Permutations

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

Abstract

This paper is a survey of some combinatorial problems related to permutations and permutation groups. It is inspired by the work of Paul Erdős in two ways. One one hand, I present some partial extensions of the seminal work of Erdős and Turán on random permutations, to groups other than the symmetric group. On the other, many of the topics considered can be regarded as analogues for sets of permutations of results on set-systems (or hypergraphs) springing from the Erdős–Ko–Rado theorem.

I begin with the celebrated Orbit-Counting Lemma, and a generalisation which connect orbits of a group on n-tuples with the probability generating function for fixed points of its elements. Various results and problems on derangements (fixed-point-free elements) are also given. In the next section, I turn from fixed points to cycles. Observing that the cycle index is the probability generating function for cycle structure, we recover the earlier theorem, as well as a recent result of Parker. Next I survey some extremal results for sets or groups of permutations with prescribed distances (distance being defined in terms of fixed points). After a brief discussion of the semilattice of subpermutations (partial permutations), I conclude with a concept to replace that of "random permutation" in the infinite case: for countable sets, there is a unique such object (this is the analogue of the Erdős–Rényi theorem on the countable random graph).

1 Introduction

The fundamental objects with which combinatorics deals are subsets, partitions and permutations. In a sense, these form a hierarchy: a partition is a set of subsets, and the cycles of a permutation form a partition. The sort of combinatorics that Paul Erdős enjoyed (extremal problems, questions about random objects, Ramsey-type theorems) is most developed at the bottom of the hierarchy, while questions of a more algebraic nature become prominent as we ascend. Nevertheless, Erdős, with Paul Turán, pioneered the study of properties of random permutations in a series of important papers [42, 29].

The mixture of algebra and combinatorics is always a potent brew. Where the set of objects forms a group, we can investigate its subgroups, and develop a richer theory than that for arbitrary subsets. For subsets of a set, we can take the group operation to be symmetric difference, and we obtain the theory of binary linear codes. For permutations, the natural operation is composition, and we obtain the theory of permutation groups, which has been of central importance in group theory since its beginnings. Some natural extremal problems in this area are a century old and still unsolved.

Subsets and partitions of a set naturally form lattices. There is no natural order on permutations. (The *Bruhat order*, see [58], requires an order on the underlying set). However, if we adjoin the *subpermutations* or bijections between subsets, we obtain a meet-semilattice which also has an algebraic structure (it is an inverse semigroup).

In this paper, I will survey some questions about permutations, sets of permutations, and permutation groups. If the legacy of Paul Erdős is not always apparent in the details, it is obvious in the contours of the landscape we survey. I have also followed Erdős in giving prominence to unsolved problems.

2 Fixed points and orbits

The *Orbit-Counting Lemma* (often attributed to Burnside, though not originally proved by him) asserts that the number of orbits of a permutation group is equal to the average number of fixed points of its elements. This is fundamental to the theory of enumeration under group action, but has other aspects too.

The Orbit-Counting Lemma is proved by counting in two ways the edges of the bipartite graph B on $X \cup G$, where X is the set on which G acts, and $\{x, g\}$ is an edge if and only if g fixes the point x.

Jerrum [64] has extended this simple idea to a Markov chain to choose a random orbit of G on X. Start with a point of X chosen from any distribution. One step in the chain consists in moving to a random neighbour g of x, and then to a random neighbour x' of g. This Markov chain is irreducible and aperiodic. The same analysis that proves the Orbit-Counting Lemma shows that, in its limiting distribution, the probability of x is inversely proportional to the size of the orbit of x; in other words, all orbits are equally likely.

This raises the question: how fast does the process converge? Goldberg and Jerrum [51] have found examples of group actions for which it is not rapidly mixing.

Problem 1. Find classes of groups for which Jerrum's Markov chain is rapidly mixing.

In the symmetric group S_n, the average number of fixed points is one. As we will see shortly, the distribution of fixed point numbers is approximately Poisson with mean one: that is, the probability that a random element has k fixed points, where k is constant or grows more slowly than n, is about $1/(\mathrm{e}k!)$. For $k = 0$, this is the *derangement problem* of elementary combinatorics.

Probably the simplest way to see this uses a generalisation of the Orbit-Counting Lemma due to Boston *et al.* [13]. To state it, we need some notation. Let G be a permutation group (a subgroup of S_n). Let

$$P(x) = \sum_{i=0}^{n} p_i x^i$$

be the probability generating function for the number of fixed points of a random element of G (that is, p_i is the proportion of elements of G having i fixed points). Also, let F_i be the number of orbits of G on ordered i-tuples of distinct points, with $F_0 = 1$ by convention, and let

$$F(x) = \sum_{i=0}^{n} \frac{F_i x^i}{i!}$$

be the exponential generating function for these numbers.

Theorem 2.1 $F(x) = P(x + 1)$.

The proof of this striking result is elementary: the Orbit-Counting Lemma applied to the action of G on ordered i-tuples gives

$$F_i = \sum_{j=i}^{n} p_j j(j-1)\cdots(j-i+1),$$

and the rest is simple manipulation. Note, in particular, that the proportion of *derangements* (fixed-point-free elements) in G is given by $F(-1)$.

For example, in S_n, we have $F_i = 1$ for $i \leq n$, so $F(x)$ is the Taylor series for e^x truncated to degree n. The facts about the distribution of number of fixed points, and the formula for the number of derangements, are immediate consequences.

The method can be extended to other permutation groups, since it is often easier to count orbits than fixed points. For example, the projective group $\mathrm{PGL}(2,q)$, for prime-powers q, has degree $n = q+1$ and has $F_0 = F_1 = F_2 = F_3 = 1$ and $F_i = (n-3)(n-4)\cdots(n-i+1)$ for $i \geq 4$, from which $P(x)$ is easily calculated. The paper [13] gives several other examples.

The method also can be used to calculate the number of derangements of each parity. The alternating group A_n has one orbit on i-tuples for $i \leq n-2$ and two for $i = n-1, n$; so

$$F_{A_n}(x) = F_{S_n}(x) + \frac{x^{n-1}}{(n-1)!} + \frac{x^n}{n!}.$$

Putting $x = -1$, we find that

$$d_n^- = d_n^+ + (-1)^n(n-1), \tag{1}$$

where d_n^+ and d_n^- are the numbers of derangements with even and odd parity respectively. Eceğlioğlu [35] asked for a bijective proof of Equation (1). This was given by Robin Chapman [28], to whom the following is due.

Let D_n the be set of derangements. We can split this set into $n-1$ equal parts according to where the permutation sends n. We look therefore only at $D_n' = \{\sigma \in D_n : \sigma(n) = n-1\}$. Define a sign-reversing involution on the set $D_n' \setminus \{(1\ 2\ 3\ \ldots\ n-2\ n\ n-1)\}$. This will give us what we want.

For $\sigma \in D_n'$ let $a(\sigma)$ be the least number a with $\sigma(a) < a$. Then $a(\sigma) < n-1$ with the sole exception $\sigma = (1\ 2\ 3\ \ldots\ n-2\ n\ n-1)$. For all $\sigma \in D_n'$ apart from this one permutation, let $f(\sigma) = (a(\sigma)\ n) \circ \sigma$.

It suffices to show that $\tau = f(\sigma)$ satisfies $\tau \in D_n'$ and $a(\tau) = a(\sigma)$.

First of all $\sigma(n) = n-1$ which is not in $\{a,n\}$, so $\tau(n) = n-1$. Suppose $\tau(j) = j$ for some j. Then $tau(j) \neq \sigma(j)$, so that $\sigma(j) = a$ or n and $\tau(j) = j = n$ or a respectively. But $\sigma(a) < a$, so $j = a$ and $\sigma(j) = n$ is impossible. Also $\tau(n) = n-1 > a$, so that $j = n$ and $\sigma(j) = a$ is impossible. Hence τ lies in D'_n.

If $j < a$, then $\sigma(j) > j$ and $\tau(j)$ equals one of $\sigma(j)$, a and n, all of which exceed j. But $\sigma(a) < a < n$ and so $\tau(a) = \sigma(a) < a$. Hence $a(\tau) = a$.

An important class of groups for which the exact values are not known consists of the symmetric groups S_n acting on k-subsets of $\{1,\ldots,n\}$. Here F_i is the number of k-hypergraphs with i labelled edges and n unlabelled vertices. The proportion p_0 of derangements tends to a limit $a(k)$ for fixed k as $n \to \infty$, but the exact value of the limit is unknown except for very small values of k. (For example, $a(1) = \mathrm{e}^{-1}$, and $a(2) = 2\mathrm{e}^{-3/2}$.)

Problem 2. Investigate the behaviour of the proportion of derangements in the group S_n acting on k-sets. In particular, show that $a(k)$ is an increasing function of k which tends to 1 as $k \to \infty$.

An even more difficult problem is the asymptotic behaviour of the proportion of derangements in S_n acting on k-sets, where k grows with n. This was investigated by Łuczak and Pyber [74]; their result will be discussed later.

