Primitive permutation groups

1 The basics

We refer to the topic essay on *Permutation groups* as background for this one. In particular, the notions of *permutation group* and *transitivity* are assumed as is the following result:

> Any transitive action of a group G is isomorphic to the action by right multiplication on the set of right cosets of a subgroup H of G (where H can be taken to be the stabiliser of a point in the given action). Moreover, the actions on the sets of cosets of two subgroups H and K are isomorphic if and only if H and K are conjugate subgroups of G.

Thus determining all the transitive actions of G is equivalent to determining the conjugacy classes of subgroups of G.

The transitive permutation group G (or transitive action of G) on the set Ω, with $|\Omega| > 1$, is *primitive* if there is no partition of Ω preserved by G except for the two trivial partitions (the partition with a single part, and the partition into singletons). It is easy to show that

> The action of G on the set of right cosets of H by right multiplication is primitive if and only if H is a maximal proper subgroup of G.

Thus, determining the primitive actions of G is equivalent to determining the conjugacy classes of maximal subgroups of G.

The *O'Nan–Scott Theorem*, which is explained below, shows that many cases of this problem can be reduced to dealing with groups G which are *almost simple*: this will be explained later.

In this essay, we explain the O'Nan–Scott Theorem, and give some examples of its use, in conjunction with the Classification of Finite Simple Groups, to obtain important results about primitive groups.

2 Minimal normal subgroups

The *socle* $\mathrm{Soc}(G)$ of a finite group G is the subgroup generated by the minimal (non-trivial) normal subgroups of G. Since the minimal normal subgroups are

pairwise disjoint, they commute in pairs, and the group they generate is their direct product. Moreover, any minimal normal subgroup is itself a direct product of isomorphic simple groups.

The socle of a primitive permutation group is more restricted, however.

Let G be a primitive permutation group on Ω, and let $N_1, N_2, \ldots$ be the minimal (non-identity) normal subgroups of G. Then $N_i \cap N_j = 1$ for $i \neq j$; so N_i and N_j commute for $i \neq j$. Also, each subgroup N_i is transitive. Now the centraliser (in the symmetric group) of a transitive subgroup is semiregular (i.e. the stabilise of any point is trivial), and a semiregular transitive group is regular. We conclude that if G has more than one minimal normal subgroup, then it has two, and both are regular.

Moreover, a regular permutation group N can be regarded as its right regular action (on itself by right multiplication); its centraliser N^* is its left regular action. Then $N \cap N^* = Z(N)$, the centre of N (which consists of elements which act the same on the left and the right). Thus, if G has two minimal normal subgroups, then they are isomorphic, and have trivial centre.

An example of such a group can be made as follows:

- Let S be a finite simple group, and let $G = S \times S$, acting on $\Omega = S$ by the rule
$$(g,h) : x \mapsto g^{-1}xh.$$
The two direct factors are minimal normal subgroups of G; so $\mathrm{Soc}(G) = G$.

If G has a unique minimal normal subgroup, then this subgroup may be abelian and regular, non-abelian and regular, or non-abelian and non-regular. Examples of each type exist:

- The *affine group*
$$\mathrm{AGL}(n,q) = \{x \mapsto xA + c : A \in \mathrm{GL}(n,q), c \in \mathrm{GF}(q)^n\}$$
of permutations of the vector space $\mathrm{GF}(q)^n$: the minimal normal subgroup is the *translation group* $\{x \mapsto x + c : c \in \mathrm{GF}(q)\}$ isomorphic to the additive group of the vector space.

- For the second type, examples are the *twisted wreath products* constructed by Aschbacher. The smallest such group has degree 60^6, with minimal normal subgroup A_5^6.

- The *symmetric group* S_n (for $n \geq 5$) has the *alternating group* A_n as its unique minimal normal subgroup.

The O'Nan–Scott Theorem examines the situation more carefully. (For a proof of the theorem, we refer to Dixon and Mortimer [4].)

