# Finding a derangement

Peter J. Cameron, CSG, January 2013

## 1 Derangements

A *derangement*, or *fixed-point-free permutation*, is a permutation on a set $\Omega$ which leaves no point fixed.

Dante Alighieri, in the *Inferno* (the first part of the Divine Comedy) said,

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

Today we do have a measuring rod for luck, namely the theory of probability; and we know also that about 36.79% (1/e) of random permutations have no "truce or pause", that is, no fixed points – a standard result of enumerative combinatorics.

However, we want to know about derangements, not in the symmetric group, but in arbitrary groups of permutations. Their existence and enumeration has applications in many other fields; I recommend to you Jean-Pierre Serre's paper "On a theorem of Jordan", in *Bull. Amer. Math. Soc.* **40** (2003), 429–440. The theorem of Jordan asserts that a transitive permutation group contains a derangement; we will see why soon.

## 2 Orbit-counting lemma and Jordan's theorem

Let $\mathrm{fix}(g)$ be the number of fixed points of the permutation $g$ (so that $g$ is a derangement if and only if $\mathrm{fix}(g) = 0$). The celebrated "Orbit-counting Lemma" asserts:

**Theorem 1** *Let $G$ be a permutation group on a finite set $\Omega$. Then the number of orbits of $G$ is equal to the average number of fixed points of $G$, that is,*

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

I will give a proof, since we will use the technique again. We count in two ways the number of pairs $(g,x)$ with $g\in G$, $x\in\Omega$, such that $xg=x$. Choosing $g$ first, this sum is clearly equal to

$$\sum_{g\in G}\mathrm{fix}\,g.$$

Now choose $x$ first. According to the *Orbit–Stabiliser Theorem*, the number of elements $g$ fixing $x$ (the order of the *stabiliser* of $x$) is equal to $|G|$ divided by the size of the *orbit* of $G$ containing $x$. This means, that the sum, over all points $x$ in a given $G$-orbit, of $|\,\mathrm{Stab}_G(x)|$, is equal to $|G|$. So the sum over all points $x\in\Omega$ is $|G|$ times the number of orbits.

Equating the two expressions proves the theorem.

Said otherwise, we form a bipartite graph on the vertex set $G\cup\Omega$ with an edge from $g$ to $x$ whenever $g$ fixes $x$. The proof of the Orbit-Counting Lemma simply involves counting edges of this graph. Mark Jerrum showed that, starting anywhere in $\Omega$, the random walk with an even number of steps (returning to $\Omega$) has limiting distribution which is uniform on the *orbits* of $G$ – a useful tool if there are some very small orbits!

Jordan's theorem is a corollary of this:

**Theorem 2** *A transitive finite permutation group on more than one point contains a derangement.*

For the average number of fixed points of the elements of the group is 1, while the identity fixes more than one point; so some element fixes less than one point.

As Serre remarks, this theorem was quantified by Arjeh Cohen and me:

**Theorem 3** *Let $G$ be a transitive finite permutation group on a set of $n$ points, where $n>1$. Then the number of derangements in $G$ is at least $|G|/n$.*

To prove this, consider the sum

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

Now $\mathrm{fix}(g)^2$ is the number of fixed points of $G$ acting on the set $\Omega^2$ of ordered pairs of points of $\Omega$; the group has at least two orbits on this set (since pairs $(x,x)$ and $(x,y)$ with $y\neq x$ lie in different orbits), so the average is at least two. Thus

$$\frac{1}{|G|}\sum_{g\in G}(\mathrm{fix}(g)^2-(n+1)\,\mathrm{fix}(g)+n)\geq 2-(n+1)+n=1.$$

On the other hand, every derangement contributes $n$ to the sum; the identity and the elements with just one fixed points contribute 0; and the contribution of any other element is negative. So we have

$$\frac{1}{|G|}\sum_{g\in G}(\mathrm{fix}(g)-1)(\mathrm{fix}(g)-n)\leq dn,$$

where $d$ is the number of derangements. So $d\geq |G|/n$, as claimed.

We see that the bound is met if and only if

- $G$ has just two orbits on $\Omega^2$ (that is, $G$ is 2-transitive);
- no non-identity element fixes more than one point.

In other words, $G$ is *sharply 2-transitive*.

# 3 Variants

A remarkable variant of Jordan's Theorem was found by Bill Kantor, and appears in a paper of Fein, Kantor and Schacher, *J. Reine Angew. Math.* **328** (1981), 39–57. Remarkably the paper is on relative Brauer groups of finite extensions of global fields.

