Lectures on derangements

Peter J. Cameron
Queen Mary, University of London

Pretty Structures
Paris, May 2011

Abstract

These are notes from my lectures at the Pretty Structures conference at the Institut Henri Poincaré in Paris, in early May 2011. I had planned to give three talks about derangements; but in the event, the third lecture was devoted to the topic of synchronization, and as a result some of this material was not covered in the talks.

A general reference on permutation groups is my book [2].

Notes on synchronization (containing far more than I put into the single lecture in Paris) can be found at

`http://www.maths.qmul.ac.uk/~pjc/LTCC-2010-intensive3/`

1 From classical times

A *derangement* is a permutation of $\{1,\ldots,n\}$ which has no fixed points. In these lectures I will consider counting and finding derangements in the symmetric group S_n and its subgroups. On the way, we will see that derangements are intimately connected with many other topics in mathematics, including number theory, game theory, enumerative combinatorics, representations of quasigroups, and more.

A classical problem asks: how many derangements are there in the symmetric group? It turns out that the number is the closest integer to $n!/\mathrm{e}$. In other words, if we choose a random permutation, the probability that it is a derangement is close to $1/\mathrm{e}$. This is sometimes known as the "secretary problem" or "hat-check problem": if a secretary types n letters and addresses the envelopes, then puts

letters in envelopes at random, the probability that nobody gets their correct letter is close to $1/\mathrm{e}$.

Here are two proofs of this fact.

First proof: Inclusion–Exclusion The number of permutations of $\{1,\ldots,n\}$ which fix a given set of k points (and possibly more) is $(n-k)!$. So, if $d(n)$ is the number of derangements, then Inclusion–Exclusion gives

$$\begin{aligned} d(n) &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \end{aligned}$$

The series is the truncation of the Taylor series for e^x at $x=-1$. It is an alternating series, so the difference between the finite sum $d(n)/n!$ and its limit $1/\mathrm{e}$ is smaller than the next term, whose modulus is $1/(n+1)!$. So the difference between $d(n)$ and $n!\mathrm{e}^{-1}$ is smaller than $1/(n+1)$, proving our assertion.

Second proof: a structural proof Every permutation is uniquely expressible as the product of a derangement and an identity permutation (since the domain decomposes uniquely into the set of fixed points and the set of moved points). So the exponential generating functions

$$P(x) = \sum_{n\geq 0} \frac{n!\,x^n}{n!} = \frac{1}{1-x}, \quad I(x) = \sum_{n\geq 0} \frac{x^n}{n!} = \mathrm{e}^x, \quad D(x) = \sum_{n\geq 0} \frac{d(n)x^n}{n!}$$

of all permutations, identity permutations, and derangements respectively, satisfy

$$D(x)I(x) = P(x).$$

So $D(x) = e^{-x}/(1-x)$, from which the same formula as before is easily derived.

This proof is most naturally expressed in the language of species [13].

We will see a third proof using the Orbit-Counting Lemma later.

2 Jordan's Theorem

Let G be a subgroup of S_n. The *orbits* of G are the equivalence classes of the relation $\sim$ defined by $i \sim j$ if there exists $g \in G$ with $i^g = j$. We say that G is *transitive* if there is just one orbit.

In 1872, Jordan [12] proved:

Theorem 2.1 *A transitive subgroup of S_n (with $n > 1$) contains a derangement.*

I highly recommend Jean-Pierre Serre's beautiful paper "On a theorem of Jordan" [16], for an account of this theorem and some spectacular applications in topology, number theory, and modular forms.

The easiest proof to explain (essentially Jordan's, but dressed up differently) uses the *Orbit-Counting Lemma* (often called Burnside's Lemma, but not due to Burnside):

Theorem 2.2 *For any subgroup G of S_n, the number of orbits of G is equal to the average number of fixed points of elements of G.*

Now, if G is transitive, the average number of fixed points is 1; the identity fixes more than one point (if $n > 1$); so some element fixes fewer than one.