For infinite permutation groups, the statistics of fixed-point numbers are in general meaningless. However, there is an important class of groups for which the other side of the equation in Theorem 2.1 can be defined.

A permutation group G is *oligomorphic* if it has only a finite number F_i of orbits on i-tuples of distinct elements for all $i \in \mathbb{N}$. Such groups are significant in part because of the theorem of Engeler [36], Ryll-Nardzewski [94], and Svenonius [98]:

Theorem 2.2 *A countable structure over a first-order language L is $\aleph_0$-categorical (that is, determined up to isomorphism by first-order axioms) if and only if its automorphism group is oligomorphic.*

This is a remarkable relationship between axiomatisability and symmetry.

If G is oligomorphic, then the function $F(x)$ is defined, at least as a formal power series. It may converge at -1, or the value $F(-1)$ may be obtainable by a summation method or by analytic continuation. It clearly cannot be interpreted as the proportion of derangements in G.

For example:

- If G is the symmetric group on an infinite set, then $F_i = 1$ for all i, so $F(x) = \mathrm{e}^x$ and $F(-1) = 1/\mathrm{e}$.

- Let G be the group of order-preserving permutations of $\mathbb{R}$. Then $F_i = i!$, so $F(x) = 1/(1-x)$ and $F(-1) = \frac{1}{2}$.

- Let G be the group of permutations preserving the circular order on the unit circle. Then $F_i = (i-1)!$ for $i > 1$, so $F(x) = 1 - \log(1-x)$, and $F(-1) = 1 - \log 2$.

- Let G be the symmetric group, in its action on the set of k-element subsets. For $k > 1$, the power series $F(x)$ diverges for all $x \neq 0$; yet, by analogy with the case $k = 1$, the appropriate number $F(-1)$ should be the number $a(k)$ defined before Problem 2 (the limiting proportion of derangements in S_n acting on k-sets as $n \to \infty$).

Problem 3. Does the number $F(-1)$ have any meaning in an oligomorphic group (where it can be defined)?

There is yet another aspect of derangements which leads to interesting open problems. Let G be a transitive permutation group of degree $n > 1$. The average number of fixed points of elements of G is 1; and the identity fixes more than one, so some element fixes less than one. In other words, G contains a derangement. This simple observation goes back at least to Frobenius. It can be quantified in various ways. For example, Cameron and Cohen [22] showed that at least a fraction $1/n$ of the elements of G are derangements, and determined all groups meeting the bound; they gave stronger bounds under additional hypotheses, as also did Guralnick and Wang [55].

Problem 4. For which classes of transitive permutation groups is the proportion of derangements bounded away from zero?

Fein, Kantor and Schacher [43] extended this in a different direction. They showed:

Theorem 2.3 *Every finite transitive permutation group of degree greater than* 1 *contains a derangement of prime-power order.*

This is no longer a simple observation, as it requires the Classification of Finite Simple Groups (see [53]) in its proof. But it raises two further questions.

We might expect that, if one prime power is sufficiently dominant in n, there would be a derangement whose order is a power of that prime. More precisely:

Problem 5. Does there exist a function $f(p, b)$ such that, if $n = p^a \cdot b$ where p is prime and $a > f(p, b)$, then any transitive permutation group of degree n contains a derangement of p-power order? If so, what is the magnitude of $f(p, b)$?

The existence of $f(2, b)$ was conjectured by Isbell [60] in 1959 in the context of game theory. It is still open. (Specifically, an n-player *simple game*, in the sense of von Neumann and Morgenstern [85], is a family of subsets (called *winning coalitions*) of an n-set – that is, sets of players which are able to force a win if they cooperate – which is closed under taking supersets and contains one of each complementary pair of subsets. A game is *homogeneous* if it admits a group of automorphisms acting transitively on the set of players – an obvious "fairness" condition. Isbell asked for which n a homogeneous game can exist. It is easy to see that no automorphism of a game can be a derangement of 2-power order, since such an element interchanges some subset with its complement. Conversely, if a transitive group contains no derangement of 2-power order, then it is contained in the automorphism group of a homogeneous game.)

It is easy to show that a transitive group of degree $n = p^a \cdot b$ with $b < p$ contains a fixed-point-free p-element. There are examples of groups of degree $p(p + 1)$ with no fixed-point-free p-element. (Take the 1-dimensional affine group over $\mathrm{GF}(p^2)$, acting on the set of lines of the affine plane over $\mathrm{GF}(p)$. The p-elements are translations, each of which fixes the lines in a parallel class.) The best result so far on the general problem is due to Bereczky [7]:

Theorem 2.4 *Let G be a transitive permutation group of degree $p^a \cdot b$, where p is an odd prime number, $a \geq 2$, and $b < \frac{3}{2}(p+1)$. Then G contains a fixed-point-free p-element.*

It is known that not every transitive group contains a derangement of *prime* order. (There are infinitely many counterexamples; the smallest has degree 12.) Marušič, Jordan and Klin [81, 65] posed variants of the following problem.

Problem 6. Is it true that every transitive 2-*closed* group contains a derangement of prime order? (The group G is 2-closed if every permutation preserving the G-orbits on ordered pairs belongs to G.) In particular, does every vertex-transitive graph (or digraph) admit a fixed-point-free automorphism of prime order?

See Marušič and Scapellato [82] for recent results on this problem. Another approach is to describe transitive groups not containing derangements of prime order. A permutation group G is *quasiprimitive* if every non-trivial normal subgroup is transitive. Michael Giudici [49] has classified the finite quasiprimitive permutation groups containing no derangement of prime order. The Mathieu group M_{11}, in its 3-transitive action of degree 12, is an example of such a group. Giudici showed that any such group is a wreath product $M_{11} \operatorname{Wr} G$ (in its product action), where G is any transitive group. Moreover, no such group can be 2-closed; so Problem 6 is solved for quasiprimitive groups.

I make a digression to discuss Giudici's argument. As in the proof of Theorem 2.3 by Fein, Kantor and Schacher [43], we can reduce to the case where the group G is simple and primitive. (The reduction is a bit more complex, requiring Praeger's version of the O'Nan–Scott Theorem [88].) Thus, we may assume that G is simple, and has a subgroup H which intersects every conjugacy class of elements of prime order (or, for the result of [43], of prime power order). Now we use the Classification of Finite Simple Groups [53] and detailed results about generation of subgroups of simpe groups by particular elements of prime order, to determine the possibilities. In most cases, the arguments of [43], or variants of them, suffice for the stronger result.

There is, however, one case where something new is needed. This occurs when G is the alternating group A_n, and H is the stabiliser of a k-set, where $k < n/2$. We argue as follows. By a theorem of Sylvester [99], the index $|G : H| = \binom{n}{k}$ is divisible by a prime $p > k$. Now G contains an element g of order p, having fewer than k fixed points; such an element fixes no k-set, and so no conjugate of g lies in H.

Sylvester's theorem generalises Bertrand's postulate, which was conjectured by Bertrand for an application in permutation group theory, and provd by Chebyshev in 1850. The first published paper of Paul Erdős [37] was a short proof of Bertrand's postulate, and shortly afterwards [38] he also provided a short proof of Sylvester's theorem. Now the second of these results, like the first, has found an application to permutation groups.

For any Mersenne prime $p = 2^q - 1$, the sharply 2-transitive group $\mathrm{AGL}(1, p^2)$, acting on the $p(p+1)$ lines of the affine plane $\mathrm{AG}(2, p)$, contains no derangements of prime order. (These groups are special cases of those mentioned before Bereczky's Theorem 2.4 above. For $p = 3$, the group is a subgroup of the Mathieu group M_{11}.) The class of transitive groups with no derangements of prime order is closed under direct and wreath products; so the set of degrees of such groups is multiplicatively closed.

Problem 7. Which transitive groups contain no derangement of prime order? In particular, do the degrees of such groups have density 0?

To conclude this section, I mention a theorem of Isaacs, Kantor and Spaltenstein [59] which is similar in appearance to some of the above results.

Theorem 2.5 *Let G be a subgroup of the symmetric group S_n, whose order is divisible by the prime p. Then the probability that a random element of G has order divisible by p is at least $1/n$.*

The authors also determine the groups which attain the bound in this theorem: they are the sharply 2-transitive groups with n a power of p, and the symmetric group S_n in the case where $n = p \geq 5$.

3 Cycles

The obvious gadget for extending our results about fixed points to cycles is the cycle index, whose theory was developed by Redfield, Pólya, de Bruijn, and others. Let $c_k(g)$ be the number of cycles of length k of the permutation g of $\{1, \ldots, n\}$ (so that $\sum k c_k(g) = n$). Let

$$z(g) = s_1^{c_1(g)} \cdots s_n^{c_n(g)},$$

a monomial in the indeterminates $s_1, \ldots, s_n$. For any group G of permutations, the *cycle index* of G is defined to be

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} z(g).$$

Thus $Z(G)$ is a polynomial in $s_1, \ldots, s_n$.

