Random Permutations: Some Group-Theoretic Aspects

PETER J. CAMERON[†] and WILLIAM M. KANTOR[‡]

[†]School of Mathematical Sciences, Queen Mary and Westfield College,
Mile End Road, London E1 4NS, U.K.

[‡]Department of Mathematics, University of Oregon, Eugene, OR 97403, U.S.A.

The study of asymptotics of random permutations was initiated by Erdős and Turán, in a series of papers from 1965 to 1968, and has been much studied since. Recent developments in permutation group theory make it reasonable to ask questions with a more group-theoretic flavour. Two examples considered here are membership in a proper transitive subgroup, and the intersection of a subgroup with a random conjugate. These both arise from other topics (quasigroups, bases for permutation groups, and design constructions).

1. Permutations lying in a transitive subgroup

S_n and A_n denote the symmetric and alternating groups on the set $X = \{1, \ldots, n\}$. A subgroup G of S_n is *transitive* if, for all $i, j \in X$, there exists $g \in G$ with $ig = j$. In a preliminary version of this paper, we asked the following question:

Question 1.1. *Is it true that, for almost all permutations $g \in S_n$, the only transitive subgroups containing g are S_n and (possibly) A_n?*

Here, of course, 'almost all $g \in S_n$ have property P' means 'the proportion of elements of S_n not having property P tends to 0 as $n \to \infty$'.

An affirmative answer to this question was given by Łuczak and Pyber, in [15]. We will discuss the motivation for this question, and speculate on the rate of convergence.

To analyse the question, we make the customary division of transitive subgroups into imprimitive and primitive ones. A subgroup G is *imprimitive* if it leaves invariant some non-trivial partition of X, and *primitive* otherwise. Imprimitive subgroups may be large, but the maximal ones are relatively few in number: just $d(n) - 2$ conjugacy classes, where $d(n)$ is the number of divisors of n. (If the permutation g lies in an imprimitive subgroup, then it lies in a maximal one, which is precisely the stabiliser of a partition of X into s parts of size r, where $rs = n$ and $r, s > 1$.) On the other hand, primitive groups are more mysterious; but it follows from the classification of finite simple groups that

-- they are *scarce* (for almost all n, the only primitive groups are S_n and A_n, see [3]);
— they are *small* (order at most $n^{c \log\log n}$ with 'known' exceptions, see [1]).

In addition, many special classes of primitive groups (for example, the doubly transitive groups), have been completely classified.

The number of permutations that lie in some primitive subgroup other than S_n or A_n can be bounded, since such permutations have quite restricted cycle structure (a consequence of minimal degree bounds, see [14] -- note that these bounds are a consequence of the classification of finite simple groups – or by more elementary means, as Łuczak and Pyber [15] do). So we will concentrate on imprimitive subgroups, and, in particular, the largest imprimitive subgroups: those preserving a partition of X into two sets of size $n/2$, for n even.

A permutation fixing such a partition must either fix some $(n/2)$-set, or interchange some $(n/2)$-set with its complement. Now a permutation interchanges some $(n/2)$-set with its complement if and only if all its cycles have even length. The number of such permutations is

$$((n-1)!!)^2 = ((n-1)(n-3)\dots 3.1)^2,$$

which is easily seen to be $n!O(1/\sqrt{n})$. (This formula is easily proved using generating function methods. A 'counting' proof is given in [2]. Curiously, it is equal to the number of permutations with all cycles of odd length, see [7, 8, 9, 10]. We are not aware of a 'counting' proof of this coincidence!)

On the other hand, a permutation fixes an $(n/2)$-set if and only if some subfamily of its cycle lengths has sum $n/2$. There seems to be no simple formula for the number of such permutations; but Łuczak and Pyber show that their proportion is at most An^{-c}, where A and c are positive constants. Indeed, more generally, the proportion of permutations fixing some k-set tends to 0 as $k \to \infty$ (as long as $n \geq 2k$).

We turn now to the motivation for this question. A *quasigroup* is a set with a binary multiplication in which left and right division are uniquely defined (equivalently, the multiplication table is a Latin square). In a quasigroup Q, left and right translations are permutations, represented by the rows and columns of the multiplication table of Q. The *multiplication group* $\mathrm{Mlt}(Q)$ of Q is the group generated by these permutations. This group 'controls' the character theory of Q [16]. In particular, if $\mathrm{Mlt}(Q)$ is 2-transitive, then the character theory of Q is trivial. Smith conjectured that this happens most of the time, and this is indeed true.

Theorem 1.2. *For almost all Latin squares A, the group generated by the rows of A is the symmetric or alternating group.*

This is proved in [2], but follows more directly from the affirmative answer to Question 1.1, since the rows of a Latin square obviously generate a transitive permutation group, and the first row of a random Latin square is a random permutation (that is, all permutations occur equally often as first rows of Latin squares).