3 First variations on Jordan's Theorem

For the purposes of computation, a subgroup of the symmetric group S_n is conveniently described by giving a set of permutations which generates it. However, there is a problem which we need to address, since in principle we may be given a huge set of permutations which would take exponentially long just to read!

The way round this is to filter the permutations as they are read. My favourite version of this is due to Mark Jerrum [11]. He shows that every subgroup of S_n has a "special" generating set, where these special sets have the following properties:

- a special set contains at most $n-1$ permutations;
- if S is a special generating set for G, and g is any permutation in S_n, then a special generating set for $\langle G, g\rangle$ can be found in time polynomial in n.

In detail, we associate with each permutation g an edge $\{i, j\}$, where i is the smallest point moved by g, and $j = i^g$. A set of permutations is special if the corresponding set of edges is acyclic. Now the first property is clear. For the second, we show that if S is special but $S \cup \{g\}$ is not, then with a polynomial amount of processing we can replace g by g' such that $S \cup \{g'\}$ and $S \cup \{g\}$ generate the same subgroup, and the smallest point moved by g' is greater than the smallest point moved by g. After at most n such moves, either the new permutation becomes the identity, or a new special set is obtained.

So, by reading all the generators and doing a polynomial amount of computation after each one is read, we obtain a set of polynomially bounded size (indeed, at most $n-1$) generating the same subgroup. (Jerrum's filter actually shows that any subgroup of S_n can be generated by at most $n-1$ elements; this is not obvious!) So, for complexity questions about permutation groups, we may assume that the generating set has polynomial size.

Problem How difficult is it to find a minimum-size set of generators for G? Note that McIver and Neumann [15] showed that any subgroup of S_n can be generated by at most $n/2$ elements if $n > 3$. This is best possible (consider the group generated by $\lfloor n/2 \rfloor$ disjoint transpositions). But their proof is not obviously constructive; I do not know whether a generating set of size at most $n/2$ can be found in polynomial time.

3.1 Is there a derangement?

Now the obvious question about derangements is: how hard is it to decide whether a subgroup of S_n contains a derangement? Given Jordan's theorem, we might expect that this would be fairly easy. However, Taoyang Wu [5] showed that, given a set of generators for G (assumed to be of polynomial size), the problem of deciding whether G contains a derangement is NP-complete.

However, we can decide efficiently (in polynomial time, even in log-space) whether G is transitive. (This just asks whether the digraph having edges (i, j) whenever there is a generator mapping i to j is connected.) If G is transitive, then Jordan gives us a constant-time algorithm for the decision problem!

Problem Given a subgroup G of S_n having at most k orbits, where k is fixed, what is the complexity of deciding whether G contains a derangement?

3.2 Finding a derangement

What about the problem of finding a derangement in a transitive group? There is an efficient randomized algorithm depending on the following result of Cameron and Cohen [3]

Theorem 3.1 *If $n > 1$, then the proportion of derangements in the transitive subgroup G of S_n is at least $1/n$.*

Proof Let π be the *permutation character* of G (so $\pi(g)$ is the number of fixed points of g). This is a character, i.e. the trace of a matrix representation (by permutation matrices). However, we don't need any character theory.

Consider the function $\theta = (\pi - 1)(\pi - n)$. The average of π^2 over G is at least 2. For $\pi^2(g)$ is the number of ordered pairs fixed by g, so the average is equal to the number of orbits of G on ordered pairs. This is at least 2, since pairs (i,i) and (i,j) (with $j \neq i$) cannot lie in the same orbit. So the average of θ is at least $2-(n+1)+n = 1$. But $\theta(g) \leq 0$ unless g is a derangement, in which case $\theta(g) = n$. So the number of derangements is at least $|G|/n$.

We can see that equality holds if and only if two things happen:

- G has two orbits on ordered pairs, i.e. it is 2-transitive;
- $\pi(g) = 0$ or 1 for all non-identity elements $g \in G$.

In other words, equality holds if and only if G is *sharply 2-transitive*. Such groups are known to be the 1-dimensional affine groups over nearfields, and are associated with particular kinds of finite projective planes.