The role of the cycle index in enumeration is well-known. But from our point of view, $Z(G)$ is the probability generating function for the joint distribution of cycle lengths: that is, the coefficient of $s_1^{a_1} \cdots s_n^{a_n}$ is the probability that a random element of G has a_k cycles of length k for $k = 1, \ldots, n$. In particular, the function $P(x)$ of Section 2 (the p.g.f. for fixed points) is given by

$$P(x) = Z(G)(x, 1, \ldots, 1).$$

Now Theorem 2.1 can be generalised if we can give an "orbit-counting" interpretation of $Z(G)(s_1 + 1, \ldots, s_n + 1)$. This is as follows.

Choose representatives for the orbits of G on the power set of $\{1, \ldots, n\}$. For each orbit representative Δ, let $G(\Delta)$ be the group of permutations of Δ induced by elements of G fixing Δ. Now define

$$\tilde{Z}(G) = \sum_{\Delta} Z(G(\Delta)); \tag{2}$$

this is the *modified cycle index* of G. Then we have

Theorem 3.1 $\tilde{Z}(G)(s_1, \ldots, s_n) = Z(G)(s_1 + 1, \ldots, s_n + 1)$.

Theorem 2.1 follows from this and the observation that k-tuples with given support Δ lie in $k!/|G(\Delta)|$ orbits of G.

In particular, with $G = S_n$, we see that

$$\tilde{Z}(S_n) = \sum_{k=0}^{n} Z(S_k).$$

The key to using this for estimation is, as for fixed points, to extend the sum to infinity. It is easily shown that

$$\sum_{k=0}^{\infty} Z(S_k) = \exp\left(\sum_{n=1}^{\infty} \frac{s_n}{n}\right). \tag{3}$$

The value of $Z(S_n)$ is obtained by truncating the series to weight n (where the weight of the term $As_1^{a_1} \cdots s_n^{a_n}$ is $\sum ka_k$), and then replacing s_k by $s_k - 1$ for each k. From the form of the generating function, it is clear that the joint distribution of cycles of lengths $1, 2, \ldots, k$ is that of independent Poisson variables with means $1, \frac{1}{2}, \ldots, \frac{1}{k}$ for fixed k as $n \to \infty$. One can also allow k

to increase slowly, and the error can be estimated. See Arratia and Tavaré [1] for details.

The *cycle index sum* $\sum Z(S_n)$, and similar infinite sums of cycle indices, have been used in enumeration theory since the original paper of Redfield [93]. But it is possible to attach such a sum to a single object. There are a few different ways of doing this. Here, I follow a group-theoretic approach developed in [18]; see Joyal [66] for a different approach.

We take Equation (2) as the definition of modified cycle index for any oligomorphic group G, where the sum is now over a set of orbit representatives of the orbits of G on the *finite* subsets of the set on which G acts. This gives a formal power series in the infinitely many indeterminates $s_1, s_2 \ldots$. (It is well-defined because a monomial $As_1^{a_1} \cdots s_n^{a_n}$ of weight $r = \sum ka_k$ is made up of contributions from sets Δ of cardinality r, and there are only finitely many orbits, by the definition of an oligomorphic group.) Thus, Equation (3) gives the modified cycle index of the infinite symmetric group. The numbers which form the subject of Problem 3 are evaluations of the modified cycle index (putting $s_1 = -1$, $s_i = 0$ for $i > 0$). For more details, see [18].

Richard Parker recently considered another specialisation of cycle index, in connection with computational Galois theory. Let G be a finite permutation group of degree n. Let $\mathcal{C}_k$ be the set of all k-cycles (in the symmetric group) which occur in elements of G. Now G acts by conjugation on $\mathcal{C}_k$; let a_k be the number of orbits of this action. Parker showed that

$$a_k = \frac{1}{|G|} \sum_{g \in G} kc_k(G). \tag{4}$$

(This generalises the Orbit-Counting Lemma, which is obtained for $k = 1$.) The *Parker vector* of G is the n-tuple $(a_1, a_2, \ldots, a_n)$.

Parker gave a probabilistic algorithm which takes as input a polynomial over the integers and produces as output the Parker vector of its Galois group over the rationals. Accordingly, it is important to know:

Problem 8. What information does the Parker vector of G carry about G? In particular, which groups or classes of groups are characterised by their Parker vectors?

Some results on this problem have been obtained by Gewurz [47].

From Equation (4), we see immediately that the sum of the components of the Parker vector is n. The extreme cases are $(n, 0, \ldots, 0)$ (for the trivial group) and $(1, \ldots, 1)$ (for the symmetric group). It is also apparent from (4) that a_k is obtained by differentiating $Z(G)$ with respect to s_k and then putting $s_i = 1$ for all i. For further details of the connection with cycle index, see Gewurz [48].

4 Other aspects of random permutations

The study of random permutations was developed in the papers of Erdős and Turán [42]. The field they pioneered is still very active: recent papers include [1, 8, 52, 101].

More recent research has been concerned with group-theoretic aspects, such as random sets of generators, or more generally, the relation of a random group element to the subgroups of the group G. If H is any subgroup of a group G which is equal to its normaliser in G, then the average number of conjugates of H containing a random element of G is equal to 1. This is the Orbit-Counting Lemma, applied to the action of G on the set of conjugates of H. It applies, in particular, when H is a non-normal maximal subgroup of G. An element g is a derangement in this action if and only if it lies outside all conjugates of H.

If G is not cyclic, we cannot find elements which lie outside *all* maximal subgroups of G, since such an element would generate G. But, if we replace single elements with d-tuples, we can ask what proportion of d-tuples of elements of G generate the group.

The first major result on this is *Dixon's Theorem* [34]:

Theorem 4.1 *The probability that two random elements of S_n generate S_n (resp. A_n) tends to $3/4$ (resp. $1/4$) as $n \to \infty$.*

Of course, the probability that the two elements are both even permutations is $1/4$; so the theorem asserts that almost all pairs of elements generate either S_n or A_n (that is, lie in no proper non-normal subgroup).

The rate of convergence has been estimated. The probability that two random permutations g, h have a common fixed point is about $1/n$; if this occurs, then they both lie in the stabiliser of this point. It can be shown that $1/n$ is the leading term in the asymptotic expansion of the probability that $\langle g, h\rangle$ is not S_n or A_n. This is because the point stabilisers are the largest subgroups of S_n (other than A_n).

A refinement of Dixon's theorem was proved by Łuczak and Pyber. Their result has an application to latin squares. A *quasigroup* is an algebraic system whose multiplication table is a latin square. Its *multiplication group* is the permutation group generated by its left and right translations; equivalently, by the rows and columns of its multiplication table (regarded as permutations of $\{1, \ldots, n\}$. Smith [97] has extended character theory from groups to quasigroups. In his theory, the multiplication group plays an important role; in particular, the character theory is "trivial" if the multiplication group is doubly transitive. (This never happens if the quasigroup is a group.)

It was shown in [19] that the multiplication group of almost all quasigroups is symmetric or alternating; indeed, the group generated by the rows alone is symmetric or alternating. This was dramatically improved by Łuczak and Pyber [74], who showed:

Theorem 4.2 *For almost all permutations g, the only transitive subgroups of S_n which contain g are S_n and the alternating group A_n.*

This immediately implies the result about quasigroups, since the first row of a random latin square is a random permutation, and the group generated by the rows of a latin square is transitive.

Dixon's Theorem 4.1 follows from Theorem 4.2 (though of course this was not the original proof). For two random permutations lie in an intransitive subgroup of S_n if and only if they both fix a k-set, for some $k \leq n/2$; the probability of this is bounded by

$$\sum_{k=1}^{\lfloor n/2 \rfloor} 1 \bigg/ \binom{n}{k} = O(n^{-1}).$$

The crucial part of the proof of Theorem 4.2 is the following assertion:

Theorem 4.3 *The probability $i(n, k)$ that a random permutation from S_n has some invariant subset of size k satisfies $i(n, k) = i(n, n-k) \leq Ak^{-0.01}$ whenever $k \leq n/2$, where A is an absolute constant.*

Problem 9. Improve the estimate in Theorem 4.3.

The small ambiguity about the alternating group in the result on quasigroups was resolved by Häggkvist and Janssen [56], who showed that the proportion of latin squares in which all rows are even permutations is exponentially small. This proportion should probably be about $1/2^n$. Indeed, more is likely to be true. We call a row of a Latin square *even* or *odd* according as it is an even or an odd permutation.

Problem 10. Show that the number of odd rows of a random latin square of order n is approximately binomial $B(n, \frac{1}{2})$ as $n \to \infty$.

Since, as we saw in Section 2, a positive proportion of permutations are derangements, Theorem 4.2 still holds when 'permutations' is replaced by 'derangements' in the statement. However, there is a different measure which can be used in connection with derangements: the probability of a permutation is proportional to the number of latin squares, normalised so that the first row is the identity permutation, which have the given permutation as second row. In this measure, derangements have positive measure (and all other permutations have measure zero); but derangements are not all equally likely. For example, (2 3 4 1) is the second row of two normalised latin squares, while (2 1 4 3) occurs in four such squares.

