Math 155 (Lecture 18)

October 17, 2011

Let's begin this lecture with a familiar question:

Question 1. How many derangements are there of the set $\{1, 2, \ldots, n\}$?

Earlier in this course, we got an answer to Question 1 using the technique of generating functions. Let's try to obtain the same answer more directly. We first reformulate the question as follows: how many permutations of the set $\{1, 2, \ldots, n\}$ are not derangements? That is, how many permutations are there which have fixed points?

For $1 \leq i \leq n$, let S_i denote the subset of the symmetric group Σ_n consisting of permutations π having i as a fixed point: that is, permutations satisfying $\pi(i) = i$. Note that S_i can be identified with the set of all permutations of the set $\{1, \ldots, i-1, i+1, \ldots, n\}$ of size $n-1$, and therefore has cardinality $(n-1)!$. This leads to the following:

Incorrect Answer 2. The number of derangements of $\{1, \ldots, n\}$ is

$$|\Sigma_n - \bigcup_{1 \leq i \leq n} S_i| = n! - \sum_{1 \leq i \leq n} (n-1)! = n! - n! = 0.$$

Answer 2 is not correct because the sets S_i are not disjoint, so we cannot determine the size of the union $\bigcup_{1 \leq i \leq n} S_i$ simply by adding the sizes of the S_i individually. We therefore need to revisit one of our most basic principles:

Fact 3. *Let X and Y be disjoint finite sets. Then $|X \cup Y| = |X| + |Y|$.*

What happens if the sets X and Y are not disjoint? In this case, we always have a strict inequality

$$|X \cup Y| < |X| + |Y|.$$

This inequality results from the fact that elements of the intersection $X \cap Y$ are counted twice on the right hand side, but only once on the left hand side. We can correct for this by adding another term: we have

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Suppose now that we're given three sets X, Y, and Z. How many elements are there in the union $X \cup Y \cup Z$? The first guess

$$|X| + |Y| + |Z|$$

is generally wrong, because elements in the intersections between these sets get counted more than once. We can try to correct this by considering subtracting the sizes of the intersections, to obtain the number

$$|X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z|.$$

However, this is still not quite right. In this expression, an element of the intersection $X \cap Y \cap Z$ gets counted three times (because it belongs to X, Y, and Z) and then subtracted three times (since it belongs to each of the pairwise intersections), so does not contribute at all. To correct for this, we need to add yet another term. In general, the cardinality of the union $X \cup Y \cup Z$ is given by

$$|X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|.$$

Let's now describe the generalization to an arbitrary (finite) number of sets. Fix a finite set X, and suppose we are given subsets $X_1, X_2, \ldots, X_n \subseteq X$. For each subset $J \subseteq \{1, \ldots, n\}$, we let X_J denote the intersection $\bigcap_{i \in J} X_i$. We then have:

Theorem 4 (Inclusion-Exclusion Principle)**.** *Given subsets $X_1, \ldots, X_n \subseteq X$ as above, we have*

$$|X_1 \cup \ldots \cup X_n| = \sum_{\emptyset \neq J \subseteq \{1,\ldots,n\}} (-1)^{|J|+1} |X_J|.$$

We can make the formula look a little bit nicer by counting the size of the set $X - \bigcup_{1 \leq i \leq n} X_i$ instead of its complement. Note that if $J = \emptyset$, then $X_J = X$. We can therefore reformulate Theorem 4 as

Theorem 5.

$$|X - \bigcup_{1 \leq i \leq n} X_i| = \sum_{J \subseteq \{1,\ldots,n\}} (-1)^{|J|} |X_J|.$$

Proof. We can rewrite the right hand side as

$$\sum_{J \subseteq \{1,\ldots,n\}} \sum_{x \in X} \begin{cases} (-1)^{|J|} & \text{if } x \in X_J \\ 0 & \text{if } x \notin X_J. \end{cases}.$$

Rearranging the order of summation, this is given by

$$\sum_{x \in X} \sum_{J \subseteq \{1,\ldots,n\}} \begin{cases} (-1)^{|J|} & \text{if } x \in X_J \\ 0 & \text{if } x \notin X_J. \end{cases}.$$

Fix an element $x \in X$, and consider the sum

$$\sum_{J \subseteq \{1,\ldots,n\}} \begin{cases} (-1)^{|J|} & \text{if } x \in X_J \\ 0 & \text{if } x \notin X_J. \end{cases}.$$

Let $I = \{i \in \{1, \ldots, n\} : x \in X_i\}$. Then we can rewrite the last sum as

$$\sum_{J \subseteq I} (-1)^{|J|}.$$

If $I = \emptyset$, this sum has just one term (which is equal to 1). If I is nonempty, then it has $2^{|I|}$ terms, half of which are equal to 1 and half of which are equal to -1. We therefore obtain

$$\sum_{J \subseteq I} (-1)^{|J|} = \begin{cases} 1 & \text{if } I = \emptyset \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\begin{aligned} \sum_{x \in X} \sum_{J \subseteq \{1,\ldots,n\}} \begin{cases} (-1)^{|J|} & \text{if } x \in X_J \\ 0 & \text{if } x \notin X_J \end{cases} &= \sum_{x \in X} \begin{cases} 1 & \text{if } x \notin \bigcup_{1 \leq i \leq n} X_i \\ 0 & \text{otherwise} \end{cases} \\ &= |X - \bigcup_{1 \leq i \leq n} X_i| \end{aligned}$$

