Math 116 Professor: Padraic Bartlett

# Lecture 3: Inclusion-Exclusion

*Week 4* *UCSB 2015*

These notes are shorter than normal, because we used Monday's class to collectively re-evaluate the course!

## 1 Inclusion-Exclusion

A problem many of you have seen before is the following:

**Question 1.** *Suppose you have a finite set $X$, along with three subsets $A, B, C$ of $X$. Can you express the size of the set $X \setminus (A \cup B \cup C)$ in terms of the sizes of the sets $A, B, C, X$ and their intersections?*

**Answer.** This is relatively easy: we claim that

$$|X \setminus (A \cup B \cup C)| = |X| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|.$$

This is not too hard to see; take any $x \in X$, and consider the following two cases.

1. $x$ is not in $A \cup B \cup C$. In this case, then $x$ is "counted" once in the right sum: it contributes 1 to the $|X|$ count, and never shows up in any of the other terms, as it is not in any of $A, B, C$ or their intersections.

2. $x$ is in one of $A, B, C$, but not two of these sets. Then $x$ contributes 1 to the $|X|$ count, $-1$ to whichever of the sets $A, B, C$ $x$ is in, and never shows up in any of the other sets (as it is not in any of the intersections.) So $x$ contributes a 0 in total.

3. $x$ is in two of $A, B, C$, but not all three of these sets. Then $x$ contributes 1 to the $|X|$ count, $2 \cdot (-1)$ from the two sets $A, B, C$ that $x$ is in, a 1 from whichever pairwise intersection $x$ is in, and never shows up in any of the other two intersections or the three-way intersection. So $x$ contributes a 0 in total again!

4. Finally, $x$ could be in all of $A, B, C$. Then $x$ contributes a 1 to the $|X|$ count, $3 \cdot (-1)$ from the three $|A|, |B|, |C|$ counts, $3 \cdot (+1)$ from the three pairwise intersections $|A \cap B|, |A \cap C|, |B \cap C|$, and $-1$ from the $|A \cap B \cap C|$ term. Again, this $x$ contributes a 0 in total.

So, the right hand sum adds up a 1 for every $x \in X \setminus (A \cup B \cup C)$ and a 0 for every other $x$; in other words, the right hand side gives us the size of $X \setminus (A \cup B \cup C)$, as claimed!

We can generalize this as follows:

**Question 2.** *Suppose you have a finite set $X$, along with $n$ subsets $A_1, A_2, \ldots A_n$ of $X$. Can you express the size of the set $X \setminus (A_1 \cup A_2 \cup \ldots \cup A_n)$ in terms of the sizes of the sets $X, A_1, \ldots A_n$ and their intersections?*

**Answer.** We do this with the same methods as above, once we build up some notation. First, for any $k$, let the sum

$$\sum_{1\leq i_1<i_2<\ldots<i_k\leq n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|$$

denote the sum over all sets of $k$ integers $i_1 < \ldots < i_k$ of the size $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|$.

This way to index a sum may look odd, but it's describing fairly intuitive; what it's trying to capture is "let's count all of the $k$-size subsets of $\{A_1, \ldots A_n\}$ exactly once." For instance, let's consider what happens for $n = 4, k = 2$; then our sum is

$$\sum_{1\leq i_1<i_2\leq 4} |A_{i_1} \cap A_{i_2}| = |A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4|.$$

Similarly, if $n = 5, k = 4$, then our sum is

$$\begin{aligned}\sum_{1\leq i_1<i_2<i_3<i_4\leq 5} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| =&|A_1 \cap A_2 \cap A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3 \cap A_5| \\ &+|A_1 \cap A_2 \cap A_4 \cap A_5| + |A_1 \cap A_3 \cap A_4 \cap A_5| \\ &+|A_2 \cap A_3 \cap A_4 \cap A_5|.\end{aligned}$$

