CS/Math 240: Introduction to Discrete Mathematics 5/5/2011

Lecture 27 : Combinatorial Arguments

Instructor: Dieter van Melkebeek Scribe: Dalibor Zelený

DRAFT

Last time we continued our discussion of counting. In general, this is a problem in which we are given a description of a finite set, and our goal is to find the set's cardinality. Last time we discussed some more examples and also the inclusion-exclusion principle which is a generalization of the sum rule from two lectures ago.

Today we give another example of the inclusion-exclusion principle. After that, we discuss the pigeonhole principle. The pigeonhole principle is not a counting technique. It allows us to prove that some events happen, but does not provide any more details about how they occur. Our last topic (today and in this course) will be combinatorial arguments. The idea behind those is that we can often count a set in multiple ways, and viewing it in different ways yields some identities and inequalities between mathematical objects.

27.1 Inclusion-Exclusion Continued

Recall that the inclusion-exclusion formula is a generalization of the sum rule. We have sets S_1 through S_s, and want to find the cardinality of their union as a function of cardinalities of other sets. In particular, we have the following identity.

$$\begin{aligned}\left|\bigcup_{i=1}^{s} S_i\right| &= \sum_{0\neq I\subseteq[s]} (-1)^{|I|+1} \left|\bigcap_{i\in I} S_i\right| \\ &= \sum_{i=1}^{s} |S_i| - \sum_{1\leq i<j\leq s} |S_i \cap S_j| + \sum_{1\leq i<j<k\leq s} |S_i\cap S_j\cap S_k| - \cdots + (-1)^{s+1} |S_1 \cap \cdots \cap S_s|\end{aligned}$$

Let's see an example. We would like to count the primes less than or equal to 100. One way to do it would be two write down all numbers between 2 and 100 and cross out nontrivial multiples of each number. The numbers that are left are primes. This algorithm is known as the *sieve of Eratosthenes*. It works fairly well for small sets of primes, but gets too complex for larger sets. We use the inclusion-exclusion formula to count the primes.

Example 27.1: Instead of counting the primes, we count integers that are at most 100 and are nontrivial multiples of other integers $k > 2$. Let M'_k be the set of multiples of k that are less than 100. That is $M'_2 = \{2, 4, 6, \ldots, 98, 100\}$, $M'_3 = \{3, 6, 9, \ldots, 96, 99\}$, and so on.

We claim that every non-prime less than 100 is divisible by a prime less than $\sqrt{100}$. We can prove this by contradiction. Every non-prime number n has two (possibly equal) prime factors. If both of them are more than $\sqrt{100} = 10$, we would have $n > 10 \cdot 10 = 100$, so n would not be an integer that's at most 100.

The previous paragraph implies that each non-prime that's at most 100 has one of the primes 2, 3, 5, 7 as a divisor. Hence, if we count the nontrivial multiples of these four primes that are at most 100 and subtract them from the total number of integers between 2 and 100, we get the number of primes between 2 and 100.

The nontrivial multiples of our four primes live in the sets M'_2, M'_3, M'_5 and M'_7. Then they live in their union. The union of those sets also contains our four primes, so after we find $|M'_2 \cup M'_3 \cup M'_5 \cup M'_7|$, we need to subtract 4 from that number to get the number of non-primes between 2 and 100. We use the inclusion-exclusion formula to count the number of elements in the union.

$$\begin{aligned}|M'_2 \cup M'_3 \cup M'_5 \cup M'_7| = {} & |M'_2| + |M'_3| + |M'_5| + |M'_7| - \\ & - |M'_2 \cap M'_3| - |M'_2 \cap M'_5| - |M'_2 \cap M'_7| - |M'_3 \cap M'_5| - |M'_3 \cap M'_7| - |M'_5 \cap M'_7| + \\ & + |M'_2 \cap M'_3 \cap M'_5| + |M'_2 \cap M'_3 \cap M'_7| + |M'_2 \cap M'_5 \cap M'_7| + |M'_3 \cap M'_5 \cap M'_7| - \\ & - |M'_2 \cap M'_3 \cap M'_5 \cap M'_7|.\end{aligned}$$

