# Derangements

Peter J. Cameron

18 April 2013

# Derangements

A derangement is a permutation with no fixed points.
Dante Alighieri, in the "Inferno" section of the *Divine Comedy*, wrote:

> *For [Luck] your science finds no measuring-rods; …*
> *Her permutations never know truce nor pause*

Perhaps we should interpret the first line as meaning "there cannot be a theory of probability", and the second as meaning "a random permutation is a derangement".

If the latter, then he was wrong, although prescient in asking the question:

Theorem

*The number of derangements of $n$ points is the integer nearest to* $n!/\mathrm{e}$.

In other words, the probability that a random permutation is a derangement is very close to $1/\mathrm{e} = 0.367879441\ldots$

# Mathematics for the masses

This problem is taken from the puzzle page of METRO, 20 December 2000. First the following question was posed.

*Match each of these languages to where they are spoken:*

| | |
|---|---|
| 1. Amharic | A. Brazil |
| 2. Farsi | B. Ethiopia |
| 3. Portuguese | C. India |
| 4. Telegu | D. Iran |
| 5. Urdu | E. Pakistan |

The paper then asked:

> *If the options for this puzzle were given in an entirely random order, how many of the five pairs of answers would line up correctly in the same row, averaged over many puzzles? What about if there were ten options in each column?*

Let's add another part. Suppose that one particular order is chosen, and the options were given by starting in a random position and then following the given order cyclically. What is the number of correct pairs on average?

# The Orbit-Counting Lemma

Let $G$ be a permutation group on a finite set $X$. For $g \in G$, let $\mathrm{fix}(g)$ be the number of points of $X$ fixed by $g$.

## Theorem

*The number of orbits of $G$ in $X$ is*

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g).$$

In other words, if we choose a random element of $G$ (from the uniform distribution), its expected number of fixed points is equal to the number of orbits of $G$, and so is 1 if $G$ is transitive. This solves the second METRO puzzle.

# On a theorem of Jordan

J.-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

Theorem (Jordan, 1872)

*A transitive permutation group on a set of size $n > 1$ contains a derangement.*

For the average number of fixed points is 1, and the identity fixes more than one …
My fifteen minutes of fame:

Theorem (Cameron and Cohen, 1992)

*In a transitive permutation group on a set of size $n > 1$, the proportion of derangements is at least $1/n$.*

# Proof

$$\begin{aligned} \sum 1 &= |G|, \\ \sum \mathrm{fix}(g) &= |G|, \\ \sum \mathrm{fix}(g)^2 &\geq 2|G|. \end{aligned}$$

So

$$\sum(\mathrm{fix}(g)-1)(\mathrm{fix}(g)-n) \geq (2-(n+1)+n)|G| = |G|.$$

In this sum, derangements contribute $n$, all other elements have non-positive contribution.

The theorem is best possible.

# Applications

See Serre's paper for a number of applications in number theory and topology. For example:

- Let $f$ be an integer polynomial of degree $n > 1$, irreducible over $\mathbb{Q}$. Then $f$ has no roots mod $p$ for infinitely many primes $p$ (indeed, for at least a proportion $1/n$ of all primes).
- Let $\pi : T \to S$ be a covering map of degree $n \geq 2$, and suppose that $T$ is arcwise connected but not empty. Then there is a continuous closed curve in $S$ which cannot be lifted to $T$.

# Prime power order

Jordan's Theorem tells us that a transitive group of degree $n > 1$ contains a derangement.

### Theorem (Fein–Kantor–Schacher)

*A transitive group of degree $n > 1$ contains a derangement of prime-power order.*

The proof uses the Classification of Finite Simple Groups, together with detailed analysis of the various families of simple groups. More on this later …
Moreover, this theorem is *equivalent* to the statement:

### Theorem (Fein–Kantor–Schacher)

*The relative Brauer group of a finite extension of global fields is infinite.*

# Which prime?

## Conjecture

*For any prime $p$, here is a function $f_p$ such that, if $n = p^a \cdot b$ with $p \nmid b$ and $a \geq f(b)$, then a transitive group $G$ of degree $n$ contains a fixed-point-free $p$-element.*

This conjecture was made (for $p = 2$) by Isbell in the early 1960s in connection with game theory (in the von Neumann–Morgenstern sense). He showed that there is a simple $n$-player game which is fair (no player has an advantage over the others) if and only if there is a transitive group of degree $n$ containing no fixed-point-free 2-element.
The conjecture is still open.