This suggests several related questions:

1 Is it true that, for almost all Latin squares, the first two rows generate the symmetric or alternating group? (By a theorem of Dixon [4], almost all pairs of permutations generate S_n or A_n; and a positive proportion of these (1/e, in the limit) have the property that the second is a derangement of the first, and hence occur as the first two rows of a Latin square. But not all derangements occur equally often.) More generally, study further the probability distribution on derangements induced by their frequency of occurrence in Latin squares. What is the ratio of the greatest to the smallest number of completions?

2 Is it true that the multiplication groups of almost all loops are symmetric or alternating? (A *loop* is a quasigroup with identity. Thus we are requiring that the first row and column of the Latin square correspond to the identity permutation, and the deduction of the analogue of Theorem 1.2 from Question 1.1 fails.)

3 What proportion of Latin squares have the property that all the rows are even permutations? (If the limit is zero, the alternating group can be struck out from the conclusion to Theorem 1.2.)

4 Is the proportion of permutations that do lie in a proper transitive subgroup $O(n^{-1/2})$? (By our remarks above, this would be best possible.)

2. Bases and intersections of conjugates

Introducing the next topic requires a fairly long detour. Let G be a permutation group on a set X. A *base* for G is a sequence $(x_1, \dots, x_r)$ of points of X whose pointwise stabiliser is the identity. It is *irredundant* if no point is fixed by the pointwise stabiliser of its predecessors. Bases are of interest in several fields, including computational group theory.

If G has an irredundant base of size r, then $2^r \leq |G| \leq n(n-1)\dots(n-r+1)$, whence $\log_n |G| \leq r \leq \log_2 |G|$. It is easy to construct examples at or near either side of this inequality. Nevertheless, it is thought that, for many interesting groups, the base size is closer to the lower bound. In particular, certain primitive groups whose order is polynomially bounded should have bases of constant size.

To elucidate this, we look more closely at primitive groups. The *O'Nan–Scott theorem* (see [1]) divides these into several classes. All but one of these classes consist of groups that can be 'reduced' in some way to smaller ones or studied by other means. The one class left over consists of groups G that are *almost simple* (that is, that have a non-abelian simple normal subgroup N such that G is contained in $\mathrm{Aut}(N)$). Using the classification of finite simple groups, it is possible to make some general statements about almost simple primitive groups. For example, the following result holds (see [1, 12]; the latter paper gives $c = 8$).

Theorem 2.1. *There is a constant c with the following property. Let G be an almost simple primitive permutation group of degree n. Then either* *(a) G is known (specifically, G is a symmetric or alternating group S_m or A_m, acting on the set of k-subsets of $\{1,\dots,m\}$ or on the set of partitions of $\{1,\dots,m\}$ into s parts of size r, or G is a classical group, acting on an orbit of subspaces of its natural module or on an orbit of pairs of subspaces of complementary dimension); or*

(b) $|G| \leq n^c$.

(The methodological point raised by this and similar theorems is that in the study of finite permutation groups, after the classical divisions into intransitive and transitive groups, and of transitive groups into primitive and imprimitive groups, one should also divide primitive groups into 'large' and 'small' groups, the large ones being 'known' in some sense. This principle applies to both theoretical and computational analysis.)

It is conjectured that *there is a constant c' (perhaps $c' = 3$) such that, if G is almost simple and primitive and does not satisfy (a), then almost every c'-tuple of points is a base for G.*

According to the classification of finite simple groups, the simple normal subgroup N of G is an alternating group, a group of Lie type, or one of the 26 sporadic groups. In the first of these three cases, we were able to prove the conjecture (with $c' = 2$).

Theorem 2.2. *Let G be an almost simple group, not occurring under Theorem 2.1(a). If the simple normal subgroup of G is an alternating group, then almost all pairs of points are bases.*

We outline the proof.

The first observation is that if G is transitive and H is a point stabiliser, the proportion of ordered pairs of points that are bases is equal to the proportion of elements $g \in G$ for which $H \cap H^g = 1$, where H^g is the conjugate $g^{-1}Hg$.

Second, primitivity of G is equivalent to maximality of the subgroup H. Moreover, if $m \neq 6$, then $\mathrm{Aut}(A_m) = S_m$, so we may assume that $G = S_m$ or A_m. Consider H (the point stabiliser in the unknown action) acting on $M = \{1,\dots,m\}$. If H is intransitive, it fixes a k-subset of M for some k; by maximality, it is the stabiliser of this k-set, and the action of G is equivalent to that on k-sets. Similarly, if H is transitive but imprimitive, then it is the stabiliser of a partition, and G acts on partitions of fixed shape. Both of these cases are included under Theorem 2.1(a). So H is primitive on M. (This is an example of the 'bootstrap principle': note that m is much smaller than n.)