With this said, I claim that our result from our earlier question generalizes as follows:

$$\left|X \setminus \left(\bigcup_{k=1}^{n} A_k\right)\right| = |X| + \sum_{k=1}^{n} \left((-1)^k \cdot \sum_{1\leq i_1<\ldots<i_k\leq n} |A_{i_1} \cap \ldots \cap A_{i_k}|\right),$$

or, if we expand the sum at right,

$$\begin{aligned}\left|X \setminus \left(\bigcup_{k=1}^{n} A_k\right)\right| = |X| &- \left(\sum_{1\leq i_1\leq n} |A_{i_1}|\right) + \left(\sum_{1\leq i_1<i_2\leq n} |A_{i_1} \cap A_{i_2}|\right) \\ &- \left(\sum_{1\leq i_1<i_2<i_3\leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|\right) + \left(\sum_{1\leq i_1<i_2<i_3<i_4\leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}|\right) \\ &- \ldots\end{aligned}$$

Our proof goes in a similar fashion to before:

1. $x$ is not in $\bigcup_{k=1}^{n} A_k$. In this case, then $x$ is "counted" once in the right sum: it contributes 1 to the $|X|$ count, and never shows up in any of the other terms, as it is not in any of $A, B, C$ or their intersections.

2. $x$ is in $l$ of the $A_i$ sets: to be specific, let's say that $x \in A_{i_1}, \ldots A_{i_l}$ for some indices $i_1 < \ldots < i_l$, and that $x$ is not in any of the other $A_j$ sets.

   In this setting, then $x$ shows up in the following:

- $x$ contributes a 1 to the $|X|$ term's size.
- $x$ is in $l$ of the $A_i$ terms, and thus contributes $(-1) \cdot l$ from the $\sum_{1 \leq i_1 \leq n} |A_{i_1}|$ terms.
- $x$ is in $\binom{l}{2}$ of the $A_i \cap A_j$ terms, because it's in $l$ sets total and there are $\binom{l}{2}$ many ways to pick out pairs of these sets to intersect. Therefore, it contributes $(+1) \cdot \binom{l}{2}$ from the $\sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}|$ terms.
- Similarly, $x$ is in $\binom{l}{3}$ of the $A_i \cap A_j \cap A_k$ terms, because it's in $l$ sets total and there are $\binom{l}{3}$ many ways to pick out triples of these sets to intersect. Therefore, it contributes $(-1) \cdot \binom{l}{3}$ from the $\sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|$ terms.
- ...
- In general, for any $k \leq l$, $x$ is in $\binom{l}{k}$ of the $A_{i_1} \cap \ldots \cap A_{i_k}$ terms, as it is in $l$ sets total and there are $\binom{l}{k}$ many ways to pick out $k$ sets from the $l$ sets in total. Therefore, in total, it contributes $(-1)^k \cdot \binom{l}{k}$ from the $(-1)^k \cdot \sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}|$ terms.

So, in total, $x$ contributes

$$1 - l + \binom{l}{2} - \binom{l}{3} + \ldots + (-1)^k \binom{l}{k}$$
$$= \sum_{k=0}^{l} \binom{l}{k} (-1)^k$$

to the right-hand side.

If we remember the binomial theorem, which says that $(x+y)^l = \sum_{k=0}^{l} \binom{l}{k} x^k y^{l-k}$, and plug in $x = -1, y = 1$, we get

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

But $(-1+1)^l = 0$; so we actually have that $x$ contributes 0 to the sum!

So, our sum adds up a 1 for every $x \in X \setminus (\bigcup_{k=1}^{n} A_k)$ and a 0 for every other $x$; in other words, the right hand side gives us the size of $X \setminus (\bigcup_{k=1}^{n} A_k)$, as claimed!

Roughly speaking, our strategy here was the following:

- To find the size of the union of a bunch of sets, we first added up the size of all of these sets; this overcounts, however, because elements in more than one set get counted multiple times!

- To correct for this overcount, we then "fix" things by subtracting off the size of all of our pairwise intersections. But this results in an undercount, as elements in more than two sets get counted by these pairwise intersections too many times!
- To correct for **this** undercount, we then add in the size of all of our triple-intersections; but this too results in an overcount ...
- But if we keep doing this, at the end we will have (magically) counted everything correctly!

