Discrete Mathematics lecture notes 10-1

November 11, 2013

27. Some applications of Inclusion-Exclusions

Last time we saw that for a collection of finite sets $A_1, A_2, \ldots, A_n$, we could compute the size of the union if we knew the size of each A_i individually along with the sizes of all intersections:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1} \left|\bigcap_{i=1}^{n} A_i\right|.$$

Let's use this to make a couple of interesting computations.

Euler's totient function. Euler's totient function $\phi : \mathbb{N}_{\ge 0} \to \mathbb{N}$ is defined by $\phi(n) = |\{1 \le i \le n | (i,n) = 1\}|$, i.e., $\phi(n)$ is the number of numbers less than n that are relatively prime to n. ϕ has a number of interesting algebraic properties; for now let's just come up with a closed-form formula for $\phi(n)$.

Let $[n]$ be the set $\{1, 2, \ldots, n\}$. $\phi(n)$ can be described the size of the set $D := \{i \in [n] | (i,n) - 1\}$. Instead of computing the size of this set directly, let's compute the size of the *complement* of D in $[n]$: $C = [n] \backslash D = \{j \in [n] | (j,n) \neq 1\}$. Clearly $|C| + |D| = |[n]| = n$, so determining $|C|$ will give us $|D|$ via the formula $|D| = n - |C|$.

For fixed n, let $p_1, \ldots, p_\ell$ be the distinct primes that divide n.[1] If $j \in C$, then $(j,n) \neq 1$, so in particular there must be some p_k such that $p_k | j$.[2] Thus, for $k = 1, 2, \ldots, \ell$, defining $C_k := \{j \in [n] | p_k | j\}$, it follows that $C = \bigcup_{k=1}^{\ell} C_k$, and we can hope to make use of Inclusion-Exclusion. We'll make use of a small technical lemma.

Lemma 1. *For $n \in \mathbb{N}_{\ge 1}$ and $d \in |\mathbb{N}$ a divisor of n, there are $\frac{n}{d}$ multiples of d that live in $[n]$.*

Proof. There is precisely one element of $[d] = \{1, 2, \ldots, d\}$ that is a multiple of d (namely d itself). As $d | n \neq 0$, we have $d \le n$ and hence $[d] \subseteq [n]$ contains exactly one element of $[n]$ that is a multiple of d. For each $j \in \{1, 2, \ldots, \frac{n}{d}\}$, let $di + [d]$ be the set $\{di + 1, di + 2, \ldots, di + d\}$: We obtain $di + [d]$ from $[d]$ by translating the elements of $[d]$ pointwise. Clearly the $\{di + [d]\}_{i=1}^{\frac{n}{d}}$ are distinct, and the assumption that $d | n$ implies that their union is all of $[n]$. Equally clearly,[3], each $di + [d]$ contains exactly one element that is a multiple of d, namely $di + d$. As there are a total of $\frac{n}{d}$ sets of the form $di + [d]$, the result follows. □

The effect of this lemma is that we calculate immediately for each prime p_k dividing n: $|C_k| = \frac{n}{p_k}$. But more is true: For $k, k' \in \{1, 2, \ldots, \ell\}$ distinct, we have $C_{k,k'} := C_k \cap C_{k'}$ is the set of elements of $[n]$ divisible by *both* p_k and $p_{k'}$. As p_k and $p_{k'}$ are prime, this set is equal to the elements of $[n]$ divisible by the product $p_k p_{k'}$.[4] Putting this all together, we have

$$\begin{aligned} |C| = \left|\bigcup_{k=1}^{\ell} C_k\right| &= \sum_{k=1}^{\ell} |C_k| - \sum_{1\le k<k'\le \ell} |C_{k,k'}| + - \ldots + (-1)^{\ell-1} \left|\bigcup_{k=1}^{\ell} C_k\right| \\ &= \sum_{k=1}^{\ell} \frac{n}{p_k} - \sum_{1\le k<k'\le \ell} \frac{n}{p_k p_{k'}} + - \ldots + (-1)^{\ell-1} \prod_{k=1}^{\ell} \frac{n}{p_k}, \end{aligned}$$

so

$$\phi(n) = |D| = n - |C| = n\left(1 - \sum_{k=1}^{\ell} \frac{n}{p_k} + \sum_{1\le k<k'\le \ell} \frac{1}{p_k p_{k'}} - + \ldots + (-1)^{\ell} \prod_{k=1}^{\ell} \frac{1}{p_k}\right) = n \cdot \prod_{k=1}^{\ell} \left(1 - \frac{1}{p_k}\right).$$

[1] Note that we're heavily relying on the fundamental theorem of arithmetic here.

[2] And even more heavily here.

[3] Prove it if not.

[4] You can prove–and should, if it's not clear!–using the fundamental theorem of arithmetic, or by looking at one of the problems on the first exam.

If the last equality is not obvious, you can prove it by induction or by mimicking the combinatorial proof of the binomial theorem.

