Derangements

Peter Cameron

Last term, Taoyang Wu showed us a proof that deciding whether a subgroup G of the symmetric group S_n with given generators contains a derangement (a fixed-point-free element) is NP-complete. If the group G is transitive, then a theorem of Jordan guarantees that the answer is "yes", so the decision problem is trivial. I don't know a deterministic polynomial-time algorithm to find a derangement. However, there is a simple randomised algorithm which finds one with high probability in polynomial time.

I will also talk about some other problems on derangements:

- What if we require that the derangement should have prime-power (or prime) order?
- Given a derangement g, how many Latin squares of order n have first row the identity and second row g? Computational results suggest that the number is approximately independent of the chosen derangement.