This idea is an incredibly useful one — to get an exact count, we can just use "at least" counts and repeatedly add and subtract off errors to get the right result at the end! It also should sound familiar, because this is basically exactly why we invented the sieve method!

In fact, we can use sieves to answer our problem above efficiently:

**Answer.** Let

- $\Omega =$ a set $X$,
- $A_1, \ldots A_n$ be a collection of subsets of $X$, and
- $P = \{P_1, \ldots P_n\}$, where an element $x \in X$ satisfies property $p_i$ if and only if $x \in A_i$.

For any $S \subset P$, let $A(S)$ denote the number of elements of $X$ that satisfy all of the properties of $S$ (and perhaps others.) Then, if $S = \{p_{i_1}, \ldots p_{i_k}\}$, we have that

$$A(S) = |A_{i_1} \cap \ldots \cap A_{i_k}|,$$

as saying that an element satisfies $p_{i_1}, \ldots p_{i_k}$ just means that it's in every one of the sets $A_{i_1} \cap \ldots \cap A_{i_k}$.

In the last week's notes, we defined

$$n_r = \sum_{|S|=r} A(S), \qquad N(x) = \sum_{r=0}^{\infty} n_r x^r,$$

and showed that if

$$e_t = \text{number of elements with } t \text{ elements}, \qquad E(x) = \sum_{t=0}^{\infty} e_t x^t,$$

then $N(x-1) = E(x)$.

In our problem above, we were interested in the size of the set $X \setminus (A_1 \cup A_2 \cup \ldots \cup A_n)$; in other words, we wanted the number of elements in $X$ that have precisely 0 properties, as these are all of the elements in $X$ that are not in any of the $A_i$'s!

On one hand, we know that $e_0$ is this quantity by definition. On the other, we know that $e_0 = E(0)$ because plugging in 0 to any power series kills off all of its non-constant terms and leaves only the constant term; therefore, because $E(0) = N(-1)$, we can use the fact that for any $1 \leq r \leq n$, we have

$$n_r = \sum_{S \subseteq P, |S|=r} A(S) = \sum_{1 \leq i_1 < \ldots < i_r \leq n} |A_{i_1} \cap \ldots \cap A_{i_r}|,$$

while $n_0 = |X|$ (because every element has at least no properties) and $n_r = 0$ for $r > n$ (because it is impossible to have more than $n$ properties.)

Therefore,

$$N(x) = |X| + \sum_{r=1}^{n} x^r \left( \sum_{1 \le i_1 < \ldots < i_r \le n} |A_{i_1} \cap \ldots \cap A_{i_r}| \right)$$

and therefore that

$$e_0 = E(0) = N(-1) = |X| + \sum_{r=1}^{n} (-1)^r \left( \sum_{1 \le i_1 < \ldots < i_r \le n} |A_{i_1} \cap \ldots \cap A_{i_r}| \right).$$

This is our answer from before; however, unlike before we didn't have to do any clever counting tricks! This is the power of generating functions; there are methods here that "automagically" perform tricks that otherwise require lots of cleverness!

We give a second example of the use of sieves to answer inclusion-exclusion flavored problems here:

**Question 3.** *For any two natural numbers $n, d$, we say that $n$ and $d$ are **relatively prime** if gcd$(n, d) = 1$; that is, if $n, d$ have no common factors.*

*For any $n \in \mathbb{N}$, let $\varphi(n)$ denote the **Euler phi function** that sends $n$ to the number of positive integers $d$ such that $d$ is relatively prime to $n$. For example, $\varphi(6) = 2$, as $\{1, 5\}$ are the two numbers in $\{1, 2, 3, 4, 5, 6\}$ that are relatively prime to 6. Similarly, $\varphi(p) = p - 1$ for any prime $p$, as no number less than $p$ has a nontrivial factor in common with $p$.*

*What is a nice formula for $\varphi(n)$ in terms of $n$?*

**Answer.** We answer this with sieves. Write $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$, for distinct prime numbers $p_1, \ldots p_l$. Set

- $\Omega = \{1, 2, \ldots n\}$, and
- $P = \{\rho_1, \ldots \rho_n\}$, where an element $d$ satisfies property $\rho_i$ if and only if $p_i$ is a factor of $d$.