Back to finding derangements. Pick m random elements of G. (See the next paragraph for how to do this.) The probability that none of these elements is a derangement is at most $(1-1/n)^m < e^{-m/n}$; so with about cn^2 random elements we find a derangement with probability exponentially close to 1.

The method of choosing a random element is due to Sims, the father of computational permutation group theory. Sims showed that any subgroup G of S_n has a *strong generating set*. This consists of subsets $S_1, S_2, \ldots, S_b$ of G, where $b < n$ and $|S_i| \leq n$ for all i, such that every element of G can be written *uniquely* in the form $s_1 s_2 \cdots s_b$ with $s_i \in S_i$ for $i = 1, \ldots, b$. He showed that such a set can be found in polynomial time. Now to choose a random element of G, we just choose random elements of the polynomial-sized sets $S_1, \ldots, S_b$ and multiply them.

What about a deterministic algorithm for finding a derangement? There is one, but proof of its correctness uses the Classification of Finite Simple Groups. I will discuss this in the next section.

4 Second variations on Jordan's theorem

There are several problems, coming from a wide range of applications, where we seek derangements with some additional property.

4.1 Derangements of prime power order

I begin with a digression.

The quaternions form an algebra (associative but non-commutative) over the real numbers. This algebra is simple (it has no non-trivial proper ideals) and its centre consists of just the scalars. Such an algebra is called *central simple*. The Pauli spin matrices show that the quaternions can be represented by 2×2 matrices over the complex numbers; indeed, if we allow complex rather than real coefficients (in other words, take the tensor product of the quaternions with the complex numbers over the real numbers), the algebra is isomorphic to the algebra of all 2×2 complex matrices.

In the case of the real numbers, the quaternions are the only such (finite-dimensional) algebra. But in other cases, things are more generous. A *local field* is either a finite extension of the rationals, or a finite extension of $F(t)$, the function field in one variable over a finite field F. Now Fein, Kantor and Schacher [8] proved the following theorem:

Theorem 4.1 *Let K be a local field, and L a finite extension of K (with $L \neq k$). Then there are infinitely many different central simple algebras A over K such that $A \otimes_K L$ is a matrix algebra over L.*

From our point of view, the remarkable thing about this theorem is the following. Let G be the Galois group of (the normal closure of) L over K. Then G is a transitive subgroup of S_n, where n is the degree of L over K. Now Fein, Kantor and Schacher prove that the conclusion of their theorem holds if and only if G contains a derangement *of prime power order*, that is, one all of whose cycle lengths are powers of a fixed prime p. So their theorem is a consequence of the following result, which should be compared to Jordan's:

Theorem 4.2 *A transitive subgroup of S_n (with $n > 1$) contains a derangement of prime power order.*

The proof of Jordan's theorem is by elementary counting. For contrast, I will sketch the proof of this theorem.

First, we may assume, without loss of generality, that G is *primitive* (this means that it preserves no equivalence relation on $\{1,\ldots,n\}$ except for the two trivial relations, equality and the relation with a single equivalence class). For, if G does preserve an equivalence relation, it induces a transitive permutation group

on the set of equivalence classes; and if h is an element of G inducing a derangement of p-power order on the equivalence classes, then some power h^m (where m is coprime to p) induces a derangement of p-power order on the original points.

Next, we may assume, without loss, that G is a simple group. For if G is primitive, then a minimal normal subgroup of G is transitive (since its orbit partition is preserved by G), and is a direct product of copies of some finite simple group. Replace G by this group G_1. Now repeat the two steps to obtain a minimal normal subgroup G_2 of G_1, which is a simple group. Finally, repeating the first step, we may assume that the action of G_2 is primitive.

In group-theoretic terms, we have a simple group, which we now call G, and a maximal subgroup H (the stabiliser of a point in G); we want to find an element of prime power order which lies in no conjugate of H.

Now the Classification of Finite Simple Groups, announced in 1980 but not proved for another quarter of a century, provides a list of all the possible simple groups. Considering the various types of simple group, using detailed information about each, it is possible to prove the theorem.