3 O'Nan–Scott I: non-basic groups

Let m and r be positive integers. The *Hamming scheme* $H(m,r)$ is the structure whose points are all the r-tuples from an alphabet of size m, where a pair of points satisfy the ith relation (or lie at distance i) if the corresponding tuples differ in i places, for $0 \leq i \leq r$.

This structure is an *association scheme* (see the topic essay on this subject for details), and indeed is one of the most important types of association schemes, both for theory and applications.

It can be shown that any automorphism of $H(m,r)$ is a product of two types of automorphisms:

- Let $g_1, \ldots, g_r$ be arbitrary permutations of the alphabet. Then there is an automorphism of $H(n,r)$ where the tuple $(x_1, \ldots, x_r)$ is mapped to $(x_1^{g_1}, \ldots, x_r^{g_r})$.
- Any element of the symmetric group of degree r acts on $H(n,r)$ by permuting the coordinates.

The full automorphism group of $H(m,r)$ is the *wreath product* $S_m \operatorname{wr} S_r$. The two types of automorphisms form subgroups, known respectively as the *base group* and the *top group* of the wreath product. The automorphism group acts primitively on the points of the Hamming scheme if $m > 2$. (For $m = 2$, the Hamming scheme is the r-dimensional cube, and the relation of being antipodal and the relation of being at even distance are both equivalence relations preserved by all automorphisms.)

A primitive permutation group G on Ω is said to be *non-basic* if Ω can be identified with the point set of a Hamming scheme $H(m,r)$ (with $m > 1$ and $r > 2$) in such a way that G acts as a group of automorphisms. If G is non-basic, then there is a sense in which it can be built out of smaller permutation groups (of degrees m and r), in much the same way as for intransitive and imprimitive groups, as in the topic essay *Permutation groups*: specifically, G is a subgroup of $H \operatorname{wr} K$, where H is the group of permutations induced on the symbols in one coordinate,

and K the group of coordinate permutations induced by G. It can be shown that the permutation group H, of degree m, is primitive and not regular, while K is transitive.

The relevant part of the O'Nan–Scott Theorem for this situation asserts that we retain control of the socle in this case:

> *If G is primitive and non-basic, and $G \leq H \operatorname{wr} K$ as above, then the socle of G has the form N^r, where N is either the socle or a minimal normal subgroup of H.*

In general, we have $\mathrm{Soc}(G) = \mathrm{Soc}(H)^r$. If this is not true, then H is a group with two minimal normal subgroups N and N^*, each of which is regular; and G has a unique minimal normal subgroup N^r, which is regular on Ω. This, as we saw, is the *twisted wreath product* case. So $\mathrm{Soc}(G) = \mathrm{Soc}(H)^r$ except in this case.

4 O'Nan–Scott II: basic groups

By a reduction of the type in the preceding section, we eventually arrive at a primitive basic group. The second part of the O'Nan–Scott Theorem describes such groups and how their socles act. We will see that the three types of groups we saw earlier are fairly typical.

- A primitive permutation group G is of *affine type* if it has an abelian regular normal subgroup (necessarily elementary abelian of order p^d for some prime p). Such a group is embedded in the affine group $\mathrm{AGL}(d,p)$, and its socle is the translation subgroup. The stabiliser of the zero vector is a subgroup H of $\mathrm{GL}(d,p)$ which acts irreducibly on the vector space $V = \mathrm{GF}(p)^d$. It can be shown that G is basic if and only if H is a *primitive linear group*, that is, there is no decomposition of V as a direct sum whose summands are permuted by H).

- A primitive permutation group G is of *diagonal type* if its socle has the form $N = T^d$ for some $d > 1$, where T is a non-abelian simple group, such that the stabiliser of a point in N is the *diagonal subgroup*

$$D = \{(t,t,\ldots,t) : t \in T\}.$$

  The largest group with such a socle is obtained by adjoining to N the outer automorphisms of T (acting in the same way on each coordinate) and the coordinate permutations.

- A group G is *almost simple* if the socle of G is non-abelian simple. This means that $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group T.