Problem 11. Show that, with the above measure, the probability that a random permutation lies in no transitive subgroup of S_n except S_n and possibly A_n tends to 1 as $n \to \infty$.

An affirmative answer to this question would immediately imply that the rows of a random *normalised* latin square almost certainly generate S_n. This would strengthen the result of [19] from quasigroups to loops, since a loop is just a quasigroup in which the first row and column of the multiplication table are the identity permutation.

The property of the symmetric group which allows such results to be proved is that its large maximal subgroups are now well understood. We already observed that the largest (apart from the alternating group) are the point stabilisers, and more generally the intransitive subgroups (the stabilisers of subsets). After these come the imprimitive subgroups (those which preserve partitions). Using the Classification of Finite Simple Groups, we know much more than previously about primitive subgroups of S_n. In particular,

- primitive subgroups are very small (having order at most $n^{c \log n}$ with known exceptions);
- there are few primitive subgroups (at most $n^{c \log n}$ conjugacy classes) (Pyber and Shalev [91]);
- for almost all n, there are no primitive subgroups except for S_n and A_n (Cameron, Neumann and Teague [25]).

A survey of asymptotic results in this area is given by Pyber [90]; see also [72, 68, 71, 91] for further results. Praeger and Shalev [89] have begun a program of extending these results to *quasiprimitive* groups (those for which every non-trivial normal subgroup is transitive).

The probability that a random d-tuple of elements generates the group has been investigated for other classes of groups. The natural setting for such a result is the class of profinite groups (these are compact in the profinite topology and so have an invariant probability measure). Results on such groups depend on examining their finite quotients. See [78, 80].

Another active area involves showing that a group has generators of a particular type, or that almost all generating sets have some particular property. For example:

- In a symmetric or classical group, a random element of order 2 and one of order 3 almost surely generate the group. (This was proved for the symmetric groups, in a more general form, independently by Th. Müller and L. Pyber, both unpublished, and by Liebeck and Shalev [70] for classical groups – it is necessary to exclude the four-dimensional symplectic groups.)

- Almost all pairs of elements of the symmetric group give rise to Cayley graphs with small diameter (Babai and Hetyei [5]), and at least some give short presentations (Liebeck and Shalev [70]).

See also [6, 4, 71].

5 Extremal properties

A number of metrics have been considered for permutations, including distance in the Cayley graph (with respect to the generating set consisting of transpositions), the Hamming and Lee metrics, l^1, l^2 and l^∞ metrics, and commutation distance. Extremal problems can be posed for each of them. See Deza and Huang [33] for a survey. I treat only Hamming distance here.

If we regard a permutation g of $\{1, \ldots, n\}$ as an n-tuple $(a_1, \ldots, a_n)$, then the Hamming distance from g to the identity permutation is simply $n - \mathrm{fix}(g)$ (the number of fixed points of g), and more generally, the Hamming distance $d(g, h)$ from g to h is $n - \mathrm{fix}(gh^{-1})$. On the other hand, if we regard g as a function, that is, a set of n ordered pairs, then the Hamming distance

$d(g,h)$ is $n - |g \cap h|$. (Note that the Hamming distance between two distinct permutations is at least 2.)

Note, in passing, that $\mathrm{fix}(gh^{-1}) = \mathrm{fix}(hg^{-1}) = \mathrm{fix}(h^{-1}g)$, since the inverse and any conjugate of a permutation g have the same numbers of fixed points as does g.

So we can formulate analogues of the classical extremal problems for uniform hypergraphs in the context of permutations. For example:

Problem 12. (a) Given n and a subset A of $\{0, \dots, n-2\}$, what is the largest cardinality of a set S of permutations of $\{1, \dots, n\}$ such that, for all distinct $g, h \in S$, we have $\mathrm{fix}(gh^{-1}) \in A$?

(b) What is the structure of such a set of permutations of maximum size?

(c) How do the answers change if we assume that S is a group?

In this section, I will discuss a few special cases of this general problem. First, we say that S is *A-intersecting* if $\mathrm{fix}(g,h) \in A$ for all distinct $g, h \in S$. We let $F(n, A)$ be the maximum cardinality of an A-intersecting subset of S_n.

Theorem 5.1 *$F(n,A)F(n,B)/F(n,A \cap B) \leq n!$. In particular, if $A \cap B = \emptyset$ then $F(n,A)F(n,B) \leq n!$.*

To see this, let S and T be A- and B-intersecting sets of maximum size. Consider the set $ST = \{st : s \in S, t \in T\}$. If an element of this set has two different representations, say $s_1t_1 = s_2t_2$, then $s_2^{-1}s_1 = t_2t_1^{-1}$, so

$$\mathrm{fix}(s_1s_2^{-1}) = \mathrm{fix}(s_2^{-1}s_1) = \mathrm{fix}(t_2t_1^{-1}) \in A \cap B,$$

so the number of representations of each element is at most $F(n, A \cap B)$.

Consider the case where $A = \{s, s+1, \dots, n\}$. An A-intersecting set consists of permutations agreeing in at least s points: we call such a set *$(\geq s)$-intersecting*, and denote the maximum size of such a set by $F(n, \geq s)$. There is an obvious $(\geq s)$-intersecting set of size $(n-s)!$, consisting of all permutations fixing s points. Deza [30, 32] asked:

Problem 13. Is it true that, if n is sufficiently large in terms of s, then $F(n, \geq s) = (n-s)!$, and a set meeting the bound is a translate of the stabiliser of s points?

This would be an analogue for permutations of the Erdős–Ko–Rado theorem [39] for families of sets.

The complementary case is easier. Suppose that $A = \{0, 1, \ldots, s-1\}$. Then an A-intersecting set consists of a set of permutations pairwise agreeing in fewer than s points. The images of a fixed s-tuple under these permutations are all distinct, so we have:

Theorem 5.2 *If $A = \{0, 1, \ldots, s-1\}$, then $F(n, A) \leq n(n-1)\cdots(n-s+1)$.*

This result, due to Deza and Frankl [32], is the analogue of the Singleton bound (see [10]). A set meeting the bound is called *sharply s-transitive.*

A sharply 1-transitive set is just the set of rows of a Latin square. Of course, examples exist for every n, and there are too many to classify! For larger s, such sets are closely connected with geometry. The existence of a sharply 2-transitive set of permutations of $\{1, \ldots, n\}$ is equivalent to that of a projective plane of order n. Examples are known only for prime power values of n. Examples of sharply 3-transitive sets are known whenever $n-1$ is a prime power.

At the other extreme, $F(n, \leq n-2) = n!$, and $F(n, \leq n-3) \leq n!/2$. (For the second assertion, take the alternating group, the set of all permutations of even parity). On the other hand, the bound of Theorem 5.2 is not attained for $s = n-3 > 3$. For $F(n, \geq n-3) \geq n$ (take the identity permutation together with all transpositions $(1\ i)$ for $2 \leq i \leq n$), and then Theorem 5.1 shows that $F(n, \leq n-4) \leq (n-1)!$. Similarly, Myrvold [84] has shown that $F(n, \leq n-c-1) > c!$ for any fixed c if n is sufficiently large.

By Theorem 5.1, if a sharply s-transitive set exists, then $F(n, \geq s) = (n-s)!$. In particular, this holds if $s = 1$ for all n, for $s = 2$ and n a prime power, and for $s = 3$ and $n-1$ a prime power.

Problem 14. Which sharply s-transitive sets of permutations exist?

This problem is much too hard for a general solution since, as we have observed, it would include a classification of finite projective planes.

We call a set of permutations an *s-distance set* if it is A-intersecting for some set A with $|A| = s$. Let $G(n, s)$ be the largest size of an s-distance set. There are upper and lower bounds, quite close together, for this function.

Theorem 5.3 *There is a constant $c > 0$ such that, for $n > 2s$, we have*

$$\left(\frac{cn}{s}\right)^{2s} \leq G(n,s) \leq \sum_{\dim(\chi)\leq s} \chi(1)^2.$$

The right-hand side is asymptotically $p(s)n^{2s}/(s!)^2$ as $n \to \infty$ for fixed s, where p is the partition function.

A 1-distance set of permutations is known as an *equidistant permutation array*. Such arrays have an extensive literature; I refer to [76] for a recent summary. The lower bound in Theorem 5.3 is proved by a simple construction from the case $s = 1$. Assuming for convenience that s divides n, we take an equidistant permutation array S of length n/s and cardinality $(cn/s)^2$, and then take all permutations obtained by concatenating s elements of S acting on disjoint blocks $\{1,\ldots,n/s\}$, $\{n/s+1,\ldots,2n/s\}$, $\ldots$. We obtain an s-distance set of cardinality $(cn/s)^{2s}$.

The upper bound depends on some knowledge of the character theory of the symmetric group. Characters are parametrised by partitions of n; the *dimension* of a character χ is $n - a$, where a is the largest part of the corresponding partition. See [17] for further discussion.

The paper of Tarnanen [100] shows that, if the character table of S_n is available, then it is possible to use Delsarte's *linear programming bound* (applied to the *conjugacy class association scheme* of the symmetric group) to obtain better bounds for $f(n,A)$ in particular cases. The paper includes tables of upper bounds for $n \leq 8$, and provides a good survey of the technique.