**Theorem 4** *A transitive finite permutation group on more than one point contains a derangement of prime power order.*

The small addition to Jordan's theorem changes things completely. A sketch of the proof: by elementary means, we can reduce to the case when the group is simple and acts primitively (that is, the stabiliser of a point is a maximal subgroup); the Classification of Finite Simple Groups gives us a list of primitive groups; then it is possible to go through the list and show that, if $G$ is a finite simple group and $H$ a maximal subgroup, then $G$ contains an element of prime power order which lies in no conjugate of $H$.

No "elementary" proof is known.

Another, much more elementary, variant arose in combinatorial enumeration.

**Theorem 5** *Let $G$ be a finite transitive permutation group. Then the average number of fixed points of all the elements in a coset $Gh$ of $G$ (in the symmetric group) is equal to* 1.

The proof is as before: we count pairs $(g, x)$ for which $xgh = x$, that is, $xg = xh^{-1}$. Again this sum is equal to $|G|$ times the average number of fixed points of elements of $Gh$; also, since the elements mapping $x$ to $xh^{-1}$ form a coset of the stabiliser of $x$, there are $|G|/|\Omega|$ such $g$ for each $x \in \Omega$, so $|G|$ pairs $(g, x)$ altogether.

# 4 Finding a derangement

It is known that the problem of deciding whether a subgroup $G$ of the symmetric group of degree $n$ (given by generating permutations) contains a derangement is NP-complete.

For transitive groups, the decision problem is trivial, by Jordan's theorem. But how hard is it to actually *find* a derangement?

Given generators for $G$, we can in polynomial time find a *base* and a *strong generating set* for $G$. Having this, it is easy to choose a (uniform) random element of $G$. Now by the quantification of Jordan's theorem, the probability that this element is not a derangement is at most $1 - 1/n$, so the probability that we don't find a derangement when we choose $m$ random elements is at most $(1 - 1/n)^m$, which is exponentially small if $m = cn^2$, for example. So there is a very easy randomized polynomial-time algorithm.

Some time ago, I asked for a deterministic polynomial-time algorithm.

Emil Vaughan pointed out that we can use Kantor's work to settle this. The reductions in Kantor's theorem, and the constructions which produce the required derangements, can all be done in polynomial time. However, the resulting algorithm is rather complicated, and requires the Classification of Finite Simple Groups to prove its correctness.

So I was delighted when Vikraman Arvind from Chennai sent me a preprint he had just posted on the arXiv (article id 1301.0379), giving an elementary and simple algorithm. In the rest of this note, I will give his algorithm.

# 5 Arvind's algorithm

We saw that the average number of fixed points of an element in a coset of a transitive group is 1. This result cannot be extended to intransitive groups; but the key to Arvind's algorithm is the following observation:

**Theorem 6** *Let $G$ be a permutation group on a finite set $\Omega$, and $h$ any permutation on $\Omega$. Then the average number of fixed points of elements in the coset $Gh$ can be computed in polynomial time.*

We follow the same argument as before, counting pairs $(x, g)$ with $xgh = x$, or $xg = xh^{-1}$. If $xh^{-1}$ is not in the $G$-orbit of $x$, there are no such elements; otherwise, the elements form a coset of the stabiliser of $x$, so their number is $|G|$ divided by the size of the $G$-orbit of $x$. So the average is obtained by summing, over all $x$ for which $xh^{-1}$ lies in the $G$-orbit of $x$, the reciprocal of the size of this $G$-orbit.

Now from this theorem, it is clear that the following is the case. Let $G$ be a permutation group on $\Omega$, and $K$ a subgroup of $G$. Then the coset $Gh$ splits into cosets of $K$; if we know coset representatives for $K$ in $G$ then, in polynomial time, we can choose a coset of $K$ contained in $Gh$ in which the average number of fixed points is at most the average over all of $Gh$.

Now start with our transitive group $G$. At any step in the algorithm, we will have a subgroup $K$ of $G$ (the stabiliser of a number of points) and a distinguished coset $Kh$ of $K$. We start with the subgroup $G$ and coset $G$.

> Choose a point and compute its stabiliser $K'$ in $K$. Then the coset $Kh$ splits into cosets of $K'$; choose one such that the average number of fixed points is at most the average over $Kh$.

Eventually the coset becomes a single element; stop at that point.

Now in the original group $G$, the average number of fixed points is 1; it decreases (non-strictly) as the algorithm runs. We can assume that it decreases strictly at the first step. For the stabiliser of a point has at least two orbits, so the average over this subgroup is 1; so there is another coset in which the average is strictly less than 1.

So the single element at the end of the algorithm has less than one fixed point; that is, it is the required derangement.