Now the second part of the O'Nan–Scott Theorem asserts:

> *A basic primitive group is of affine or diagonal type or is almost simple.*

Note that we have described the action of the socle completely in the case of the affine and diagonal types, but have said nothing at all about it in the almost simple case. As noted earlier, finding the primitive actions of the almost simple groups is equivalent to classifying their maximal subgroups up to conjugacy. To progress further, we need to know more about the simple groups. It turns out that such knowledge is also important for finding the irreducible (or primitive) linear groups, which we need to determine the groups of affine type.

5 The Classification of Finite Simple Groups

After a huge international effort stretching over many years, the non-abelian simple groups have been classified:

> *A non-abelian finite simple group is an alternating group, a group of Lie type, or one of* 26 *"sporadic groups".*

The richest class consists of the groups of Lie type. These are, roughly speaking, matrix groups over finite fields factored by the subgroup consisting of scalar matrices. For example, $\mathrm{PSL}(n,q)$ is obtained by taking the group of $n \times n$ matrices over $\mathrm{GF}(q)$ having determinant 1 and factoring by the scalar matrices. It is simple except in the two cases $(n,q) = (2,2)$ and $(n,q) = (2,3)$.

An account of the classification, and some properties of the simple groups, can be found in [5].

6 Applications

Now we have a machine which is capable of answering many questions about primitive permutation groups. Here are a few of the theorems which have been found. For more details see [1, 4] and the references cited therein.

- All the 2-transitive groups are known. (A group is 2-*transitive* if any ordered pair of distinct points can be mapped to any other by some element of the group.) Using this knowledge, all t-transitive groups (analogously defined) can be determined for $t > 2$.

- All the primitive groups of rank 3 are known. (The *rank* of a permutation group is the number of its orbits on the set of all ordered pairs. So the rank 3 groups are those which are either

  – transitive on the 2-subsets but not 2-transitive; or

  – transitive on ordered edges and ordered non-edges of a graph.)

  See [6].

- Questions about the maximality of one primitive group in another have been resolved [7].

- It is known that primitive groups are both

  – *rare* (for almost all n, the only primitive groups of degree n are the symmetric and alternating groups, see [2]); and

  – *small* (of order at most $n^{c \log n}$ with known exceptions), see [9] for the best possible result here.

- The graph isomorphism problem is solvable in polynomial time for graphs of bounded valency [8].

We mention briefly an application taken from [3]. It is not hard to show that, if the permutation group G acts block-transitively on a t-design, and H is a supergroup of G in the symmetric group, then H also acts block-transitively on a t-design with the same block size (but possibly larger λ). So, in order to determine the possible (v,k,t) for which non-trivial block-transitive t-designs exist, it is enough to consider maximal subgroups of the symmetric or alternating group. Using the O'Nan–Scott Theorem and the Classification of Finite Simple Groups, it can be shown (for example) that necessarily $t \leq 7$ here (though in fact no examples with $t > 5$ are known).

References

[1] Peter J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts **45**, Cambridge University Press, Cambridge, 1999.

[2] Peter J. Cameron, Peter M. Neumann and D. N. Teague, On the degrees of primitive permutation groups, *Math. Z.* **180** (1982), 141–149.

[3] P. J. Cameron and C. E. Praeger, Block-transitive t-designs, II: large t, in *Finite Geometry and Combinatorics* (ed. A. Beutelspacher *et al.*), Cambridge University Press, 1993, pp. 103–119.

[4] John D. Dixon and Brian Mortimer, *Permutation Groups*, Springer, 1996.

[5] D. Gorenstein, *Finite Simple Groups: An Introduction to their Classification*, Plenum Press, New York, 1982.

[6] Martin W. Liebeck, The affine permutation groups of rank 3, *Proc. London Math. Soc.* (3) **54** (1987), 477–516.

[7] Martin W. Liebeck, Cheryl E. Praeger and Jan Saxl, The classification of the maximal subgroups of the finite symmetric and alternating groups, *J. Algebra* **111** (1987), 365–383.

[8] Eugene M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Comput. Syst. Sci.* **25** (1982), 42-65.

[9] Attila Maróti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631–640.

Peter J. Cameron

August 27, 2004