Now we turn to the special case where the set is a group. By the closure property, a group G is A-intersecting if and only if $\mathrm{fix}(g) \in A$ for all $g \in G$. (This is similar to the relation between distances and weights in a linear code.)

For groups, much stronger bounds hold. The following result was proved by Blichfeldt [11]. It was ignored for many years until it was rediscovered by Kiyota [67].

Theorem 5.4 *Let G be an A-intersecting subgroup of S_n. Then*

$$|G| \leq \prod_{a\in A}(n-a).$$

Groups meeting this bound are called *sharp groups*. Note that if $A = \{0,\ldots,s-1\}$, then a sharp group is just a sharply s-transitive group. Such groups have been completely determined for $s > 1$ by Zassenhaus [103, 102].

Problem 15. Determine the sharp groups.

Some results on this are to be found in [61] and subsequent papers including [14]. We cannot expect a list of groups in all cases. For example, if $A = \{a\}$, then a group of order $n - a$ which fixes a points and acts regularly (sharply transitively) on the other points is sharp. We could ask for a determination of all sharp groups not of this type. In this connection, we have the following more general result (in which sharpness is not assumed):

Theorem 5.5 *Let G be a permutation group in which every non-identity element fixes exactly a points. Then G has at most $2a - 1$ non-regular orbits. Moreover, there is a finite list $L(a)$ of groups such that one of the following holds:*

(a) G has a fixed set Δ of size a, and the kernel N of the action on Δ is semiregular outside Δ; or

(b) G belongs to the list $L(a)$.

Furthermore, in case (a), if G acts non-trivially on Δ, then N is nilpotent; and if G^{Δ} has even order, then N is abelian.

Problem 16. In case (b) of the above theorem, find an explicit bound (in terms of a) for the order of the groups in the finite list. (For $a = 2$, Iwahori [62] showed that the exceptional groups under (b) are the rotation groups of the regular tetrahedron, octahedron and icosahedron, acting on the set of vertices, edges and faces of the corresponding polyhedron; so the right bound is 60.)

6 Permutation geometries

A *subpermutation* of a finite set X is a bijection between subsets of X. The set $\mathcal{S}(X)$ of all subpermutations of X carries two natural structures:

- Regarding a subpermutation as a subset of $X \times X$, the set $\mathcal{S}(X)$ is a *meet-semilattice* with respect to inclusion;

- With the operation of composition, that is,

$$f \circ g = \{(x,z) : (\exists y \in X)(x,y) \in f, (y,z) \in g\},$$

$\mathcal{S}(X)$ is an *inverse semigroup.*

Note that the maximal elements in the semilattice are the permutations, which form the symmetric group.

Now many problems of extremal set theory or about random permutations can be extended to this setting. Very little has been done! I am only concerned with one example here, due to Michel Deza. This is the analogue of the concept of a *matroid.* Deza called these structures *permutation geometries*, by analogy with *combinatorial geometries* (an alternative term for simple matroids).

The most convenient form of the definition of a matroid to generalise is that in terms of subspaces. Thus, a *permutation geometry* is a non-empty set H of subpermutations satisfying the following conditions:

- H is closed under intersection (so is a meet-semilattice).
- H is *ranked*, that is, all maximal chains have the same length s (so that we can define a *rank function* r, where $r(f)$ is the length of a maximal chain with greatest element f).
- Let $f \in H$ and $(x,y) \in X^2$ have the property that $x \notin \mathrm{dom}(f)$ and $y \notin \mathrm{ran}(f)$ (where $\mathrm{dom}(f)$ and $\mathrm{ran}(f)$ are the domain and range of f respectively). Then there exists $g \in H$ such that $r(g) = r(f) + 1$ and $f \cup \{(x,y)\} \subseteq g$. (This element is necessarily unique.)

Rather than investigating this concept in general, we will impose an extra condition, which is the analogue for permutations of the definition of a *perfect matroid design* [31]:

- There are integers $a_0, a_1, \ldots, a_s$ such that, if $r(f) = i$, then $|f| = a_i$. Clearly $a_s = n$; and we assume that $a_{s-1} < n - 1$.

Let $M(H)$ be the set of maximal elements of the permutation geometry H. Then $M(H)$ is easily seen to be an A-intersecting set of permutations, where $A = \{a_0, \ldots, a_{s-1}\}$, and to satisfy

$$|M(H)| = \prod_{i=0}^{s-1}(n - a_i).$$

This is exactly the cardinality of an A-intersecting sharp group, as discussed in the last section, although the context is quite different. Several further properties hold:

- H is the closure of $M(H)$ under intersection.
- If $g \in M(H)$, then the elements of H lying below g are the flats of a matroid on the set g (in fact, a perfect matroid design).

The set H (which determines the geometry $M(H)$) is called a *geometric set* of permutations, of *rank* s and *type* $(a_0, a_1, \ldots, a_{s-1})$.

Problem 17. Which geometric sets of permutations exist?

This problem is unlikely to have a simple solution. A sharply s-transitive set of permutations is geometric of type $A = \{0, 1, \ldots, s-1\}$; and we already noted after Problem 14 that the existence of sharply 2-transitive sets is equivalent to that of projective planes of order n.

A related problem asks for the analogue for permutations of a theorem of Deza, Erdős and Frankl [31] for sets. This also includes Problem 13 as a special case: see [30, 32].

Problem 18. Let A be a finite set of non-negative integers. Show that, for n sufficiently large in terms of A, an A-intersecting set of permutations in S_n has cardinality at most $\prod_{a\in A}(n-a)$, with equality if and only if it is a geometric set of type A.

If a geometric set of permutations is also a subgroup of S_n, it is called a *geometric group*. (This name is not completely satisfactory, since there are other ways in which a group could be "geometric".) If G is a geometric group, then the corresponding permutation geometry (the meet-semilattice generated by G) is a subsemigroup of the inverse semigroup $\mathcal{S}(X)$.

The finite geometric groups have been completely determined by Maund [83] in her thesis (though, regrettably, she has never published the results). Maund's argument was inductive, and made use of the Classification of Finite Simple Groups. A weaker result, the determination of the finite geometric groups of rank at least 7, was proved without using the classification by Zil'ber [104]. This result was used by Zil'ber in his work on totally categorical first-order theories. In Zil'ber's case, only the "generic" examples appear; these are wreath products of regular groups with symmetric groups or certain large subgroups of these, alternating groups, general linear groups (and subgroups of these stabilising some vectors), and affine groups (and subgroups of these preserving certain translations). Maund had to deal with various "sporadic" examples of small rank, including the sharply s-transitive groups.

An application of geometric groups in universal algebra was given by Cameron and Szabó [26]. An *independence algebra* is an algebra (in the sense of universal algebra) in which the following conditions hold:

(a) the *bases* (minimal generating sets) satisfy the Exchange Axiom;

(b) any map from a basis into the algebra extends to an endomorphism of the algebra.

Clearly this definition only depends on the subalgebras and endomorphisms; we call two algebras on the same set *equivalent* if they have the same subalgebras and endomorphisms. (Thus, an algebra equivalent to an independence algebra is an independence algebra.)

Using Maund's Theorem, Cameron and Szabó were able to determine all finite independence algebras up to equivalence. The key observation is that the automorphism group of an independence algebra must be a geometric group. The subalgebras are the fixed point sets of the subgroups of this group. Some work is required to identify the endomorphisms.

7 Bases

A *base* for a permutation group G is a sequence of points whose pointwise stabiliser is the identity. It is *irredundant* if no point in the sequence is fixed by the stabiliser of its predecessors. From any base, we obtain a unique irredundant base by omitting "redundant" points.

For example, any $n-1$ points form a base for the symmetric group S_n, and any $n-2$ points a base for the alternating group A_n; a basis for a vector space V is also a base for the general linear group acting on V.

Bases are used in computational group theory: since a group element is completely determined by its effect on a base, we can exploit a small base to reduce the memory requirements of a computation. They also have a central role in extremal and asymptotic problems, as we shall see. The application suggests that an important invariant of a permutation group G is its *minimum base size*, denoted $b(G)$. This invariant is also connected to the *minimal degree* $\mu(G)$ of G, the least number of points moved by a non-identity element of G. Indeed, it is easy to see that $b(G)\mu(G) \geq n$ for any transitive group G of degree n. See [54] for recent results on minimal degree.

A striking result of Pyber [90] puts the problem in context.

Theorem 7.1 *There is a positive constant c such that almost all subgroups G of S_n satisfy $b(G) \geq cn$.*

To make this result plausible, here is a construction of large numbers of subgroups. Suppose that n is even, and let $m = n/2$. Let t_i be the transposition $(2i-1\ 2i)$. Then the transpositions $t_1, \ldots, t_m$ generate an elementary abelian group of order 2^m. This group has roughly $2^{m^2/4} = 2^{\frac{1}{16}n^2}$ subgroups, which can be identified with linear codes of length m. The order of a subgroup is 2^b, where b is its minimum base size. The distribution of b is very sharply concentrated at $m/2$ (that is, $n/4$). Note that the orders of subgroups of this form are concentrated around $2^{n/4}$.

