Permutations

Peter J. Cameron
School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS
U.K.

Paul Erdős Memorial Conference
Budapest, Hungary
5 July 1999

Erdős and Turán on random permutations

P. Erdős and P. Turán, On some problems of a statistical group theory,
I, *Z. Wahrscheinlichkeitstheorie und Verw. Gebeite* **4** (1965), 175–186;
II, *Acta Math. Acad. Sci. Hungar.* **18** (1967), 151–164;
III, *ibid.* **18** (1967), 309–320;
IV, *ibid.* **19** (1968), 413–435;
V, *Period. Math. Hungar.* **1** (1971), 5–13;
VI, *J. Indian Math. Soc.* (N.S.) **34** (1971), 175–192;
VII, *Period. Math. Hungar.* **2** (1972), 149–163.

Extremal problems

How many permutations in a set (or group) with prescribed distances?

The *distance* between permutations $g,h \in S_n$ is the number of positions where g and h disagree (this is $n - \mathrm{fix}(g^{-1}h)$).

For $S \subseteq \{0,\dots,n-2\}$, let $f_S(n)$ be the size of the largest subset X of S_n with $\mathrm{fix}(g^{-1}h) \in S$ for all distinct $g,h \in X$; for $s < n$, let $f_s(n)$ be the size of the largest s-distance subset of S_n. Let $f_S^g(n)$ and $f_s^g(n)$ be the corresponding numbers for subgroups of S_n.

Results and problems

Theorem $(c_1 n/s)^{2s} \le f_s(n) \le (c_2 n/s)^{2s}$.

Problem Does $s(f_s(n))^{1/2s} \sim cn$ as $n \to \infty$? (for fixed s, or for $s \to \infty$).

Theorem (Blichfeldt) $f_S^g(n)$ divides

$$\prod_{s \in S} (n-s).$$

Problem Which groups attain Blichfeldt's bound?

Problem Is it true that

$$f_S(n) \le \prod_{s \in S} (n-s)$$

for S fixed, n large?

A specific problem

Theorem (Blake–Cohen–Deza) If $S = \{0, 1, \ldots, t-1\}$, then

$$f_S(n) \leq n(n-1)\cdots(n-t+1).$$

Equality holds if and only if a *sharply t-transitive set* of permutations exists.

Theorem If $S' = \{0, \ldots, n-1\} \setminus S$ then

$$f_S(n) \cdot f_{S'}(n) \leq n!.$$

Problem If $S = \{t, \ldots, n-1\}$, is $f_S(n) \leq (n-t)!$ for n large relative to t?
(The extremal configuration should be a coset of the stabiliser of t points.)

The bound holds if a sharply t-transitive set exists. Compare the Erdős–Ko–Rado theorem.

Derangements and Latin squares

A *derangement* is a permutation which has no fixed points. It is well-known that the number of derangements in S_n is the nearest integer to $n!/\mathrm{e}$.

If a Latin square of order n is normalised so that the first row is $(1\,2\,\ldots\,n)$, then the other rows are derangements.

Every derangement occurs as the second row of a normalised Latin square.

Problem Is it true that the distribution of the number of rows of a random Latin square which are even permutations is approximately binomial $B(n, \frac{1}{2})$?

Derangements and Latin squares, continued

Problem Choose a random permutation π as follows: select a Latin square from the uniform distribution, normalise, and let π be the second row. (So the permutations which occur with positive probability are the derangements.)

- How does the ratio of the probability of the most and least likely derangement behave?

- Is it true that, with probability tending to 1, a random derangement lies in no transitive subgroup of S_n except S_n and possibly A_n?

Derangements of prime power order

Theorem (Frobenius) A non-trivial finite transitive permutation group contains a derangement.

Theorem (Kantor [CFSG]) A non-trivial finite transitive permutation group contains a derangement of prime power order.

Problem (Isbell) Is it true that, if a is sufficiently large in terms of p and b (p prime), then a transitive permutation group of degree $n = p^a \cdot b$ contains a derangement of p-power order?

Derangements of prime order

Call G *elusive* if it is transitive and contains no derangement of prime order.

Theorem (Giudici [CFSG]) A quasiprimitive elusive group is isomorphic to $M_{11} \wr H$ for some transitive group H.

Problem Does the set of degrees of elusive groups have density zero? (This set contains $2n$ for every even perfect number n, and is multiplicatively closed.)

Problem (Jordan, Marušič) Show that the automorphism group of a vertex-transitive graph is non-elusive.

Bertrand, Sylvester and Erdős

Bertrand's Postulate was proposed for an application to permutation groups. The first published paper of Paul Erdős was a short proof of Bertrand's Postulate.

Sylvester generalised Bertrand's Postulate as follows:

Theorem The product of k consecutive numbers greater than k is divisible by a prime greater than k.

Erdős also gave a short proof of this. It deals with a case in the proof of Giudici's Theorem which cannot be handled by group-theoretic methods, where G is a symmetric or alternating group in its action on k-element subsets. Sylvester's Theorem gives a derangement of prime order in this case.

Counting orbits

The *orbit-counting lemma* asserts that the number of orbits of a finite permutation group G is equal to the average number of fixed points of elements of G. It is proved by counting edges in the bipartite graph on $\{1,\ldots,n\} \cup G$, where i is joined to g if g fixes i.

Jerrum's Markov chain on $\{1,\ldots,n\}$: one step consists of two steps in a random walk on the graph. The limiting distribution is uniform on the orbits. This gives a method for choosing random 'unlabelled' structures.

Problem For which families of permutation groups is this Markov chain rapidly mixing?

An infinite analogue

There is no natural way to choose a random permutation of a countable set, since the symmetric group is not compact.

Parallels:

- The countable random graph (the generic countable graph), Erdős and Rényi.
- A permutation of a finite set is given by a pair of total orders of the set.

So instead of the random permutation, consider the generic pair (or n-tuple) of total orders. Note that the generic (or random) total order is isomorphic to $\mathbf{Q}$.