diagonal subgroup of N. The diagonal group G is primitive if and only if it acts primitively (in the first sense) on the direct factors of the socle by conjugation. Thus, if the socle has just two factors, then G may have two minimal normal subgroups!
This is the loophole through which the twisted wreath products slipped in the original version of the O'Nan–Scott Theorem.

Second digression

I promised a reduction for imprimitive groups. Here it is.



Suppose that the transitive group G preserves a partition of Ω. Let H be the permutation group induced on a part by its setwise stabiliser, and K the permutation group induced on the set of parts by G. Note that both of these groups are transitive. Then G is embedded in the wreath product of H and K, the group generated by

- the direct product of copies of H acting on the parts of the partition (one copy of H for each part); and
- the group K, permuting the parts.

For finite permutation groups, if H and K are not primitive, we may reduce them further; the process eventually terminates with a collection of primitive groups. However, neither the reduction process, nor the final list of primitive groups, is unique.
For infinite groups, the process may fail to terminate.
I won't be discussing this here.

Third digression



In his 51-page paper on the *Second Mémoire* of Galois, Ιeter Neumann has shown that Galois was a bit confused about whether a primitive group was one for which the only invariant partitions are trivial, or one for which the only partitions into orbits of normal subgroups are trivial.
A group satisfying the second condition (i.e., that any non-trivial normal subgroup is transitive) is now called quasiprimitive. Cheryl Praeger has developed the idea that in many cases the hypothesis "G primitive" can be replaced by the weakening "G quasiprimitive". But that is another story!

A convention

For convenience, I will say that a structure of any kind on Ω (subset, partition, graph, etc.) is trivial if it is invariant under the symmetric group on Ω. This avoids having to redefine "trivial" in each new situation.
This usage for partitions agrees with what we saw earlier: the trivial partitions are the partition into singletons and the partition with a single part. The trivial subsets are the empty set and Ω, and the trivial graphs are the complete and null graphs.

Second definition

A permutation group G on Ω is primitive if there is no non-trivial G-invariant equivalence relation on Ω.
This definition is the same as the previous one because of the equivalence relation theorem, the correspondence between equivalence relations on a set and partitions of the set.
If there were time, I would argue that the equivalence relation theorem is the modern *pons asinorum*.

Variation

Helmut Wielandt, in his work on infinite permutation groups, defined a permutation group to be strongly primitive if there is no non-trivial G-invariant reflexive and transitive relation on Ω.
Clearly strong primitivity implies primitivity.

For finite transitive permutation groups, the two concepts are equivalent: a reflexive and transitive relation invariant under a transitive permutation group is necessarily symmetric. In other words, in a city with a transitive symmetry group, if you can walk from any point to any other, then you can drive!

Proof.
Let $R(\alpha)$ be the set of points which can be reached from α, obeying the one-way signs. Clearly, if $\beta \in R(\alpha)$, then $R(\beta) \subseteq R(\alpha)$. But, by transitivity, $|R(\alpha)| = |R(\beta)|$. So equality holds, whence $\alpha \in R(\beta)$. □

For infinite groups, primitivity and strong primitivity are not equivalent. The group of order-preserving permutations of $\mathbb{Q}$ is primitive but not strongly primitive: the order relation on $\mathbb{Q}$ is reflexive and transitive but not symmetric.
We can define a permutation group G to be strong if every G-invariant reflexive and transitive relation is symmetric; then G is strongly primitive if and only if it is strong and primitive.
For example, any torsion group (one in which all elements have finite order) is strong.

Third definition


The first mathematics book I read really seriously (as a DPhil student in Oxford, under Пeter Neumann's supervision) was Helmut Wielandt's *Finite Permutation Groups*. Here is Wielandt's definition of primitivity.
A block for the permutation group G on Ω is a subset Δ of Ω with the property that, for all $g \in G$, we have either $\Delta g = \Delta$ or $\Delta g \cap \Delta = \emptyset$.
Now G is primitive if the only blocks for G are the empty set, singletons, and the whole of Ω.

The equivalence of this definition with the others is not quite so trivial. It is clear that any part of a G-invariant partition is a block. Conversely, a little thought shows that, if Δ is a non-empty block, then so is Δg for all $g \in G$; so the images of Δ are equal or disjoint. If G is transitive, then every point of Ω lies in a (unique) image of Δ.

Fourth definition

Let G be a transitive permutation group on Ω, where $|\Omega| > 1$. Let H be the stabiliser of the point α of Ω. Then the action of G on Ω can be defined "internally": it is (up to isomorphism) the same as the action of G by right multiplication on the set of right cosets of H in G.
Now G is primitive if H is a maximal proper subgroup of G. This is because, if $H \leq K \leq G$, then the K-orbit containing α is a block for G; so primitivity means that either this orbit is a singleton (so $K = H$) or it is the whole of Ω (so $K = G$).