It is possible that subgroups of this form are among the commonest subgroups of the symmetric group. (Already in 1967, Schinzel conjectured that almost all subgroups of S_n are soluble.) It is known that the number of subgroups of S_n is bounded above by $24^{(\frac{1}{6}+o(1))n^2}$, and that almost all subgroups of S_n are intransitive (see [73]), but more detailed results about almost all subgroups are currently out of reach.

Now the following simple result connects minimal base size to the order of a permutation group.

Theorem 7.2 *Let G be a subgroup of S_n with minimal base size $b(G)$. Then*

$$\log |G| / \log n \leq b(G) \leq \log |G| / \log 2. \tag{5}$$

The left-hand inequality holds because the order of a group with base size b cannot exceed the number of bases, which is not greater than n^b. For the right-hand bound we note that, in an irredundant base, the stabiliser of the first $i+1$ base points is properly contained in the stabiliser of the first i points, so G has a chain of subgroups of length b.

It is thought that a typical subgroup of S_n comes close to meeting the right-hand bound in Equation (5). On the other hand, Pyber has conjectured that the left-hand bound is asymptotically correct for primitive groups.

Problem 19. Prove Pyber's Conjecture, in the following form: there exists a universal constant c such that a primitive permutation group G of degree n has a base of size at most $c \log |G| / \log n$.

This was proved by Seress [96] for soluble groups; in fact, he showed that primitive soluble groups have a base of size at most 4. See also [50, 71].

Equation (5) also implies that an arbitrary irredundant base has size at most $b(G)\log_2 n$. (This approximation is useful because determining $b(G)$ is NP-hard.) We now turn to a better approximation to the minimum base size of an arbitrary group, discovered by Blaha [9].

A *greedy base* is one in which each point lies in an orbit of maximum size of the stabiliser of its predecessors. Blaha showed that a greedy base has size at most $cb(G)\log\log n$ for some constant c.

Problem 20. Is there a function f such that any greedy base for a *primitive* group G has size at most $f(b(G))$? Could this even be true with a linear function?

We would certainly have $f(2) = 2$: if there is a base of size 2, then the greedy algorithm will find one. (This is true in any transitive group: for, if the stabiliser of a point in a transitive group has a regular orbit, then this orbit is the largest.)

In the case of the symmetric group S_n in its action on 2-sets, the greedy algorithm finds a base whose size is asymptotically $(9/8)b(G)$.) These were the 'worst' known examples until recently. However, Cavenagh [27] has found examples of primitive groups with minimal base size 3 in which the greedy algorithm finds a base of size 4. The first such example is the wreath product $S_3 \operatorname{Wr} H$, in its product action of degree 3^{60}, where $H = S_2 \operatorname{Wr} S_2 \operatorname{Wr} S_{15}$ in its usual imprimitive action of degree 60.

No such bound holds for arbitrary permutation groups, as was shown by Blaha [9]. For a simple example illustrating his method, consider the cyclic group of order 210, acting with orbits of lengths 14, 15 and 35. A minimal base has size 2 and contains one point from each of the first two orbits. The greedy algorithm, however, chooses first a point from the orbit of length 35, and then still has to choose a point from each of the other two orbits.

In order to connect bases with the extremal results described earlier, we make a short detour. Recall Blichfeldt's bound (Theorem 5.4)

$$|G| \text{ divides } \prod_{a\in A}(n-a) \tag{6}$$

for the order of an A-intersecting group G of degree n. In his paper [11], he attributed the result to Maillet [77]. But Maillet's hypotheses were different.

First, he proved Equation (6) under the assumption that the number of fixed points of every *subgroup* lies in A (rather than just every *element*, as in Blichfeldt's theorem). Now the case of equality is interesting:

Theorem 7.3 *Let A be a set of positive integers less than $n-1$. Then the following conditions on a permutation group $G \leq S_n$ are equivalent:*

- *G satisfies Maillet's hypothesis and attains his bound;*
- *G permutes its irredundant bases transitively;*
- *G is a geometric group of type A.*

By Maund's result, we have a classification of such groups.

Cameron and Fon-Der-Flaass [23] considered a wider class of groups which they called *IBIS groups* (an acronym for Irredundant Bases of Invariant Size). An IBIS group is one satisfying the three equivalent conditions

- all irredundant bases of G have the same size;
- the irredundant bases of G are preserved by re-ordering;
- the irredundant bases of G are the bases of a matroid.

Problem 21. Determine the IBIS groups (or, at least, the corresponding matroids).

A curious example is provided by the Mathieu group M_{24}. It is associated with a well-known matroid of rank 6, whose hyperplanes are the blocks of the Steiner system $S(5,8,24)$. But M_{24} is an IBIS group of rank 7, so it acts on a different matroid on the same set. It is transitive on unordered bases, but not on ordered bases, of this matroid.

Maillet proved a theorem stronger than the one we have quoted. He assumed only that the numbers of fixed points of subgroups *of prime power order* belong to A, and reached the same conclusion as before. (Assume this hypothesis. Then, by the theorem quoted, the orders of the subgroups of prime power order divide $\prod_{a\in A}(n-a)$; and $|G|$ is the least common multiple of these orders, by Sylow's Theorem.)

Problem 22. Which permutation groups attain the bound in the above stronger form of Maillet's Theorem?

Examples include direct products of geometric groups of coprime orders. (It follows from Maund's classification that any geometric group of rank at least 2 has even order, so the examples constructed in this way act regularly on all but one orbit.)

There are many other open problems associated with bases. Here is a short selection.

Problem 23.

- Which groups have the property that all greedy bases have the same size? Or that greedy bases are preserved by re-ordering? Can a matroid or similar structure be associated with the greedy bases under suitable conditions?

- What about variants of the greedy algorithm? For example, Maund proposed considering choosing the next base point to maximise the number of orbits of its stabiliser.

- Liebeck and Shalev [71] proved that there is an absolute bound on the minimum base size of an almost simple primitive group with "known" exceptions. They give no estimate for the constant, but it is believed to be 5. Prove this.

Here is a question which is not directly related to bases, but comes up in the same context of computational permutation group theory.

Problem 24. Any subgroup of S_n can be generated by at most $n-1$ elements. This follows from an 'on-line' algorithm due to Jerrum [63] which, given a set S of at most $n-1$ permutations and a permutation g, produces (in polynomial time) a set S' with $|S'| \leq n-1$ such that S' generates the same subgroup as $S \cup \{g\}$. McIver and Neumann [75] have shown that, in fact, any subgroup of S_n can be generated by at most $\lfloor n/2 \rfloor$ elements for $n > 3$; this is best possible. The problem is to find an efficient algorithm (preferably an 'on-line' algorithm in the above sense) to find such a generating set.

A base for the permutation group G can be regarded as a b-tuple lying in a regular G-orbit on Ω^b. A related line of investigation concerns regular orbits of G on the power set $\mathcal{P}(\Omega)$. It is known that, for primitive groups of degree n other than S_n and A_n, almost all G-orbits on $\mathcal{P}(\Omega)$ are regular [16]. In particular, with the exception of S_n, A_n and finitely many others, every primitive group has a regular orbit on the power set. The finite list of exceptions has not bee completely determined, but includes the Mathieu group M_{24} among others: see [24].

8 Automorphism groups

This section gives some problems on automorphism groups.

It is known that every finite group is the full automorphism group of a finite graph (Frucht [45]), and that almost all finite graphs have trivial automorphism group (Erdős and Rényi [40]). In [15], I gave a result including both of these facts:

Theorem 8.1 *For any finite group G, there is a rational number $\alpha(G)$ such that, if X is a random G-invariant graph, the probability that* $\mathrm{Aut}(X) = G$ *tends to $\alpha(G)$ as $n \to \infty$. Moreover, $\alpha(G) = 1$ if and only if G is a direct product of symmetric groups; but the values of $\alpha(G)$, even for metabelian groups G, are dense in the unit interval.*

Problem 25. Which rational numbers occur as $\alpha(G)$ for some finite group G?

Problem 26. It is known that one can prescribe a wide range of properties and still find a graph with these properties having any given automorphism group. (See Babai [2], Babai and Goodman [3], for surveys.) Extend Theorem 8.1 to some of these classes; for example, to the class of cubic graphs.

Not every permutation group is the automorphism group of a graph. The alternating group, indeed, is not the automorphism group of any hypergraph. Nevertheless, on can ask:

Problem 27. Show the existence of a function f with the following property: Every primitive permutation group G of degree n, except the alternating group, has the property that almost all G-invariant $f(n)$-uniform hypergraphs have automorphism group precisely G. Establish the smallest possible f for which this holds.

This problem was posed by Mikhail Klin. László Babai and I have some partial (unpublished) results.

Problem 6 on automorphism groups of graphs, posed by Marušič, Jordan and Klin, also fits here.

