Derangements

Peter J. Cameron
University of St Andrews

26 January 2017

For [Luck] your science finds no measuring-rods;...
Her permutations never know truce nor pause

Dante Alighieri, *Commedia I: Inferno*

Derangements in transitive permutation groups

This is an Australia Day celebration: the work was done by Michael Giudici, Gordon Royle, Rosemary and me last September in Perth.
Let G be a transitive permutation group of degree n, where $n > 1$.

- G contains a derangement. (Jordan 1872)
- G contains a derangement of prime power order. (Fein, Kantor and Schacher 1982: uses CFSG)
- The number of derangements in G is at least $|G|/n$. (Cameron and Cohen, 1992)
- To what extent is G determined by its derangements? (Question to Michael Giudici, Iran, 2016).

Frobenius groups

A Frobenius group is a transitive group in which the stabiliser of any two points is the identity.
In a Frobenius group G of degree n,

- the identity and the derangements form a normal subgroup N of order n (the Frobenius kernel);
- G/N is isomorphic to a point stabiliser (a Frobenius complement), and has order dividing $n-1$;
- the structure of N and G/N is very restricted (N is nilpotent, G/N is metacyclic or involves $\mathrm{SL}(2,3)$ or $\mathrm{SL}(2,5)$).

The bound in the second part is attained, e.g. by the group

$$\mathrm{AGL}(1,q) = \{x \mapsto ax+b : a,b \in \mathrm{GF}(q), a \neq 0\}.$$

The subgroup generated by derangements

One way to make the question precise is to ask: Let $D(G)$ be the subgroup generated by derangements. (Note that it is a normal subgroup.) How large is $D(G)$, and when is it equal to G?
Note that, if G is a Frobenius group, then $D(G)$ is the Frobenius kernel, and $G/D(G)$ is isomorphic to the Frobenius complement.
Some statistics:

- of the 3302368 transitive groups of degree from 2 to 47 inclusive, only 885 have $D(G) \neq G$ (of which 103 are Frobenius groups);
- of the 24558 primitive groups of degree from 2 to 4095 inclusive, only 9155 have $D(G) \neq G$ (of which 7872 are Frobenius groups).

Theorem

- $D(G)$ *is transitive.*
- $D(G)$ *contains every element of* G *whose number of fixed points is different from* 1.
- *If* r_G *and* $r_{D(G)}$ *denote the permutation ranks of* G *and* $D(G)$*, then*

$$r_{D(G)} - 1 = (r_G - 1)|G : D(G)|.$$

- *The* $D(G)$*-orbits on ordered pairs of distinct elements are permuted semiregularly by* $G/D(G)$.

[The rank of a transitive permutation group is the number of orbits of the point stabiliser.]
The first two parts are due to Zantema (1982). Proofs follow.

Proofs

Let $\mathrm{fix}(g)$ be the number of fixed points of G, and let $D(G)$ have m orbits. By the Orbit-counting Lemma we have

$$\begin{aligned} \sum_{g \in G} (\mathrm{fix}(g) - 1) &= 0, \\ \sum_{g \in D(G)} (\mathrm{fix}(g) - 1) &= (m-1)|D(G)|, \end{aligned}$$

so

$$\sum_{g \in G \setminus D(G)} \mathrm{fix}(g) - 1 = -(m-1)|D(G)|.$$

But the left-hand side is ≥ 0, while the right is ≤ 0. The first two parts of the theorem follow.

The rank of a transitive group is the number of its orbits on ordered pairs. We have

$$\begin{aligned} |G|(r_G - 1) &= \sum_{g \in G} (\mathrm{fix}(g) - 1)^2, \\ |D(G)|(r_{D(G)} - 1) &= \sum_{g \in D(G)} (\mathrm{fix}(g) - 1)^2. \end{aligned}$$

Since every element of $G \setminus D(G)$ has $\mathrm{fix}(g) = 1$, the two displayed expressions are equal, which proves the third part. The last part follows easily.

How large can $|G : D(G)|$ be?

It follows from what we have shown that this index divides $n - 1$. Equality holds for sharply 2-transitive groups, for example the affine group $\mathrm{AGL}(1, q)$. Subgroups of this group realise all divisors of $n - 1$ (in the case where n is a prime power).

Conjecture

If G is transitive but not a Frobenius group, then $|G : D(G)| \leq \sqrt{n} - 1$.

This is easy to prove for imprimitive groups, so we may suppose that G is primitive.
We succeeded in proving this in all cases except affine primitive groups.

What about $G/D(G)$?

Question

What groups H can occur as $G/D(G)$ for some transitive group G?

Considering Frobenius groups, we see that any Frobenius complement can occur. These groups are rather restricted, as we saw.

We found to our surprise that other groups can occur. For example, the Klein group V_4 and the symmetric group S_3 are both realised as $G/D(G)$ for primitive groups of degree $5^4 = 625$ (numbers 41 and 113 in the Magma list).

Does every finite group occur??