Digression

A transitive permutation group G on Ω is strongly primitive if and only if the stabiliser of a point is a maximal proper subsemigroup of G.
This is not the last time that semigroups will appear.

Cellular algebras and coherent configurations


Boris Weisfeiler and Donald Higman independently (and several other people – the history is somewhat complicated) had the idea of treating the set of orbits of G on Ω^2 as a combinatorial and algebraic object.
Weisfeiler called this object a cellular algebra, but this term is now used with a completely different meaning, so I will use Higman's term: a coherent configuration. (Sometimes it is called an association scheme, but this term also has a different meaning, which I will refer to later.)

Orbital graphs

There are two types of orbits of G on Ω^2:

- diagonal orbits, which consist of pairs (α, α). These correspond to the orbits of G on Ω, which are the fibres of the configuration.
- non-diagonal orbits, consisting of pairs (α, β) with $\alpha \neq \beta$. The pairs of such an orbit can be regarded as the edge of a directed graph on the vertex set Ω. These graphs are the orbital graphs of G.

A directed graph is connected if it is possible to move from any vertex to any other along edges, ignoring the directions; it is strongly connected if it is possible to do so following the directions.
We saw earlier that a finite vertex-transitive directed graph is strongly connected if and only if it is connected.

Fifth definition

A transitive permutation group G on Ω is primitive if all its orbital graphs are connected.
For if an orbital graph is disconnected, then the partition into connected components is preserved by G; conversely, if π is a non-trivial G-invariant partition, and α and β are two points in the same part of π, then the orbital graph with edge set $(\alpha, \beta)G$ is disconnected.
For infinite groups, we have a similar result: G is strongly primitive if and only if all its orbital graphs are strongly connected.

The universal transversal property

The next two definitions of primitivity have their roots in semigroup theory, to which João Araújo was my introduction.
The permutation group G on Ω has the k-universal transversal property, or k-ut for short, if the following holds:

> *Given any subset Δ of Ω, and any partition π of Ω, with $|\Delta| = |\pi| = k$, there is an element $g \in G$ such that Δg is a transversal for π.*

Sixth definition

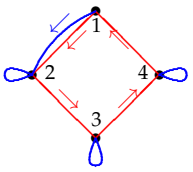
A transitive permutation group G on Ω is primitive if it has the 2-universal transversal property.
This is because a graph is connected if and only if, for any partition of the vertex set into two parts, there is an edge of the graph with one end in each part. So this definition is equivalent to connectedness of all the orbital graphs of G.

Digression

It is natural to ask what we can say about the k-universal transversal property for other values of k.
João and I looked at this in connection with a question about transformation semigroups. We gave a classification of the permutation groups G with the property that, for any rank k map $f : \Omega \to \Omega$, the semigroup $\langle G, f \rangle$ is regular.
Our result is that, for $k > 2$, the k-universal transversal property is equivalent to k-homogeneity (k-set transitivity) with some known exceptions and some cases which we were not able to resolve.

Synchronization

Let G be a permutation group on Ω, and $f : \Omega \to \Omega$ a map which is not a permutation. We say that G synchronizes f if the semigroup $\langle G, f \rangle$ contains an element of rank 1, i.e. one whose image is a singleton.



	B	R	R	R	B	R	R	R	B
1	2	3	4	1	2	3	4	1	2
2	2	3	4	1	2	3	4	1	2
3	3	4	1	2	2	3	4	1	2
4	4	1	2	3	3	4	1	2	2

This shows that the cyclic group of order 4 synchronizes the map given by the blue arrows.

Seventh definition

Let G be a transitive permutation group on Ω, with $|\Omega| = n$.
Then G is primitive if it synchronizes every map of rank $n - 1$.
This is a theorem of Rystsov. We need to take a small detour through graph homomorphisms in order to make it "obvious" that this definition is equivalent to the other six.

Graph endomorphisms and colourings

Graphs now are simple undirected graphs. A homomorphism from a graph X to a graph Y is a map between their vertex sets which maps edges to edges. (We do not specify what happens to a non-edge; it may map to a non-edge, or to an edge, or collapse to a single vertex.) An endomorphism of a graph X is a homomorphism from X to X.
As an exercise, show that a homomorphism from X to a complete graph on k vertices is just a proper vertex-colouring of X with k colours.
We let $\omega(X)$ denote the clique number of X (the size of the largest complete subgraph); $\chi(X)$ the chromatic number (the least number of colours required for a proper vertex-colouring), and $\mathrm{End}(X)$ the endomorphism semigroup of X.