Unfortunately, the proof of CFSG, as I shall call it for short, is very long (of the order of 10000 pages) and not at all easy to read even for a specialist. So adding the words "of prime power order" to Jordan's Theorem is done at great cost!

The other important thing to remark is that all the reductions in the proof, and finding the required element in each type of simple group, can be done in polynomial time. So we have finally answered the question at the end of the last section, in strengthened form: there is a deterministic polynomial-time algorithm for finding a derangement of prime power order in a transitive subgroup of S_n. Of course, the algorithm is rather complicated, and the proof of its correctness requires CFSG.

In computer science there is the notion of "derandomisation", finding a deterministic version of a randomised algorithm. In this case, where the randomised algorithm is so simple, and the deterministic algorithm so complicated, it may be worth testing these techniques to see whether they can be applied!

As a final remark, since the number-theoretic statement of Fein, Kantor and Schacher is equivalent to the statement about derangements, there is the possibility of finding a direct proof of their number-theoretic statement and deducing the fact about derangements from it, avoiding the need for CFSG. It is not at all clear to me whether such a proof could be made algorithmic.

4.2 Derangements of prime order

Not every transitive group contains a derangement of prime order; but examples are not so common. A transitive group is called *elusive* if it has no derangement of prime order. The smallest elusive group has degree 12. Elusive groups were studied in [4].

Here are two problems.

Problem Is it true that the set of degrees of elusive permutation groups has density zero?

Problem We say that a permutation group G is 2-*closed* if every permutation which preserves all G-orbits on ordered pairs belongs to G; equivalently, G is the automorphism group of an edge-coloured digraph. Mikhail Klin asked: Is it true that no 2-closed transitive group is elusive (i.e. every such group contains a derangement of prime order)? The truth of this would show that every vertex-transitive graph is a *pseudo-circulant*: that is, it can be partitioned into circulant graphs of prime order. This could be useful in the study of vertex-transitive graphs.

4.3 Which prime?

50 years ago, Isbell [10] was studying n-player zero-sum games, in the sense of von Neumann and Morgenstern. The theory of such games is of course very complicated; but there is a class of such games, called *simple games*, where all that matters is coalitions between players. If one set of players cooperate, we have essentially a 2-player game between this set and all the rest; the theory of such games is of course known. So an n-player game is determined by the set $\mathscr{W}$ of *winning coalitions*. This set has the following properties:

- it is closed upwards;
- for any set A of players, either A or its complement belongs to $\mathscr{W}$.

Isbell's intention was to study fair games, where no player has any advantage over any other. His idea was that a game is fair if its symmetry group (the group of permutations of the players preserving the game structure) acts transitively on the players. Now it is easy to see that

> A subgroup G of S_n is contained in the symmetry group of a simple game if and only if it contains no derangement of order a power of 2.

For if g is a derangement of 2-power order, then all its cycles have even length; taking alternate points in the cycles, we obtain a set A which is mapped to its complement by g. But if $\mathscr{W}$ is the set of winning coalitions in a simple game, then one or other of A and its complement belongs to $\mathscr{W}$; so $\mathscr{W}$ cannot be preserved by g. Conversely, it can easily be shown that, if G is a group containing no such derangement, then the orbits of G on subsets fall into complementary pairs; taking one of each pair (using the larger if the cardinalities are unequal) gives the set of winning coalitions in a simple game.

Isbell's conjecture There is a function f such that if $n = 2^a.b$ with $a > f(b)$, then any transitive group of degree n contains a derangement of 2-power order.

This would immediately imply that, for such values of n, there is no fair simple game on n players. This conjecture has been open for half a century now; it is one of the problems I would most like to see solved.

The conjecture can be generalised from 2 to an arbitrary prime: the general form asserts that there is a function f_p for any prime p such that, if $n = p^a.b$ with $a > f_p(b)$, then a transitive group of degree n contains a derangement of p-power order. This is open for all p. Halpenny and Spiga showed that it is true for primitive groups (unpublished), though this is no help for transitive groups.