# A possible approach?

The conjecture is not typical of permutation group problems, in that there is no simple reduction to the case of primitive groups (unlike the Fein–Kantor–Schacher theorem).
It would follow from the truth of the following statement:

> *For any prime $p$, there is a function $g_p$ such that a $p$-group with $b$ orbits each of size at least $p^{g_p(b)}$ has a fixed-point-free element.*

However, this statement is false for $p \geq 5$: Crestani and Spiga constructed a pro-$p$ group which can be “cut off” at infinitely many levels to give counterexamples.

# An example

### Example

There is a constant $\alpha_k > 0$ so that the proportion of derangements in $S_n$ acting on $k$-sets tends to $\alpha_k$ as $n \to \infty$. (For example, $\alpha_1 = \mathrm{e}^{-1} = 0.3679\ldots$, while $\alpha_2 = 2\mathrm{e}^{-3/2} = 0.4463\ldots$.)

There is a formula for $\alpha_k$ as a sum over subsets of the partitions of $k$. But most of the terms cancel, so I suspect there is a much simpler formula!

### Problem

*Is it true that $\alpha_k \to 1$ monotonically as $k \to \infty$?*

Persi Diaconis *et al.* have some recent results relevant to this.

# A shift theorem

Let $G$ be a permutation group on $X$.
Let $P_G(x)$ be the probability generating function for fixed points: the coefficient of $x^d$ is the probability that a random element of $G$ has exactly $d$ fixed points.
Let $Q_G(x)$ be the exponential generating function for orbits on $d$-tuples of distinct elements: the coefficient of $x^d$ is the number of such orbits divided by $d!$.
A simple application of the Orbit-Counting Lemma gives

## Theorem

$Q_G(x) = P_G(x+1)$.

In particular, the proportion of derangements is $P_G(0) = Q_G(-1)$.
For the symmetric group, $Q_G(x)$ is the truncated exponential series, so $P_G(0)$ is very close to $\mathrm{e}^{-1}$.

# A puzzle

What happens for infinite permutation groups?

It may be difficult to give a meaning to “the probability that a random element has $d$ fixed points”: there may be elements with infinitely many fixed points, and $G$ may have no natural probability measure (it may fail to be locally compact).

However, $Q_G(x)$ makes sense (at least as a formal power series) in the case of oligomorphic permutation groups, those which have only finitely many orbits on $d$-tuples of distinct elements for all $d$.

For such groups it may be possible to give a meaning to $Q_G(-1)$; can we make sense of it as the “probability of a derangement”?

# Examples

- If $G$ is the symmetric group on an infinite set, then there is just one orbit on $d$-tuples of distinct elements for all $d$. So $Q_G(x) = \mathrm{e}^x$, and $Q_G(-1) = \mathrm{e}^{-1}$. This seems reasonable if we regard $G$ as a limit of finite symmetric groups …
- Let $G$ be the group of order-preserving permutations of the rational numbers. Then $G$ has $d!$ orbits on $d$-tuples (corresponding to the possible orderings), and $Q_G(x) = \sum x^d = 1/(1-x)$. Thus $Q_G(-1) = 1/2$: recall Euler's equation

  $$1 - 1 + 1 - 1 + \cdots = \tfrac{1}{2}.$$

  Is there a sense in which half the elements of this group are derangements? There is no sequence of finite groups with limit $G$.
- Let $G$ be the group of permutations preserving the cyclic ordering of the complex roots of unity. Then $Q_G(x) = \log(1-x)$, and $Q_G(-1) = \log 2$.

In the previous cases, either $Q_G(x)$ converges at $x = -1$, or the value there can be obtained by analytic continuation. But this is by no means typical.

- Let $G$ be the infinite symmetric group acting on the set of 2-element subsets of its natural domain. Then $Q_G(x)$ diverges for all $x \neq 0$. However, $Q_G(x)$ is a different sort of limit. Let $G^{(m)}$ denote the symmetric group of degree $m$ acting on 2-sets. Then the coefficient of $x^n$ in $Q_{G^{(m)}}(x)$ is constant for $m > 2n$, and equals the coefficient in $Q_G(x)$; so we have a very strong form of coefficient-wise convergence. And $Q_{G^{(m)}}(-1)$ tends to the limit $2\mathrm{e}^{-3/2}$ as $m \to \infty$.

These examples are not typical of oligomorphic groups, but in general we have no way to establish a “value” for $Q_G(-1)$.

# Finding a derangement

Given a permutation group $G$ on $n$ points (e.g. by a set of generating permutations), how do we go about finding a derangement in $G$? Of course, $G$ may be bigger than exponential in $n$.