9 Movement

Cheryl Praeger, in [87] and subsequent papers with a number of co-authors, has considered the "movement" of a permutation group, that is, the maximum Hamming distance from a set to any of its images under elements of the group. In [46], for example, the following result is proved.

Theorem 9.1 *Let G be a permutation group on a set Ω with no fixed points in Ω and let m be a positive integer. If no element of G moves any subset of Ω by more than m points (that is, if $|\Gamma \setminus \Gamma g| \leq m$ for every $\Gamma \subseteq \Omega$ and $g \in G$), then Ω is finite, and $|\Omega| \leq 5m - 2$. If G is transitive on Ω, then $|\Omega| \leq 3m$.*

In [79], all transitive groups attaining the bound of this theorem are determined.

For a "dual" result, see [86].

10 Generic tuples of orders

In this section I consider briefly the problem of extending analysis of random permutations to permutations of infinite sets.

We must expect things to be very different. In a similar context, Erdős and Rényi [40] showed that there is a unique "countable random graph", whose structural properties are wholly unlike those of finite random graphs. According to Erdős and Spencer [41], this demolishes the theory of countable random graphs; but it creates instead the theory of *the* countable random graph (see [21]).

There is an added difficulty in that there is no natural measure on permutations of a countable set, since the symmetric group is not compact. So we proceed differently. A permutation of a finite set can be regarded as the relationship between two total orderings of a finite set. (The fact that a unique permutation corresponds to a pair of orderings is a consequence of the fact that an ordering of a finite set is rigid; we have to abandon this convenience in the infinite case.)

Now there is a simple model for choosing a random ordering of a countable set $\{a_0, a_1, \ldots\}$. When we consider each point a_n, its n predecessors will already be ordered, and so there are $n + 1$ possible intervals or gaps into which we could put a_n; we assign to each interval the probability $1/(n+1)$, independent of earlier decisions.

It turns out that, with probability 1, the resulting order is dense and without endpoints, hence isomorphic to $\mathbb{Q}$, by Cantor's Theorem. For example, the probability that no point lies between a_m and a_n, assuming these points are adjacent after a_n has been assigned, is

$$\prod_{i>n}\left(1-\frac{1}{i+1}\right)=0.$$

Now, in place of a random permutation, we can consider a *generic pair* of total orders. Both orders will be dense, but more will hold: for example, if $<_1$ and $<_2$ are the two orders, then for any four points a,b,c,d satisfying $a<_1 b$ and $c<_2 d$, there exists x with $a<_1 x<_1 b$ and $c<_2 x<_2 d$. (Indeed, there are points in each of the nine possible relationships to a,b,c,d.)

A pair of orders of a countable set having this property is unique up to isomorphism. It is also *universal* (every pair of orders of a finite set is embeddable in it) and *homogeneous* (any isomorphism between finite subsets extends to an automorphism). (By isomorphism here we mean a bijection preserving both orders.) The uniqueness then follows from Fraïssé's theory of countable homogeneous relational structures (see [44]).

From the generic pair of orders, we can construct the generic countable *permutation graph*, by joining s to y whenever the two orders disagree on x and y. (Its edges are the analogue of the set of inversions in a random permutation.) Also, the intersection of the two orders describes a partially ordered set which is the generic countable 2-*dimensional poset*.

In an exactly analogous way, there is a generic n-tuple of orders on any countable set.

The most natural source of problems here is to look for analogues of the properties of the random graph. Here is one example. The random graph admits a cyclic automorphism, but the generic order $\mathbb{Q}$ does not – indeed, the only countable total order admitting a cyclic automorphism is $\mathbb{Z}$. However, $\mathbb{Q}$ admits the group $\mathbb{Z}\times\mathbb{Z}$ acting regularly. (To see this, take any irrational α, and define an order on $\mathbb{Z}\times\mathbb{Z}$ by the rule that $(x_1,y_1)<(x_2,y_2)$ if $x_1+\alpha y_1<x_2+\alpha y_2$. This order admits all translations in the group, and is dense without endpoints, and so is isomorphic to $\mathbb{Q}$.)

Problem 28. For which pairs m,n does the group $\mathbb{Z}^m$ have a regular action on the generic n-tuple of orders? (I conjecture that this holds if and only if

$m > n$.)

Acknowledgment I am grateful to Laci Pyber for a large number of suggestions which have markedly improved the quality of this paper; to Michel Deza and Wendy Myrvold, for information about permutation codes; and to Robin Chapman for the solution to Ömer Eceğlioğlu's problem on derangements.

References

[1] R. Arratia and S. Tavaré, The cycle structure of random permutations, *Ann. Probability* **20** (1992), 1567–1591.

[2] L. Babai, On the abstract group of automorphisms, pp. 1–40 in *Combinatorics* (ed. H. N. V. Temperley), London Math. Soc. Lecture Notes **52**, Cambridge University Press, Cambridge, 1981.

[3] L. Babai and A. J. Goodman, On the abstract group of automorphisms, pp. 121–143 in *Coding Theory, Design Theory, Group Theory* (ed. D. Jungnickel and S. A. Vanstone), Wiley, New York, 1993.

[4] L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks and P. P. Pálfy, Short presentations for finite groups, *J. Algebra* **194** (1997), 79–112.

[5] L. Babai and G. L. Hetyei, On the diameter of random Cayley graphs of the symmetric group, *Combinatorics, Probability and Computing* **1** (1992), 201–208.

[6] L. Babai, W. M. Kantor and A. Lubotzky, Small-diameter Cayley graphs for finite simple groups, *Europ. J. Combinatorics* **10** (1989), 507–522.

[7] A. Bereczky, Fixed-point-free p-elements in transitive permutation groups, *J. London Math. Soc.* (2) **27** (1995), 447–452.

[8] P. Biane, Minimal factorizations of n-cycle and central multiplicative functions of the infinite symmetric group, *J. Combinatorial Theory* (A) **76** (1996), 197–212.

[9] K. D. Blaha, Minimal bases for permutation groups: the greedy approximation, *J. Algorithms* **13** (1992), 297–306.

[10] I. F. Blake, G. Cohen and M. Deza, Coding with permutations, *Inform. Control* **43** (1979), 1–19.

[11] H. F. Blichfeldt, A theorem concerning the invariants of linear homogeneous groups, with some applications to substitution groups, *Trans. Amer. Math. Soc.* **5** (1904), 461–466.

[12] A. V. Borovik, L. Pyber and A. Shalev, Maximal subgroups in finite and profinite groups, *Trans. Amer. Math. Soc.* **348** (1996), 3745–3761.

[13] N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, J. Leavitt, D. T. Ose and D. A. Jackson, The proportion of fixed-point-free elements of a transitive permutation group, *Commun. Algebra* **21** (1993), 3259–3275.

[14] D. P. Brozovic, On primitive sharp permutation groups, *Commun. Algebra* **24** (1996), 3979–3994.

[15] P. J. Cameron, On graphs with given automorphism group, *Europ. J. Combinatorics* **1** (1980), 91–96.

[16] P. J. Cameron, Regular orbits of permutation groups on the power set, *Discrete Math.* **62** (1986), 307–309.

[17] P. J. Cameron, Metric and geometric properties of sets of permutations, pp. 39–53 in *Algebraic, Extremal and Metric Combinatorics* (M.-M. Deza, P. Frankl & I. G. Rosenberg, eds.), London Math. Soc. Lecture Notes **131**, Cambridge University Press, Cambridge, 1988.

[18] P. J. Cameron, *Oligomorphic Permutation Groups*, London Math. Soc. Lecture Notes **152**, Cambridge University Press, Cambridge, 1990.

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

[20] P. J. Cameron, Cofinitary permutation groups, *Bull. London Math. Soc.* **28** (1996), 113–140.

[21] P. J. Cameron, The random graph, pp. 331–351 in *The Mathematics of Paul Erdős*, (J. Nešetřil and R. L. Graham, eds.), Springer, Berlin, 1996.

[22] P. J. Cameron and A. M. Cohen, On the number of fixed point free elements of a permutation group, *Discrete Math.* **106/107** (1992), 135–138.

[23] P. J. Cameron and D. G. Fon-Der-Flaass, Bases for permutation groups and matroids, *Europ. J. Combinatorics* **16** (1995), 537–544.

[24] P. J. Cameron, P. M. Neumann and J. Saxl, On groups with no regular orbits on the set of subsets, *Arch. Math.* **43** (1984), 295–296.

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

[26] P. J. Cameron and C. Szabó, Independence algebras, *J. London Math. Soc.*, to appear.

[27] N. J. Cavenagh, personal communication.

[28] R. J. Chapman, personal communication.

[29] J. Dénes, P. Erdős, and P. Turán, On some statistical properties of the alternating group of degree n, *Enseignement Math.* (2) **15** (1969), 89–99.

[30] M. Deza, Matrices dont deux lignes quelconque coincident dans un nombre donne de positions communes, *J. Combinatorial Theory* (A) **20** (1976), 306–318.

[31] M. Deza, P. Erdős and P. Frankl, Intersection properties of systems of finite sets, *Proc. London math. Soc.* (3) **36** (1978), 369–384.

