Two decks of cards

INCLUSION–EXCLUSION PRINCIPLE and the number of derangements are the topics of the problem [1] in this section.

> ### Problem
>
> A deck of n different cards is shuffled and laid on the table by your left hand, face down. An identical deck of cards, independently shuffled, is laid at your right hand, also face down. You start turning up cards at the same rate with both hands, first the top card from both decks, then the next-to-top cards from both decks, and so on. What is the probability that you will simultaneously turn up identical cards from the two decks?

The shuffling implies equally likely outcomes so the probability is the number of outcomes with an identical card turning up divided by the number of total outcomes. The number of total outcomes is $(n!)^2$ since there are $n!$ possible shuffling outcomes of one deck (the number of permutations of S_n).

The set of outcomes where an identical card turns up seems harder to count. It feels easier to count its complement: the number of outcomes when no identical card comes up. There are $n!$ ways in which the first deck is shuffled. For a given permutation $\pi \in S_n$ of the first deck we need to count all the permutations $\rho \in S_n$ of the second deck for which $\forall i : 1 \leq i \leq n : \rho(i) \neq \pi(i)$. Let $A_\pi = \{\rho \in S_n : \forall i : 1 \leq i \leq n : \rho(i) \neq \pi(i)\}$.

Let $D_n = \{\tau \in S_n : \forall i : 1 \leq i \leq n : \tau(i) \neq i\}$. A permutations from D_n is called a **derangement**. We introduce the notation $!n = |D_n|$ for the number of derangements.

Lemma 1.1.
$$|A_\pi| = |D_n|$$

Proof. We need to present a bijection $f : D_n \to A_\pi$. We define $f(\tau) =$

$\pi \circ \tau$. First we verify that f is well-defined, i.e. $f(\tau) \in A_\pi$.

$$\forall i : 1 \leq i \leq n :$$
$$f(\tau)(i) = (\pi \circ \tau)(i)$$
$$= \pi(\tau(i)) \neq \pi(i)$$
$$\text{because } \tau(i) \neq i$$

Next we show that f is injective: $f(\tau_1) = f(\tau_2)$ implies $\pi \circ \tau_1 = \pi \circ \tau_2$. S_n is a group, so $\tau_1 = \tau_2$. Also f is surjective because: $\forall \rho \in A_\pi$ we have $\pi^{-1} \circ \rho \in D_n$ because $\rho(i) \neq \pi(i)$ implies $(\pi^{-1} \circ \rho)(i) \neq i$. $f(\pi^{-1} \circ \rho) = \rho$. $\square$

From lemma 1.1 we now know that the number of outcomes when no identical card comes up is $!n \cdot n!$ and the probability requested in the problem is

$$P = 1 - \frac{!n \cdot n!}{n!^2} = 1 - \frac{!n}{n!}$$

What remains is to compute $!n$. Let us look again at the set of derangements: $D_n = \{\tau \in S_n : \forall i : 1 \leq i \leq n : \tau(i) \neq i\}$. It sometimes helps to consider the complement of a set when we have to compute its cardinality. To more precisely define the complement of D_n we will define the following subsets of S_n: $F_n(k) = \{\tau \in S_n : \tau(k) = k\}$. We then have:

$$D_n = S_n \setminus \left(\bigcup_{k=1}^{n} F_n(k) \right)$$

For any given $k \in \{1, 2, \ldots, n\}$ we have $|F_n(k)| = (n-1)!$ (see footnote[2] why), so

$$\left| \left(\bigcup_{k=1}^{n} F_n(k) \right) \right| = n(n-1)! = n!$$

But this can't be right. It would mean that $|D_n| = 0$ and $D_n = \emptyset$. But cleary D_n is not empty, for example the permutation:

$$\rho(i) = \begin{cases} i+1 & i < n \\ 1 & i = n \end{cases}$$

is a member of D_n. The problem here is that the $F_n(k)$ are not disjoint, so calculating the size of their union needs to be done more carefully. It turns out that this is a perfect use case of the inclusion-exclusion principle.

The **inclusion-exclusion principle** provides a method of counting the size of the union of subsets that are not necessarily disjoint.

We illustrate the method on a simple example of three sets A, B, C as in Figure 1.1. We would like to compute $|A \cup B \cup C|$. The expression

[2] One position is fixed and the rest behave like a permutation in S_{n-1}.

