Z. Abel, B. Chapman, E. Demaine

Lecture 17: More Counting

(If notation is unfamiliar, see Appendix!)

1 Inclusion/Exclusion

Recall the Sum Rule: $|A \cup B| = |A| + |B|$ **if** A, B are disjoint. What if they're not?!

How many queens and/or hearts are in a standard deck of cards?
$4\text{Q} + 13\heartsuit = 17$ cards? But then Q$\heartsuit$ would be counted twice! Instead: $4 + 13 - 1 = 16$.

In general, $|A \cup B| = |A| + |B| - |A \cap B|$. Easier to see using a Venn Diagram (draw picture).

Similar formula for 3 sets:

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

Application: Let $n = pqr$, product of 3 different primes. How many numbers in $\{1, 2, \ldots, n\}$ are relatively prime to n?

How many aren't? Let A_p be the set of numbers in $\{1, 2, \ldots, n\}$ that are divisible by p, same for A_q and A_r. Our answer is $n - |A_p \cup A_q \cup A_r|$.

Inc exc: $|A_p| = n/p$ and same for q, r, $|A_p \cap A_q| = n/(pq)$ and same for other pairwise intersections, and $|A_p \cap A_q \cap A_r| = n/(pqr) = 1$. Formula gives

$$\begin{aligned}
|A_p \cup A_q \cup A_r| &= |A_p| + |A_q| + |A_r| - |A_p \cap A_q| - |A_p \cap A_r| - |A_q \cap A_r| + |A_p \cap A_q \cap A_r| \\
&= n/p + n/q + n/r - n/(pq) - n/(pr) - n/(qr) + n/(pqr) \\
&= qr + pr + qp - r - q - p + 1 \\
&= pqr - (pqr - qr - pr - qp + r + q + p - 1) \\
&= n - (p-1)(q-1)(r-1).
\end{aligned}$$

so answer is n minus that! Simplifies to $(p-1)(q-1)(r-1)$.

Even more generally:

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots \cup A_n| = &\sum_i |A_i| \\ &- \sum_{i<j} |A_i \cap A_j| \\ &+ \sum_{i<j<k} |A_i \cap A_j \cap A_k| \\ &\cdots \\ &\pm |A_1 \cap A_2 \cap \cdots \cap A_n|.\end{aligned}$$

Add the initial sets, subtract the 2-way intersections, add the 3-way intersections, subtract 4-way intersections, etc., all the way to the n-way intersection.

Can also be expressed as follows:

Theorem 1 (PIE)**.** *Let $\mathcal{U} = \bigcup_{i \in [n]} A_i$ be a finite universe of discourse. Then*

$$\sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| = 0,$$

where $\bigcap \emptyset = \mathcal{U}$ by convention.

Proof. For $x \in \mathcal{U}$, let $I_x \subseteq [n]$ be the set of indices i for which $x \in A_i$. For every $I \subseteq I_x$, $x \in \bigcap_{i \in I} A_i$. This means x contributes $+1$ to the LHS for each such I of even size, and x contributes -1 to the LHS for each such I of odd size. I_x is non-empty by definition of $\mathcal{U}$, so contains some index i. Now symmetric difference with $\{i\}$ gives a self-inverting bijection between even-size and odd-size subsets $I \subseteq I_x$, so x contributes 0 in total to the LHS. □

Example: If we take $n = 2$ and expand out the LHS, this is saying that

$$\overset{I=\emptyset}{(-1)^0 \cdot |\mathcal{U}|} \ + \ \overset{I=\{1\}}{(-1)^1 \cdot |A_1|} \ + \ \overset{I=\{2\}}{(-1)^1 \cdot |A_2|} \ + \ \overset{I=\{1,2\}}{(-1)^2 \cdot |A_1 \cap A_2|} \ = \ 0.$$

Example: If we take $n = 3$ and expand out the LHS, this is saying that

$$\overset{I=\emptyset}{|\mathcal{U}|} - \overset{I=\{1\}}{|A_1|} - \overset{I=\{2\}}{|A_2|} - \overset{I=\{3\}}{|A_3|} + \overset{I=\{1,2\}}{|A_1 \cap A_2|} + \overset{I=\{1,3\}}{|A_1 \cap A_3|} + \overset{I=\{2,3\}}{|A_2 \cap A_3|} - \overset{I=\{1,2,3\}}{|A_1 \cap A_2 \cap A_3|} = 0.$$