I made an even stronger conjecture in the hope of making progress on this. The conjecture asserted that, for any prime p, there is a function g_p such that, if P is a permutation group of p-power order having b orbits each of size at least p^a, for $a > g_p(b)$, then P contains a derangement. Taking P to be the Sylow subgroup of a group G as in Isbell's conjecture, we see that the truth of this conjecture would imply that of Isbell's. Sad to say, this conjecture is false for all primes $p > 3$; this was shown by Crestani and Spiga [6].

5 Miscellanea

This section contains some miscellaneous results which fell off the end of the lectures.

5.1 The Shift Theorem

There's more to be said about counting derangements. The following result is due to Boston *et al.* [1]. Let P_i be the probability that a random element of G has exactly i fixed points, and $P(x) = \sum_{i=0}^{n} P_i x^i$, the probability generating function

for the number of fixed points of a random element. Also, let F_i be the number of orbits of G on the set of i-tuples of distinct points, and $F(x) = \sum_{i=0}^{n} F_i x^i/i!$ its exponential generating function. Often it is easier to compute the numbers F_i than the P_i: for example, if G is the symmetric group S_n, then

$$F_i = \begin{cases} 1 & \text{for } 0 \le i \le n, \\ 0 & \text{otherwise,} \end{cases}$$

so that $F(x)$ is the truncated exponential function.

The Shift Theorem asserts:

Theorem 5.1 *With the above notation, $F(x) = P(x+1)$. In particular, $P(x) = F(x-1)$, so that $P(0)$, the proportion of derangements in G, is equal to $F(-1)$.*

We recover the proportion of derangements in the symmetric group. In fact, we see that the distribution of fixed points in a random permutation is approximately Poisson with parameter 1.

The proof is easy. Since a permutation with j fixed points fixes $j(j-1)cdots(j-i+1)$ i-tuples of distinct points; so the Orbit-Counting Lemma gives

$$F_i = \sum_{j \ge 0} P_j j(j-1)\cdots(j-i+1).$$

Multiply by $x^i/i!$, sum over i, and reverse the order of summation on the right:

$$F(x) = \sum_{j \ge 0} P_j \sum_{i \ge 0} \binom{j}{i} x^i = \sum_{j \ge 0} P_j (1+x)^j = P(1+x).$$

In fact, this can be generalised. It is possible to calculate the joint distribution of the numbers of cycles of lengths $1, 2, 3, \ldots$, in the symmetric group; they are approximately independent Poisson variables with parameters $1, 1/2, 1/3, \ldots$. Indeed, there are multivariate forms of both polynomials P and F, and a multivariate Shift Theorem.

5.2 Other groups

One can ask about the limiting proportion of derangements in other permutation groups. For example, let $G(n,k)$ be the permutation group induced by S_n on the set of k-subsets of $\{1,\ldots,n\}$. For $n > 2k$ this is the automorphism group of the Kneser graph $K_{n,k}$.

One can show that, for fixed k, the proportion of derangements in $G(n,k)$ tends to a limit α_k as $n \to \infty$. Thus, $\alpha_1 = e^{-1}$. Also, it can be shown that $\alpha_2 = 2e^{-3/2}$. However, calculations by John Britnell and Mark Wildon show that the convergence to the limit is rather complicated. In addition, it is not known whether α_k increases monotonically with k, though Britnell and Wildon verified this for $k \leq 23$.

The reason for the importance of this class of groups can be seen from a paper of Diaconis, Fulman and Guralnick [7], which shows that they are in a sense the only classes of primitive groups in which the proportion of derangements is bounded away from zero.

5.3 Latin squares and quasigroups

A Latin square is an $n \times n$ array with n distinct entries, each of which occurs once in each row and once in each column. In other words, if the symbols are $1, \ldots, n$, then each row or column is a permutation.

A *quasigroup* is an algebraic structure consisting of a set with a binary operation whose Cayley table is a quasigroup; that is, if the operation is multiplication, then left and right division are unique (that is, the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions x and y for given a and b.