In general, it is known that even the question of *existence* of a derangement is NP-complete (even if $G$ is an elementary abelian 2-group).

However, if $G$ is transitive (which we can easily check), then we know by Jordan's theorem that the answer to the existence question is "yes". The problem of finding one remains.

# A randomized algorithm

Let $G$ be transitive.
We can pre-process the generators for $G$ to get a strong generating set, using which we can choose a sequence of independent random elements of $G$. Each one has probability at least $1/n$ of being a derangement; so by choosing about $n^2$ random elements, the probability of not obtaining a derangement is at most $(1-1/n)^{n^2} \approx \mathrm{e}^{-n}$. So we will succeed very quickly.
Can this algorithm be derandomized?

# First approach

Emil Vaughan pointed out that the method of Fein, Kantor and Schacher is constructive, and can be implemented in polynomial time – so we can even find a derangement of prime power order.

However, it is not straightforward, and requires CFSG to prove its correctness.

By passing to a normal subgroup, and to the action on a system of blocks of imprimitivity, we can assume that $G$ is a simple group, and the point stabiliser is a maximal subgroup $H$. We need to find a conjugacy class of elements (of prime power order) lying outside $H$. For this we have to identify the natural action of $G$, and then choose appropriate elements there.

For example, if $G$ is $\mathrm{PSL}(n, q)$, then the class of transvections avoids most of the maximal subgroups, while irreducible cycles of order a primitive divisor of $q^n - 1$ handle the rest.

# Second approach

This year, I received a preprint from Vikraman Arvind in Chennai, in which there is a beautifully simple deterministic algorithm for finding a derangement.

Recall the puzzle about matching languages to countries. If we start with a fixed ordering and then permute it by a random cyclic permutation, how many pairs are correct (on average)? The answer is 1, but strictly this requires a generalisation of the Orbit-Counting Lemma.

### Theorem

*Let $G$ be a transitive permutation group of degree $n$. Then the average number of fixed points of the elements in any coset of $G$ (in the symmetric group) is equal to* 1*.*

If $G$ is not transitive, there is no formula for the average number of fixed points of the elements of a coset, but it can be computed in polynomial time, as follows.

Consider the coset $Gh$, for $h \in S_n$. Count pairs $(x, g)$, with $x \in X$ and $g \in G$, such that $xgh = x$. This is $|G|$ times the average we are trying to compute.

This sum can be computed another way. We require $xg = xh^{-1}$. If $x$ and $xh^{-1}$ lie in different $G$-orbits, there are no such pairs; otherwise, the set of possible $g$ is a coset of the stabiliser of $x$, and so the number is $|G|$ divided by the orbit size.

So the algorithm is: for $x \in X$, check whether $x$ and $xh^{-1}$ lie in the same $G$-orbit: if so, add in the reciprocal of the size of this orbit. The final total is the required average.

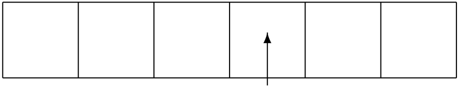
In particular, if $G$ is transitive, we sum $1/n$ for all $n$ points of $X$, obtaining the answer 1.

The algorithm works as follows. We start with a permutation group $G$, and assume we also have a base, a sequence $(x_1, x_2, \ldots, x_b)$ of points of $X$ whose (pointwise) stabiliser is the identity.

We begin with the coset $G$, in which the average number of fixed points is 1.

If we are in a coset $G_ih_i$, where $G_i$ is the stabiliser of $(x_1, \ldots, x_i)$, then we split it into cosets of $G_{i+1}$, and choose one where the average number of fixed points is at most the average in the original coset $G_ih_i$.

Cosets of $G_{i+1}$ in $G_ih_i$



Average number of fixed points $= a$

Coset with average $\leq a$

At the first stage, we can assume that the average is strictly less than 1, since the coset $G_1$ has average greater than 1 – it is an intransitive group.
At each subsequent stage, the average decreases (perhaps not strictly).
At the last stage, our coset is a single element whose number of fixed points is strictly less than 1, i.e. a derangement.

### Problem

*Is there an "elementary" algorithm (not requiring CFSG to prove its correctness) to find a derangement of prime power order?*

Another open problem is:

### Problem

*What is the complexity for the problem of counting the number of derangements in a transitive group?*

It is known that this number can be efficiently approximated.
For not necessarily transitive groups, the problem is #P-complete.