[32] M. Deza and P. Frankl, On the maximum number of permutations with given maximal or minimal distance, *J. Combinatorial Theory* (A) **22** (1977), 352–360.

[33] M. Deza and T. Huang, Metrics on permutations, a survey, *J. Combinatorics, Information and System Sciences* **23** (1998), 173–185.

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

[35] Ö. Eceğlioğlu, problem posed at the Seventeenth British Combinatorial Conference, Canterbury, 1999.

[36] E. Engeler, Äquivalenzklassen von n-Tupeln, *Z. Math. Logik Grundl. Math.* **5** (1959), 340–345.

[37] P. Erdős, Beweis eines Satzes von Tschebyschef, *Acta Sci. Math. (Szeged)* **5** (1930–1932), 194–198.

[38] P. Erdős, A theorem of Sylvester and Schur, *J. London Math. Soc.* **9** (1934), 282–288.

[39] P. Erdős, C. Ko, and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford* (2) **12** (1961), 313–320.

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

[41] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, New York/Akad. Kiadó, Budapest, 1974.

[42] 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.

[43] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II, *J. Reine Angew. Math.* **328** (1981), 39–57.

[44] R. Fraïssé, Sur certains relations qui généralisent l'ordre des nombres rationnels, *C. R. Acad. Sci. Paris* **237** (1953), 540–542.

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

[46] A. Gardiner and C. E. Praeger, Transitive permutation groups with bounded movement, *J. Algebra* **168** (1994), No.3, 798-803.

[47] D. A. Gewurz, Reconstruction of permutation groups from their Parker vectors, *J. Group Theory*, to appear.

[48] D. A. Gewurz, Parker vectors and cycle indices of permutation groups, in preparation.

[49] M. R. Giudici, Quasiprimitive groups with no fixed point free elements of prime order, preprint.

[50] D. Gluck and K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, *J. London Math. Soc.* (2) **58** (1998), 603–618.

[51] L. A. Goldberg and M. R. Jerrum, The "Burnside process" converges slowly, Proceedings of Random 1998, in *Randomisation and Approximation Techniques in Computer Science* (M. Luby et al., eds.), Springer-Verlag Lecture Notes in Computer Science, No. 1518, pp. 331–345.

[52] S. W. Golomb and P. Goal, On the number of permutations of n objects with greatest cycle length k, *Advances Appl. Math.* **70** (1998), 98–107.

[53] D. Gorenstein, *Finite Simple Groups: An Introduction to their Classification*, Plenum Press, New York, 1982.

[54] R. Guralnick and K. Magaard, On the minimal degree of a primitive permutation group, *J. Algebra* **207** (1998), 127–145,

[55] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* **101** (1997), 255–287.

[56] R. Häggkvist and J. C. M. Janssen, All-even latin squares, *Discrete Math.* **157** (1996), 199–206

[57] W. A. Hodges, *Model Theory*, Cambridge University Press, Cambridge, 1993.

[58] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, Cambridge, 1990.

[59] I. M. Isaacs, W. M. Kantor, and N. Spaltenstein, On the probability that a group element is p-singular, *J. Algebra* **176** (1995), 139–181.

[60] J. R. Isbell, Homogeneous games II, *Proc. Amer. Math. Soc.* **11** (1960), 159–161.

[61] T. Ito and M. Kiyota, Sharp permutation groups, *J. Math. Soc. Japan* **33** (1981), 435–444.

[62] N. Iwahori, On a property of a finite group, *J. Fac. Sci., Univ. Tokyo* **11** (1964), 47–64.

[63] M. R. Jerrum, A compact representation for permutation groups, *J. Algorithms* **7** (1986), 60–78.

[64] M. R. Jerrum, Computational Pólya theory, pp. 103–118 in *Surveys in Combinatorics, 1995* (Peter Rowlinson, ed.), London Math. Soc. Lecture Notes **218**, Cambridge University Press, Cambridge, 1995.

[65] D. Jordan, Eine Symmetrieeigenschaft von Graphen, Graphentheorie und ihre Anwendungen, (Stadt Wehlen 1988), 17–20, Dresdner Reihe Forsch. 9, Dresden, 1988.

[66] A. Joyal, Une theorie combinatoire des séries formelles, *Adv. Math.* **42** (1981), 1–82.

[67] M. Kiyota, An inequality for finite permutation groups, *J. Combinatorial Theory* (A) **27** (1979), 119.

[68] M. W. Liebeck and L. Pyber, Upper bounds for the number of conjugacy classes of a finite group, *J. Algebra* **198** (1997), 538–562.

[69] M. W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra* **184** (1996), 31–57.

[70] M. W. Liebeck and A. Shalev, Classical groups, probabilistic methods and the (2,3)-generation problem, *Annals of Math.* **144** (1996), 77–125.

[71] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.

[72] A. Lucchini, F. Menegazzo and M. Morigi, Asymptotic results for primitive permutation groups and irreducible linear groups, to appear.

[73] A. Lucchini, F. Menegazzo and M. Morigi, Asymptotic results for transitive permutation groups, *Bull. London Math. Soc.*, to appear.

[74] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combinatorics, Probability & Computing* **2** (1993), 505–512.

[75] A. McIver and P. M. Neumann, Enumerating finite groups, *Quart. J. Math. Oxford* (2) **38** (1987), 473–488.

[76] A. Mahmoodi and P. J. Schellenberg, Equidistant permutation arrays, pp. 326–328 in C. J. Colbourn and J. H. Dinitz (eds.), *The CRC handbook of combinatorial designs*, CRC Press, Boca Raton, 1996.

[77] L. Maillet, Sur quelques propriétés des groupes de substitutions d'ordre donnée, *Ann. Fac. Sci. Toulouse*, **8** (1895), 1–22.

[78] A. Mann, Positively finitely generated groups, *Forum Mathematicum* **8** (1996), 429–459.

[79] A. Mann and C. E. Praeger, Transitive permutation groups of minimal movement, *J. Algebra* **181** (1996), 903–911.

[80] A. Mann and A. Shalev, Simple groups, maximal subgroups, and probabilistic aspects of profinite groups, *Israel J. Math.* **96** (1996), 449–468.

[81] D. Marušič, On vertex symmetric digraphs, *Discrete Math.* **36** (1981), 69–81.

[82] D. Marušič and R. Scapellato, Permutation groups, vertex-transitive digraphs and semiregular automorphisms, *Europ. J. Combinatorics* **19** (1998), 707–712.

[83] T. Maund, D. Phil. thesis, Oxford University, 1989.

[84] W. Myrvold, personal communication.

[85] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, 1944.

[86] P. M. Neumann and C. E. Praeger, An inequality for tactical configurations, *Bull. London Math. Soc.* **28** (1996), 471–475.

[87] C. E. Praeger, On permutation groups with bounded movement, *J. Algebra* **144** (1991), 436–442.

[88] C. E. Praeger, An O'Nan–Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs, *J. London Math. Soc.* (2) **479** (1993), 227–239.

[89] C. E. Praeger and A. Shalev, in preparation.

[90] L. Pyber, Asymptotic results for permutation groups, pp. 197–219 in *Groups and Computation*, (Larry Finkelstein and William M. Kantor, eds.), DIMACS Series in Discrete Mathematics and Theoretical Computer Science **11**, American Mathematical Society, Providence, RI, 1993.

[91] L. Pyber and A. Shalev, Asymptotic results for primitive permutation groups, *J. Algebra* **188** (1997), 103–124.

[92] R. Rado, Universal graphs and universal functions, *Acta Arith.* **9** (1964), 331–340.

[93] J. H. Redfield, The theory of group-reduced distributions, *Amer. J. Math.* **49** (1927), 433–455.

[94] C. Ryll-Nardzewski, On category in power $\leq \aleph_0$, *Bull. Acad. Pol. Sci. Sér. Math. Astr. Phys.* **7** (1959), 545–548.

[95] B. Sagan, *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*, Wadsworth & Brooks/Cole, Pacific Grove, CA, 1991.

[96] Á. Seress, The minimal base size of primitive solvable permutation groups, *J. London Math. Soc.* II. Ser. **53** (1996), 243–255.

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

[98] L. Svenonius, $\aleph_0$-categoricity in first-order predicate calculus, *Theoria* **25** (1959), 82–94.

[99] J. J. Sylvester, On arithmetical series, *Messenger of Math.* **21** (1892), 1–19; *Collected Mathematical Papers* Vol. 4 (1912), 687–731.

[100] H. Tarnanen, Upper bounds on permutation codes via linear programming, *Europ. J. Combinatorics* **20** (1999), 101–114.

[101] D. Zagier, On the distribution of the number of cycles of elements in symmetric groups, *Nieuw Arch. Wiskunde*, IV. Ser. **13** (1995), 489–495.

[102] H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, *Abh. Math. Sem. Hamburg* **11** (1936), 17–40.

[103] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg* **11** (1936), 187–220.

[104] B. I. Zil'ber, The structure of models of uncountably categorical theories, pp. 359–368 in *Proc. Internat. Congr. Math.* (Warsaw 1983).