Such is our answer:

$$\phi(n) = n \cdot \prod_{k=1}^{\ell} \left(1 - \frac{1}{p_k}\right),$$

which may not look like much at first. However, this solution is closed (i.e., it does not depend on an inductive or recursive calculation), so long as you know all the primes that divide n. Moreover, second term in the product does not depend on the number n itself, only on the distinct prime divisors of n. Thus 12 and 18 have the same second term, and their ϕ-values differ by the ratio of 12 to 18 directly. This observation has many implications in number theory.

Derangements. We begin with some notation that will play a major role in the last part of the course:

Definition 2. Let X be a set. The *symmetric group*[5] *of* X is the set $\Sigma_X := \{\sigma : X \to X | \sigma \text{ is a bijection}\}$, i.e., Σ_X is the set of bijective self-maps of X.

Similarly, for $n \in \mathbb{N}$, define $\Sigma_n := \Sigma_{[n]}$ to be the set of bijective selfmaps of the set $[n] = \{1, 2, \ldots, n\}$. This is often called the *symmetric group on* n *letters* or the *symmetric group of degree* n.

In either case, elements of the symmetric group are called *permutations*.

Exercise. Remind yourself why $|\Sigma_{[n]}| = n!$.

Exercise. Suppose that X and Y are sets and $f : X \xrightarrow{\sim} Y$ is a bijection. Use f to construct a bijection $\widetilde{f} : \Sigma_X \xrightarrow{\sim} \Sigma_Y$.

As a consequence of the previous exercise, we see that if $|X| = n$, then there is a bijection $\Sigma_X \xrightarrow{\sim} \Sigma_n$. As we adopt the view that *bijection* is the right notion of sets being "the same," this allows us to focus our attention on the collection of symmetric groups $\{\Sigma_n\}_{n\in\mathbb{N}}$ without losing any essential information about the symmetric groups of *finite* sets.[6] As we'll see in the next lecture, this convention also has the advantage of making it easier to describe the elements of Σ_n.

It was an easy exercise to compute the size of Σ_n, and knowledge of Inclusion-Exclusion was not really necessary. Let's consider a slightly harder problem that will.

Definition 3. Let X be a finite set of size n. A *derangement of* X is a permutation $\sigma \in \Sigma_X$ such that $\sigma(x) \neq x$ for all $x \in X$. In other words, σ is a derangement if it fixes[7] no element of X.

Denote the set of derangements of X by δ_X, and the derangements of Σ_n by δ_n.

Question: What is $|\delta_X|$? By our observation that we can replace Σ_X by Σ_n when $|X| = n$, we can simplify our question to ask: What is $|\delta_n|$ as a function of n?

To answer this question, let's define $\Phi_n \subseteq \Sigma_n$ to be the set of permutations that fix *at least one element*. Thus $\Sigma_n = \Phi_n \amalg \delta_n$, or $|\Sigma_n| = |\Phi_n| + |\delta_n|$. As the size fo the entire symmetric group is know, this allows us to state $|\delta_n| = n! - |\Phi_n|$, so we can compute $|\delta_n|$ by computing $|\Phi_n|$ first.

For each $i \in [n]$, set

$$F_i := \{\sigma \in \Sigma(n) | \sigma(i) = i\}.$$

That is, F_i is the set of permutations on n letters that fix the element i. Note that there are *no* requirements on what an element of F_i does to any other element: For $j \neq i$, we could have $\sigma(j) = j$ or $\sigma(j) \neq j$ and this would have no effect on whether $\sigma \in F_i$.

Let's also define, for $i \neq j$ two distinct elements of $[n]$, $F_{i,j} := F_i \cap F_j$. Thus $\sigma \in F_{i,j}$ if and only if $\sigma(i) = i$ and $\sigma(j) = j$. Similarly define $F_{i,j,k}$ for triples of distinct elements of $[n]$, etc.

[5] More on the meaning of this word soon.

[6] Symmetric groups of infinite sets are another matter entirely; we will not concern ourselves with them.

[7] I.e., sends an element to itself.

It is immediate that $\Phi_n = \bigcup_{i=1}^{n} F_i$, so

$$|\Phi_n| = \left|\bigcup_{i=1}^{n} F_i\right| = \sum_{i=1}^{n} |F_i| - \sum_{1\le i<j\le n} |F_{i,j}| + \sum_{1\le i<j<k\le n} |F_{i,j,k}| - + \ldots + (-1)^{n-1} \left|\bigcup_{i=1}^{n} F_i\right|.$$

Exercise. Show that $|F_i| = (n-1)!$, $|F_{i,j}| = (n-2)!$, $|F_{i,j,k}| = (n-3)!$, etc., for any choice of indices.

Using this exercise, and the fact that there are $\binom{n}{k}$ elements in the k summand of our expression for $|\Phi_n|$,[8] we fine

$$|\Phi_n| = \binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \binom{n}{3}(n-3)! - + \ldots + (-1)^{n-1}\binom{n}{n}(n-n)! = \sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)!$$

Using our formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, this becomes

$$|\Phi_n| = \sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!(n-k)!}\cdot(n-k)! = \sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!}.$$

Remembering now that we're really interested in $|\delta_n| = n! - |\Phi_n|$, we get

$$|\delta_n| = n! - \sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!} = n!\cdot\left(1 - \sum_{k=1}^{n}(-1)^{k-1}\frac{1}{k!}\right) = n!\cdot\sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

[8] Why?