2 Pidgeyhole Principle

Theorem 2 (Pidgeyhole Principle)**.** *If $|A| > |B|$, and $f : A \to B$ is a total function, then f is not injective. In other words, there exist $a_1, a_2 \in A$ such that $a_1 \neq a_2$ and $f(a_1) = f(a_2)$.*

More generally, any total relation $R \subseteq A \times B$ is not injective: there must exist at least two distinct $a_1, a_2 \in A$ that relate to the same $b \in B$.

Name comes from medieval times: cubbies for domestic pigeons to rest in. A is pigeons, B is pigeonholes. If more birds than cubbies, then some pigeons must share.

Example: strictly more than 26 people in the room, so two of us must have names that start with the same first letter.

Example: n differently colored pairs of socks; how many single socks do I need to pick before I'm guaranteed to have a matching pair? Pidgeyhole Principle says $n + 1$ is enough. And can't be less, because I might accidentally pick one from each pair. So $n + 1$ is the exact answer.

Example: there exist two non-bald Bostonians ($\approx 650,000$) with the same number of hairs on their head ($\leq 200,000$). Assuming less than 2/3 of Boston is bald, we have more Bostonians than possible hair counts, so must be true by Pidgeyhole.

Note: **nonconstructive**! We know they exist, but we don't know who! Pidgeyhole Principle says there must be a collision, but doesn't give an easy way to actually find the people.

Example: no lossless compression scheme that strictly shortens all n-bit strings. There are 2^n bitstrings with length n, but only $2^{n-1} + 2^{n-2} + \cdots + 2^1 + 2^0 = 2^n - 1$ shorter strings (including the empty string). Any total function from bigger set to smaller set must have collisions, so it's not lossless.

Theorem 3 (Generalized Pidgeyhole Principle)**.** *If* $|A| > k \cdot |B|$*, then every total relation/function from* A *to* B *must have at least* $k + 1$ *elements in* A *that map to the same element in* B*.*

With either version, proofs are often short but can sometimes require cleverness! Gotta pick your pigeons, holes, and/or the map between them carefully; not all choices are useful.

One more example: on an 8×8 chessboard, we fill 33 of the 64 cells with Rooks. Show we can find 5 of them that don't attack each other, i.e., lie in 5 distinct rows *and* 5 distinct columns.

Clever idea: Choose 8 pigeonholes, where each one is a subset of 8 cells like this:

2	3	4	5	6	7	8	1
3	4	5	6	7	8	1	2
4	5	6	7	8	1	2	3
5	6	7	8	1	2	3	4
6	7	8	1	2	3	4	5
7	8	1	2	3	4	5	6
8	1	2	3	4	5	6	7
1	2	3	4	5	6	7	8

Label each rook with the number on its cell. There are 8 labels and 33 rooks, so at least 5 of them must have the same label. These 5 are in different rows and columns; done!

3 Combinatorial Proofs / Double Counting

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Proof. How many subsets of $\{1, 2, \ldots, n\}$ are there?

Idea: For each $0 \leq k \leq n$ there are $\binom{n}{k}$ subsets of size k, so together these should add to the total number of subsets, 2^n.

More precisely: Let S be the set of all subsets of $\{1, 2, \ldots, n\}$. We will count $|S|$ in two different ways.

First, $|S| = 2^n$ since each element is either in or out.

Let's instead work by cases, depending on the size of the subsets. Let S_k be the set of subsets of size k, and note that $S_0, S_1, \ldots, S_n$ form a ***partition*** of S: every member of S belongs to exactly one of the S_k. By the sum rule, this means $|S| = \sum_{k=0}^{n} |S_k|$. But $|S_k| = \binom{n}{k}$, so we get $2^n = |S| = \sum \binom{n}{k}$, as claimed. □

This is a special case of a useful theorem. We've been using binomial coefficients a lot already; here's their eponym:

Theorem 4 (Binomial Theorem)**.** *For any x, y, and for $n \in \mathbb{N}$:*

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k},$$

where $0^0 = 1$ by convention.