Synchronization

Let S be a transformation semigroup on Ω. We say that S is synchronizing if it contains an element of rank 1.
There is a single obstruction to synchronization:

Theorem
The transformation semigroup S on Ω is non-synchronizing if and only if there is a non-trivial graph X on Ω such that $\omega(X) = \chi(X)$ and $S \leq \mathrm{End}(X)$.

Proof.
An edge cannot be collapsed by an endomorphism.
Conversely, define a graph $\mathrm{Gr}(S)$ by the rule that vertices v and w are joined if and only if there is no element $f \in S$ with $vf = wf$. It is not hard to show that $\mathrm{Gr}(S)$ has the required properties. □

Rystsov's Theorem

Now we can prove Rystsov's Theorem.

Proof.
Suppose that G fails to synchronize the map f of rank $n - 1$.
Then there is a graph X with $G \leq \mathrm{Aut}(X)$ and $f \in \mathrm{End}(X)$. Let v and w be the two vertices having the same image under f.
Then v and w are not joined, and f maps the neighbours of each bijectively to the neighbours of $vf = wf$. So v and w have the same neighbours. Then the relation "have the same neighbours" is a G-invariant equivalence relation on Ω, and G is imprimitive.
Conversely, if G is imprimitive, then the complete multipartite graph whose parts are the parts of a G-invariant partition has an endomorphism of rank $n - 1$. □

Synchronizing groups


By abuse of terminology, we call a permutation group G on Ω synchronizing if it synchronizes every non-permutation on Ω.

Problem

Which permutation groups are synchronizing?

We know that synchronizing groups are primitive, but the converse is not true. The problem for particular classes of groups (symmetric groups acting on subsets of fixed size, general linear groups acting on subspaces of fixed dimension, classical groups acting on their polar spaces) leads to some very difficult questions in extremal set theory and vector space analogues and about ovoids and spreads in polar spaces. We are far from a complete answer!

Araújo's Conjecture

Araújo's conjecture supports the feeling that the gap between "primitive" and "synchronizing" is not too large. A map on Ω is called uniform if the inverse images of points in its image all have the same size.

Conjecture

A primitive permutation group synchronizes every non-uniform map.

This is still open; but we have improved Rystsov's Theorem by showing that a primitive group of degree n synchronizes every map of rank $n-2$, and also synchronizes every non-uniform map of rank at most 5.

Association schemes

I didn't *define* coherent configurations before; I explained how they arise from permutation groups. There is a purely combinatorial definition, which I won't reproduce here.
Coherent configurations on a given set form a lattice, in which the top element corresponds to the symmetric group, and bottom element to the trivial group.
An *association scheme* is a coherent configuration in which every relation is symmetric (i.e., $(\alpha,\beta)\in R$ implies $(\beta,\alpha)\in R$).
Association schemes are closed under join but not under meet.

Association schemes are older than coherent configurations, having arisen in statistics in the work of R. C. Bose and his school.
Two particular association schemes are the group-divisible scheme (associated with the wreath product of two symmetric groups in the imprimitive action) and the Hamming scheme (associated with the wreath product in the product action).
More information is in Rosemary's book.

Eighth definition

A transitive permutation group G on Ω is primitive if it does not preserve a group-divisible association scheme on Ω.
This is rather easily seen to be equivalent to the first definition.
However, we can continue. In the analysis of the O'Nan–Scott Theorem, it is helpful to say:
A primitive permutation group G on Ω is basic if it does not preserve a Hamming association scheme on Ω.
This gives a reduction process similar to the reduction to primitive groups. The O'Nan–Scott Theorem tells us that a basic group is affine, diagonal, or almost simple.

AS-free groups

Cristy Alejandro, Rosemary Bailey and I decided to push this to the obvious conclusion:
A transitive permutation group G on Ω is AS-free if it does not preserve any non-trivial association scheme on Ω.
Note that the analogous notion of "CC-free" is equivalent to 2-transitivity; this is the basis of Weisfeiler's and Higman's approaches.

An AS-free group is

- primitive (since it preserves no group-divisible association scheme);
- basic (since it preserves no Hamming association scheme).

By the O'Nan–Scott Theorem, it is affine, diagonal or almost simple.

- An affine AS-free group must be 2-homogeneous. (The abelian regular normal subgroup shows that the coherent configuration for the group is commutative, and hence its symmetrization is an association scheme.)
- A diagonal AS-free group must have at least four simple factors in its socle. (If two, it would preserve the conjugacy class scheme of the simple group; if three, it would preserve a Latin square scheme corresponding to the multiplication table of the group.) It is not known what happens for four or more factors.
- There are some almost simple AS-free groups which are not 2-transitive, but the position is not understood.

A final problem

"Synchronizing" and "AS-free" are both conditions on permutation groups which are intermediate between primitivity and 2-transitivity.

Problem

Is there any connection between these two conditions?

You see that I haven't run out of things to think about!