A representation theory of quasigroups, generalising that for groups, has been developed by J. D. H. Smith. It is "controlled" by the *multiplication group* of the quasigroup Q, the group generated by the rows and columns of the Cayley table of Q (regarded as permutations, that is, elements of the symmetric group). The representation theory is "trivial" if and only if the multiplication group is doubly transitive (that is, transitive on ordered pairs of distinct elements).

Now I conjectured that almost all quasigroups have trivial representation theory. ("Almost all" here means that the proportion of objects with the given property tends to 1 as $n \to \infty$.) This conjecture was proved by Łuczak and Pyber [14]:

Theorem 5.2 *For almost all Latin squares, the group generated by the rows is the symmetric group.*

Their proof used the following remarkable result:

Theorem 5.3 *For almost all elements g of the symmetric group S_n, the only transitive subgroups of S_n containing g are S_n and (possibly) A_n.*

The class of permutations referred to are in some sense the opposite extreme from derangements, which are permutations which lie in no point stabiliser. Similarly, cycles are the only permutations lying in no intransitive subgroup. The theorem asserts that most permutations lie in no proper transitive subgroup. The rate of convergence in the theorem is not known.

Now the first row of a random Latin square is a random permutation, and the group generated by the rows is obviously transitive; so almost always it is symmetric or alternating. The proof is finished by a theorem of Häggkvist and Janssen [9], asserting that the probability that all rows of a Latin square are even permutations is exponentially small.

A *loop* is a "group without the associative law", a quasigroup with identity and inverses. Is it also true that almost all loops have trivial representation theory? The above argument no longer applies, since (assuming that the first element is the identity) the first row is the identity permutation. But the second row is a (nnon-uniform!) random derangement.

In detail, we define a probability measure on derangements can be defined as follows. Say that a Latin square is "normalised" if its first row is the identity. Now define the probability of a derangement g to be the proportion of normalised Latin squares which have second row g. This probability depends only on the cycle structure of the derangement, but is not the uniform distribution for $n > 3$. For example, when $n = 4$, the derangement $(1,2)(3,4)$ has probability $1/6$, while $(1,2,3,4)$ has probability $1/12$. (Said otherwise, there are 4 normalised Latin squares with second row $[2,1,4,3]$, but only 2 with second row $[2,3,4,1]$.

However, experiment suggests that this probability distribution is very close to the uniform distribution.

For example, for $n = 7$, the table below gives the numbers of normalised Latin squares having a given derangement with a specified cycle type as second row.

Cycle type	Number of squares
7	6566400
5.2	6604800
4.3	6543360
3.2.2	6635520

5.4 Further directions

There are interesting things to say about infinite analogues (not of derangements themselves, but of the formal methods for counting them, including the Shift The-

orem), and about analogues for linear groups over finite fields; but I will not speak of these here.

References

[1] 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.

[2] Peter J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts **45**, Cambridge University Press, Cambridge, 1999.

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

[4] Peter J. Cameron, Michael Giudici, Gareth A. Jones, William M. Kantor, Mikhail H. Klin, Dragan Marušić and Lewis A. Nowitz, Transitive permutation groups without semiregular subgroups, *J. London Math. Soc.* (2) **66** (2002), 325-333.

[5] P. J. Cameron and T. Wu, The complexity of the weight problem for permutation and matrix groups, *Discrete Math.* **310** (2010), 408–416.

[6] Eleonora Crestani and Pablo Spiga, Fixed-point-free elements in p-groups, *Israel J. Math.* **180** (2010), 413–424.

[7] Persi Diaconis, Jason Fulman, and Robert Guralnick, On fixed points of permutations, *Journal of Algebraic Combinatorics* **28** (2007), 189–218.

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

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

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

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

[12] C. Jordan, Recherches sur les substitutions, *J. Math. Pures Appl. (Liouille)* **17** (1872), 351–387.

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

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

[15] Annabel McIver and Peter M. Neumann, Enumerating finite groups, *Quart. J. Math.* (2) **38** (1987), 473–488.

[16] Jean-Pierre Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.