Proof. Expand $(x + y)^n$ to get a sum of 2^n terms of the form $a_1 a_2 \cdots a_n$, where a_i are either x or y. By commutativity, we can group like terms of the form $x^k y^{n-k}$. There are $\binom{n}{k}$ such terms; this is the number of ways we can choose k of the n indices i for which $a_i = x$. □

Example: If $n = 3$, we have $(x + y)^3 = y^3 + 3xy^2 + 3x^2y + x^3$.
The coefficient of $(x^0)y^3$ is $\binom{3}{0} = 1$.

The coefficient of xy^2 is $\binom{3}{1} = 3$.

The coefficient of x^2y is $\binom{3}{2} = 3$.

The coefficient of $x^3(y^0)$ is $\binom{3}{3} = 1$.

Similarly:

Theorem 5 (Multinomial Theorem). *For any $x_1, x_2, \ldots, x_m$, and for $n \in \mathbb{N}$:*

$$\left(\sum_{i=1}^{m} x_i\right)^n = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} \prod_{i=1}^{m} x_i^{k_i}.$$

As before, $0^0 = 1$ by convention, and the summation is over non-negative integers k_i that sum to n. $\binom{n}{k_1, k_2, \ldots, k_m}$ is the multinomial coefficient *defined by*

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1! k_2! \cdots k_m!}.$$

Another useful identity:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Could prove this by algebra using factorials, but no intuition! Here's a combinatorial proof:

Proof. How many subset of $\{1, 2, \ldots, n\}$ have size k? Let S be this set of size-k subsets. Then $|S| = \binom{n}{k}$. But let's count these in a different way. Every size-k subset of $\{1, 2, \ldots, n\}$ either includes n or doesn't. Let A be the set of ones that include n, and B the set of ones that don't, so S is the disjoint union of A and B.

Note: $|B| = \binom{n-1}{k}$, because we're not allowed to use n. Also, $|A| = \binom{n-1}{k-1}$, because we must pick n, and then $k-1$ other numbers from $\{1, \ldots, n-1\}$. So $|S| = |A| + |B|$, which is exactly the identity above. □

Note: this fact shows that if we put the numbers $\binom{n}{k}$ in a big triangle, each is the sum of the 2 above it. This is Pascal's Triangle. Above we showed that the sum of row k is 2^k, and in homework you'll show that the sums of diagonals gives Fibonacci Numbers!

Fun exercise: Find a combinatorial proof that

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

Appendix: Notation

Just as $\sum_{i=1}^{n} x_i := x_1 + x_2 + \ldots + x_n$, we can similarly define n-way products, unions, and intersections:

$$\prod_{i=1}^{n} x_i := x_1 \times x_2 \times \ldots \times x_n$$

$$\bigcup_{i=1}^{n} S_i := S_1 \cup S_2 \cup \ldots \cup S_n$$

$$\bigcap_{i=1}^{n} S_i := S_1 \cap S_2 \cap \ldots \cap S_n$$

There are also different notations for indexing:

$$[n] := \mathbb{N} \cap (0, n] = \{1, 2, \ldots, n\}$$

$\sum_{i \in [n]} x_i$ is another way to write $\sum_{i=1}^{n} x_i$.

More generally, for a finite *indexing set* S, $\sum_{x \in S} f(x)$ means $\sum_{i=1}^{|S|} f(\phi(i))$, where $\phi : [|S|] \to S$ is any bijection.

A common abuse of notation is to write $\sum_{P(x)} f(x)$ instead of $\sum_{x \in \{y : P(y)\}} f(x)$.

One can even omit the index entirely: $\sum S$ means $\sum_{x \in S} x$.

All of these notations extend naturally to $\prod$, $\bigcup$, $\bigcap$.

$\sum \emptyset = 0$ by convention, because 0 is the *identity* of $+$. Basically, it should be true that $\sum_{i=1}^{m} x_i + \sum_{i=m+1}^{n} x_i = \sum_{i=1}^{n} x_i$. Taking $m = 0$ tells us $\sum_{i=1}^{0} x_i = \sum \emptyset = 0$.

Similarly, for $\prod$ we have $\prod \emptyset = 1$, and $\bigcup \emptyset = \emptyset$, and $\bigcap \emptyset = \mathcal{U}$, where $\mathcal{U}$ is the universe of discourse, or "everything".