Finding a derangement

Peter Cameron

A derangement is a permutation with no fixed points.

An elementary theorem of Jordan asserts that a transitive permutation group of degree $n > 1$ contains a derangement. Arjeh Cohen and I showed that in fact at least a fraction $1/n$ of the elements of the group are derangements. So there is a simple and efficient randomised algorithm to find one: just keep picking random elements until you succeed.

Bill Kantor improved Jordan's theorem to the statement that a transitive group contains a derangement of prime power order. The theorem is constructive but requires the classification of finite simple groups. Emil Vaughan showed that Kantor's theorem yields a polynomial-time (but not at all straightforward) algorithm for finding one.

This month, Vikraman Arvind from Chennai posted a paper on the arXiv giving a very simple deterministic polynomial-time algorithm to find a derangement in a transitive group. The proof is elementary and combinatorial.