$|A| + |B| + |C|$ would count the elements from $(A \cap B) \setminus (A \cap B \cap C)$, $(A \cap C) \setminus (A \cap B \cap C)$ and $(B \cap C) \setminus (A \cap B \cap C)$ twice and elements from $A \cap B \cap C$ three times. So $|A \cup B \cup C| < |A| + |B| + |C|$. To compensate we subtract the pairwise intersection sizes and our expression becomes $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$. This is almost right except for $A \cap B \cap C$ which we lost in the adjustment (it was counted three times and then subtracted three times). We add it back and get

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

In general, if we want to count $|\cup_{i=1}^{n} A_i|$ we start with $\sum_{i=1}^{n} |A_i|$ which includes pairwise intersections $A_i \cap A_j$ twice, so we exclude with $-(\sum_{1 \leq i < j \leq n} |A_i \cap A_j|)$. But this excludes the triple intersections so we include those with $\sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k|$. This overcounts quadruple intersections which we exclude etc. We stop with the exclusion or inclusion of the intersection of all A_i.

Figure 1.1: Union of three not necessarily disjoint sets.

Theorem 1.2. *Inclusion-exclusion principle.*
Given n sets A_j, $1 \leq j \leq n$

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{J \subseteq \mathbb{N}_n, \, |J|=k} \left| \bigcap_{j \in J} A_j \right| \right)$$

Proof. We are going to prove the theorem by tracing the contributions of one element $a \in \bigcup_{j=1}^{n} A_j$ to the left-hand side and right-hand side of the equation. On the left it will be 1 since this is the union of sets and not multisets. For the right-hand side, we observe that there is a non-empty index set $I \subseteq \{1, 2, \ldots, n\}$ such that $\forall i \in I : a \in A_i$. The element a will contribute ± 1 from all the set intersections in which it appears, so all the terms in the sum where index set J satisfies $J \subseteq I$ (since these are intersections, a won't appear in any of the other terms). The hope is that the sum of all these ± 1 will be 1.

Let $m = |I|$. Then any index set J with size greater than m cannot be a subset of I, so the running index k of the sum only needs to go to m. For each k there are $\binom{m}{k}$ index subsets J of size k from I. In each a weighs in with 1, so the contributions of a add up to:

$$\sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k}$$

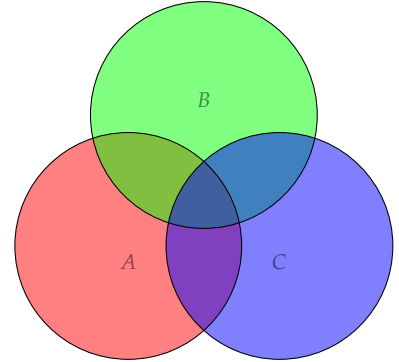We add and subtract $\binom{m}{0}$ to this sum and get

$$\sum_{k=1}^{m}(-1)^{k+1}\binom{m}{k} = \binom{m}{0} - \binom{m}{0} + \sum_{k=1}^{m}(-1)^{k+1}\binom{m}{k}$$

$$= \binom{m}{0} - \sum_{k=0}^{m}(-1)^{k+1}\binom{m}{k}$$

$$= \binom{m}{0} + \sum_{k=0}^{m}(-1)^{k}\binom{m}{k}$$

$$= \binom{m}{0} + \sum_{k=0}^{m}1^{m-k}(-1)^{k}\binom{m}{k}$$

$$= \binom{m}{0} + (1-1)^{m}$$

$$= \binom{m}{0} = 1$$

On both sides of the equation in the theorem an arbitrary element a of the union of the sets contributes 1. This proves the inclusion-exclusion principle. $\square$

Let us return to computing derangements. We now know how to compute $|(\bigcup_{k=1}^{n} F_n(k))|$ by using the inclusion-exclusion principle:

$$|(\bigcup_{k=1}^{n} F_n(k))| = \sum_{k=1}^{n}(-1)^{k+1}(\sum_{J \subseteq \mathbb{N}_n, |J|=k} |\bigcap_{j \in J} F_n(j)|)$$

For a given index set $J \subseteq \mathbb{N}_n$, $|J| = k$ the intersection contains all the permutations that are fixed in the positions $j \in J$, so the size of this intersection is $(n-k)!$. There are $\binom{n}{k}$ such index sets J of size k, so our expression becomes:

$$|(\bigcup_{k=1}^{n} F_n(k))| = \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}(n-k)!$$

We then have

$$!n = n! - \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}(n-k)!$$

$$= n! + \sum_{k=1}^{n}(-1)^{k}\binom{n}{k}(n-k)!$$

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

The probability of turning up identical cards from the two decks is

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

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

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

This probability converges fairly quickly to approximatively 0.7 so you have a 0.7 chance of turning up identical cards from the two decks.

Bibliography

M. Beck and R. Geoghegan. *The Art of Proof: Basic Training for Deeper Mathematics*. Undergraduate Texts in Mathematics. Springer New York, 2010. ISBN 9781441970237.