□

Let's now return to Question 1. We will take $X = \Sigma_n$ to be the set of all permutations of the set $\{1, \ldots, n\}$, and X_i to be the set of permutations π which fix the element i. Then $|X - \bigcup_{1 \leq i \leq n} X_i| = D_n$ is the number of derangements of the set $\{1, \ldots, n\}$. Using the inclusion-exclusion principle, we see that this is given by

$$D_n = \sum_{J \subseteq \{1, \ldots, n\}} (-1)^{|J|} |X_J|.$$

If $J \subseteq \{1, \ldots, n\}$ has cardinality k, then X_J can be identified with the set of all permutations of a set $\{1, \ldots n\} - J$ having $n - k$ elements. It follows that $|X_J| = (n-k)!$. It follows that the contribution coming from a set J depends only on the cardinality of J. There are exactly $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ subsets of $\{1, \ldots, n\}$ with k elements, so we can rewrite our sum as

$$D_n = \sum_{k \geq 0} (-1)^k \binom{n}{k} (n-k)! = \sum_{k \geq 0} (-1)^k \frac{n!}{k!} = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!}),$$

thereby recovering our earlier formula for D_n.

Let's see another application of the inclusion-exclusion principle.

Question 6. How many integers in the set $\{1, \ldots, n\}$ are relatively prime with n?

Remark 7. An equivalent formulation of Question 6 is the following: how many elements of the ring $\mathbf{Z}/n\mathbf{Z}$ are invertible?

The answer to Question 6 is often denoted by $\phi(n)$, and the function

$$n \mapsto \phi(n)$$

is called *Euler's ϕ-function.* To compute it, let S be the set of all prime divisors of n. Let $X = \{1, \ldots, n\}$, and for each $p \in S$ let $X_p = \{p, 2p, \ldots, n\}$ be the subset of X consisting of those numbers which are divisible by p. Then

$$\phi(n) = |X - \bigcup_{p \in S} X_p|.$$

Applying the inclusion-exclusion principle, we deduce that

$$\phi(n) = \sum_{J \subseteq S} (-1)^{|J|} |X_J|.$$

Note that if $J = \{p_1, \ldots, p_k\}$ is a set of prime numbers belonging to S, then X_J is just the subset of X consisting of integers that are divisible by the product $p_1 p_2 \ldots p_k$. It follows that

$$|X_J| = \frac{n}{p_1 \ldots p_k} = \frac{n}{\prod_{p \in J} p}.$$

We therefore obtain

$$\frac{\phi(n)}{n} = \sum_{J \subseteq S} \frac{(-1)^J}{\prod_{p \in J} p} = \sum_{J \subseteq S} \prod_{p \in J} \frac{-1}{p} = \sum_{J \subseteq S} \prod_{p \in S} \begin{cases} \frac{-1}{p} & \text{if } p \in J \\ 1 & \text{if } p \notin j. \end{cases}$$

Applying the distributive law, we get

$$\frac{\phi(n)}{n} = \prod_{p \in S} (1 - \frac{1}{p}) = \prod_{p \in S} \frac{p-1}{p}.$$

We can write this as

$$\phi(n) = n \prod_{p|n} \frac{p-1}{p}.$$

In other words, if n has the prime factorization $p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, then $\phi(n)$ is given by

$$(p_1 - 1)p_1^{k_1-1}(p_2 - 1)p_2^{k_2-1} \cdots .$$

Question 8. How many surjective maps are there from the set $\{1, \ldots, m\}$ to the set $\{1, \ldots, n\}$?

Let X be the set of all maps from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$. For $1 \leq i \leq n$, let $X_i \subseteq X$ be the subset consisting of those maps f for which $f^{-1}\{i\}$ is empty. Then

$$X - \bigcup_{1 \leq i \leq n} X_i$$

is the set of surjective maps from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$. Consequently, the answer to Question 8 is given by

$$|X - \bigcup_{1 \leq i \leq n} X_i| \quad = \quad \sum_{J \subseteq \{1, \ldots, n\}} (-1)^{|J|} |X_J|.$$

Note that for $J \subseteq \{1, \ldots, n\}$, X_J is the set of all maps from $\{1, \ldots, m\}$ into $\{1, \ldots, n\} - J$. If $|J| = k$, then there are exactly $(n-k)^m$ such maps. In particular, the summand

$$(-1)^{|J|} |X_J| = (-1)^k (n-k)^m$$

depends only on the size of J. We may therefore rewrite our answer as

$$\sum_{k \geq 0} \binom{n}{k} (-1)^k (n-k)^m$$

(here $\binom{n}{k}$ is the number of subsets of $\{1, \ldots, n\}$ of size k). Replacing k by $n-k$, we can rewrite this as

$$\sum_{k \geq 0} \binom{n}{k} (-1)^{n-k} k^m.$$