As before, we are interested in the number of elements in $\{1, \ldots n\}$ with **no** properties, as an element has no properties if and only if it has no factors in common with $n$ — that is, if it is relatively prime to $n$.

Again, we start by calculating $A(S)$; I claim that if $S = \{\rho_{i_1}, \ldots \rho_{i_k}\}$, we have that

$$A(S) = \frac{n}{p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_k}}.$$

This is because satisfying a property $\rho_i$ is the same thing as being a multiple of $p_i$; therefore, the number of things that satisfy properties $\{\rho_{i_1}, \ldots \rho_{i_k}\}$ is just the collection of all multiples of $p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_k}$. There are precisely $\frac{n}{p_{i_1} \cdot p_{i_k}}$ of these elements in $\{1, 2, \ldots n\}$ (think about this if you don't see why,) which justifies our claim!

Therefore, we have that for any $1 \leq r \leq n$, we have

$$n_r = \sum_{S \subseteq P, |S|=r} A(S) = \sum_{\{\rho_{i_1}, \ldots \rho_{i_r}\} \subseteq P} \frac{n}{p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_k}},$$

while $n_0 = n$ (because every element has at least no properties) and $n_r = 0$ for $r > n$ (because it is impossible to have more than $n$ properties.)

Therefore,

$$N(x) = n + \sum_{r=1}^{n} x^r \left( \sum_{\{\rho_{i_1}, \ldots \rho_{i_r}\} \subseteq P} \frac{n}{p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_k}} \right),$$

and therefore that

$$e_0 = E(0) = N(-1) = n + \sum_{r=1}^{n} (-1)^r \left( \sum_{\{\rho_{i_1}, \ldots \rho_{i_r}\} \subseteq P} \frac{n}{p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_k}} \right).$$

Some clever factoring on the right hand side gives us

$$\begin{aligned} & n + \sum_{r=1}^{n} (-1)^r \left( \sum_{\{\rho_{i_1}, \ldots \rho_{i_r}\} \subseteq P} \frac{n}{p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_k}} \right) \\ =& n \left( 1 - \left( \sum_{1 \leq i_1 \leq n} \frac{n}{p_i} \right) + \left( \sum_{1 \leq i_1 < i_2 \leq n} \frac{n}{p_{i_1} p_{i_2}} \right) - \left( \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} \right) + \ldots \right) \\ =& n \cdot \prod_{i=1}^{n} \left( 1 - \frac{1}{p_i} \right). \end{aligned}$$

In other words, we've proven that for any $n$, the Euler $\varphi$-function has the closed form

$$\varphi(n) = n \cdot \prod_{i=1}^{n} \left( 1 - \frac{1}{p_i} \right).$$

Cool!

To test it out, let's try finding $\varphi(35)$. On one hand, we can see that

$$\begin{aligned} \varphi(35) &= 35 \cdot \left( 1 - \frac{1}{5} \right) \left( 1 - \frac{1}{7} \right) \\ &= 35 \cdot \frac{4}{5} \cdot \frac{6}{7} \\ &= 24. \end{aligned}$$

On the other hand, we can just list all of the numbers from 1 to 35 and strike out all of the ones that have factors in common with 35:

1, 2, 3, 4, ~~5~~, 6, ~~7~~, 8, 9, ~~10~~, 11, 12, 13, ~~14~~, ~~15~~, 16, 17, 18, 19,
~~20~~, ~~21~~, 22, 23, 24, ~~25~~, 26, 27, ~~28~~, 29, ~~30~~, 31, 32, 33, 34, ~~35~~

There are 24 numbers left over, as claimed!