Thus, finally, we need a result about random permutations.

Proposition 2.3. *Let H be a primitive subgroup of S_m, not S_m or A_m. Then, for almost all permutations $g \in S_m$, we have $H \cap H^g = 1$.*

This is true, and can be shown by a simple counting argument, except in the case of the largest primitive groups (the automorphism groups of the line graphs of K_r or $K_{r,r}$, with $m = \binom{r}{2}$ or r^2 respectively), where some special pleading is required. In outline: count triples (h,k,g) with $h,k \in H$, $h,k \neq 1$, $g \in G$ and $h^g = k$. The number of such triples is not more than $|H|^2c$, where c is the largest order of the centralizer of a non-identity element in H: and it is not less than the number of elements g with $H \cap H^g \neq 1$. Now use the fact that primitive groups are small, and their elements have relatively few fixed points (and so relatively small centralizers).

Remark. There is an analogy between intersections of conjugates and automorphism groups. (For example, if the group G is the automorphism group of a particular structure S, then the intersections of pairs of conjugates of G represent those groups that can be represented in the following way: impose two copies of the structure S on the underlying set, and consider all those permutations which are automorphisms of both structures simultaneously.)

Thus, Proposition 2.3 should be compared with the statement 'almost all graphs have trivial automorphism group' [6]. As the analogue of Frucht's theorem [11], we propose the following conjecture.

Conjecture 2.4. *Let $G_1, G_2, \ldots$ be primitive groups of degrees $n_1, n_2, \ldots$, where $n_i \to \infty$ and $G_i \neq S_{n_i}$ or A_{n_i} for all i. Let X be an abstract group that is embeddable in G_i for infinitely many values of i. Then, for some i, and some permutation $g \in S_{n_i}$, we have $G_i \cap G_i^g = X$.*

This has been proved by Kantor [13] for the family of groups $G_i = \mathrm{P\Gamma L}(i, q)$, $n_i = (q^i - 1)/(q-1)$, for a fixed prime power q. (In this case, every finite group is embeddable in G_i for all sufficiently large i.) Kantor used this result to show that, for a fixed prime power q, every finite group is the automorphism group of a square 2-$((q^i - 1)/(q-1), (q^{i-1} - 1)/(q-1), (q^{i-2} - 1)/(q-1))$ design for some i.

References

[1] Cameron, P. J. (1981) Finite permutation groups and finite simple groups. *Bull. London Math. Soc.* **13** 1 22.

[2] Cameron, P. J. (1992) Almost all quasigroups have rank 2. *Discrete Math.* **106/107** 111–115.

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

[4] Dixon, J. D. (1969) The probability of generating the symmetric group. *Math. Z.* **110** 199–205.

[5] Donnelly, P. and Grimmett, G. (to appear) On the asymptotic distribution of large prime factors. *J. London Math. Soc.*

[6] Erdős, P. and Rényi, A. (1963) Asymmetric graphs. *Acta Math. Acad. Sci. Hungar.* **14** 295–315.

[7] Erdős, P. and Turán, P. (1965) On some problems of a statistical group theory, I. *Z. Wahrscheinlichkeitstheorie und verw. Gebeite* **4** 175–186.

[8] Erdős, P. and Turán, P. (1967) On some problems of a statistical group theory, II. *Acta Math. Acad. Sci. Hungar.* **18** 151–163.

[9] Erdős, P. and Turán, P. (1967) On some problems of a statistical group theory, III. *Acta Math. Acad. Sci. Hungar.* **18** 309-320.

[10] Erdős, P. and Turán, P. (1968) On some problems of a statistical group theory, IV. *Acta Math. Acad. Sci. Hungar.* **19** 413–435.

[11] Frucht, R. (1938) Herstellung von Graphen mit vorgegebener abstrakter Gruppe. *Compositio Math.* **6** 239–250.

[12] Kantor, W. M. (1988) Algorithms for Sylow p-subgroups and solvable groups. *Computers in Algebra* (Proc. Conf. Chicago 1985), Dekker, New York 77–90.

[13] Kantor, W. M. (to appear) Automorphisms and isomorphisms of symmetric and affine designs. *J. Algebraic Combinatorics.*

[14] Liebeck, M. W. and Saxl, J. (1991) Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc.* (2) **63** 266–314.

[15] Łuczak, T. and Pyber, L. (to appear) *Combinatorics, Probability and Computing.*

[16] Smith, J. D. H. (1986) *Representation Theory of Infinite Groups and Finite Quasigroups*, Sém. Math. Sup., Presses Univ. Montréal, Montréal.