Inclusion-Exclusion and Derangements

The goal here is to count the number **derangements**, i.e, the number of bijective (or one-to-one) functions[1] $\pi : [n] \to [n]$ which have the property that $\pi(i) \neq i$ for all $i \in [n]$. We are after a formula which is a function of n – call $D(n)$ the number of such derangements. For example, $D(3) = 2$. This is easy to see because the only two solutions are

$$(2, 3, 1)$$

and

$$(3, 1, 2)\ .$$

(Here, (a, b, c) is to be read as $\pi(1) = a$, $\pi(2) = b$, and $\pi(3) = c$.) But what about $D(n)$ for an arbitrary n? We are going to show that $D(n)$ is close to $n!/e$, where $e = 2.71828\ldots$ is Euler's number.

Setting up the problem. Towards using the inclusion-exclusion principle, we need to think of the set of derangements as being described by the set of π's satisfying

$$\pi(1) \neq 1\ \wedge\ \pi(2) \neq 2\ \wedge \pi(3) \neq 3\ \wedge \cdots\ \wedge\ \pi(n) \neq n\ .$$

By DeMorgan's laws, this is equivalent to counting the number of π's that do *not* satisfy

$$\pi(1) = 1\ \vee\ \pi(2) = 2\ \vee \pi(3) = 3\ \vee \cdots\ \vee\ \pi(n) = n\ .$$

We formalize this using *sets*. First of all, let S_n be the set of one-to-one $\pi : [n] \to [n]$. We know that $|S_n| = n!$ already. Also, for any $i \in [n]$, let

$$A_i = \{\pi \in S_n\ :\ \pi(i) = i\}\ .$$

Note that we have defined n sets here, $A_1, \ldots, A_n$. Now, by the above, we want the set of π's which are in S_n, but not in $A_1 \cup \cdots \cup A_n$. In other words,

$$D(n) = |S_n \backslash (A_1 \cup \cdots \cup A_n)| = |S_n| - |A_1 \cup \cdots \cup A_n| = n! - |A_1 \cup \cdots \cup A_n|\ , \tag{1}$$

where the second equality follows from the fact that $A_1 \cup \cdots \cup A_n \subseteq S_n$, because the A_i' s are defined as subsets of S_n.

Using inclusion-exclusion. We now want to evaluate (1) above. By the inclusion-exclusion principle,

$$|A_1 \cup \cdots \cup A_n| = \sum_{\varnothing \neq I \subseteq [n]} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|\ . \tag{2}$$

To continue, we need to know what $|\bigcap_{i \in I} A_i|$ is. Note that for any non-empty $I \subseteq [n]$, having $\pi \in \bigcap_{i \in I} A_i$ means that $\pi(i) = i$ for all $i \in I$, but there is no restriction on $\pi(j)$ for $j \in [n] \backslash I$ –

[1] Recall that $[n]$ is a shorthand for $\{1, \ldots, n\}$.

therefore, there are $(n - |I|)!$ ways of choosing $\pi(j)$'s for $j \in [n] \setminus I$. (Remember, we look at π's which are one-to-one!) In other words,

$$\left| \bigcap_{i \in I} A_i \right| = (n - |I|)! \tag{3}$$

for all non-empty $I \subseteq [n]$.

Now, we plug (3) into (2), and obtain

$$|A_1 \cup \cdots \cup A_n| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} (n - |I|)! \,. \tag{4}$$

Let us now simplify this. We are summing over all non-empty $I \subseteq [n]$ – i.e., there are $2^n - 1$ summands – and the summand is $(-1)^{k+1}(n-k)!$ for any I with size k, regardless of how I exactly looks like. Moreover, there are $\binom{n}{k}$ such I's for each $k \in [n]$. Therefore, we can instead write

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!(n-k)!} \cdot (n-k)! = \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!} \,. \tag{5}$$

Note that the second equality follows from the definition of the binomial coefficient, and the last equality follows by simplifying $(n-k)!$ away.

To wrap up, let us plug (5) into (1), and obtain

$$D(n) = n! - \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!} = n! + \sum_{k=1}^{n} (-1)^{k} \frac{n!}{k!} = \sum_{k=0}^{n} (-1)^{k} \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \,, \tag{6}$$

where the first equality uses that $(-1)^{k+1} = (-1) \cdot (-1)^k$ (and this allows us to "flip" the sign!), and the second uses the fact that $(-1)^k \frac{n!}{k!} = 1$ for $k = 0$ – so we have taken-in the $n!$ as the $k = 0$ term into the sum.

Interpreting this. We are actually done – i.e.,

$$D(n) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

is the best we can expect to prove as an *exact* formula. However, we can get a feel of what this means, by observing that for any x,

$$\sum_{k=0}^{n} \frac{x^k}{k!}$$

converges to e^x as n goes to infinity. Therefore, in our case, $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ goes towards $e^{-1} = 1/e$ as n goes to infinity. Which explains why (as we claimed above) $D(n) \approx n!/e$ as n grows large.

In fact, one can do even better, and show that $D(n)$ is always the closest integer to $n!/e$ (the latter is never an integer).

Was I supposed to come up with it by myself? This goes beyond the type of homework questions we are going to ask – but it is entirely solvable with the tools from class. The problem was first posed by Pierre Raymond de Montmort, a French mathematician, in 1708. He only solved it in 1713, and so did Nicholas Bernoulli, a Swiss mathematician, and one out of many Bernoullis who are famous mathematicians.