We have shown some facts about sets related to our sets M'_k on the previous homework. In particular, M_k was the set of all multiples of k, and if p and q are two different primes, we showed that $M_p \cap M_q = M_{pq}$ This fact transfers to our "primed" versions of the sets, i.e., we have $M'_p \cap M'_q = M'_{pq}$ for any primes p and q. In fact, this generalizes even more. For any set of distinct primes $p_1, p_2, \ldots, p_r$, we have $M'_{p_1} \cap M'_{P_2} \cap \cdots \cap M'_{p_r} = M_{p_1 p_2 \cdots p_r}$. Hence, we can rewrite our expression for $|M'_2 \cup M'_3 \cup M'_5 \cup M'_7|$ as follows.

$$\begin{aligned}|M'_2 \cup M'_3 \cup M'_5 \cup M'_7| = {} & |M'_2| + |M'_3| + |M'_5| + |M'_7| - \\ & - |M'_6| - |M'_{10}| - |M'_{14}| - |M'_{15}| - |M'_{21}| - |M'_{35}| + \\ & + |M'_{30}| + |M'_{42}| + |M'_{70}| + |M'_{105}| - \\ & - |M'_{210}|.\end{aligned}$$

The last two sets in the expression above are actually empty. There are no multiples of 105 or 210 that are at most 100. In general, the largest multiple of k that belongs to M'_k is $\lfloor 100/k \rfloor$, and we can use this to find the number of integers that are at most 100 and are multiples of at least one of our primes.

$$\begin{aligned}|M'_2 \cup M'_3 \cup M'_5 \cup M'_7| & = 50 + 33 + 20 + 14 - \\ & \quad - 16 - 10 - 7 - 6 - 4 - 2 + \\ & \quad + 3 + 2 + 1 + 0 - \\ & \quad - 0 \\ & = 78.\end{aligned}$$

We need to subtract 4 from this number because M' contains four primes. It follows that there are 74 integers between 2 and 100 that are not primes, so there are $99 - 74 = 25$ primes between 2 and 100. ⊠

The example we just worked out seemed to be a lot of work. Indeed, for primes up to 100, carrying out the sieve of Eratosthenes could be a faster way. However, for finding the number of primes up to n for a large n, it would be faster to use our inclusion-exclusion strategy because just writing down all integers from 2 to n would take a long time. What makes inclusion-exclusion appealing for this is that we can characterize all the intersections that arise during the computation. This saves a considerable amount of work.

27.2 Pigeonhole Principle

The pigeonhole principle is not a counting technique, but it is a powerful tool, so it deserves mentioning now. It often gets used after we find the cardinality of some set.

Theorem 27.1 (Pigeonhole principle)**.** *Let S and T be sets such that $|T| > |S|$. Then for every total function $f : T \to S$, there are at least two elements in T that map to the same element of s under f.*

Before we see an application, let's discuss why this is called the pigeonhole principle. In the theorem above, think of the elements of T as pigeons, and of elements of S as pigeonholes. Since $|T| > |S|$, there are more pigeons than pigeonholes, so after all pigeons enter some pigeonhole, there has to be at least one hole that contains at least two pigeons.

Example 27.2: The UW-Madison student ID-numbers are 10 digits long, and each digit is an integer between 0 and 9. The smallest the sum of those digits can be is 0 (when all digits are zero), and the largest the sum can be is 90 (when all digits are nine). Thus, there are 91 possibilities for the sum of the digits in a UW-Madison student ID number.

Let S be the set of all possible digit sums of student ID numbers. We have just seen that $|S| = 91$. There are 95 students enrolled in CS/Math 240 right now. Let T be the set of all students enrolled in CS/Math 240. Since $|T| > |S|$, the pigeonhole principle implies that there are at least two students in CS/Math 240 whose student ID numbers have the same digit sum. ⊠

We remark that regardless of its simplicity, the pigeonhole principle is quite a powerful tool that is used throughout mathematics. Its power stems from the fact that it makes no assumptions whatsoever about the sets S and T, and that all we need in order to apply it is to know $|S|$ and $|T|$.

The drawback is that since we don't know anything about the sets S and T besides their cardinalities, we cannot find two elements of T that map to the same element of S. The pigeonhole principle merely asserts their existence, but does not give us a way of finding them. Thus, arguments using the pigeonhole principle are *nonconstructive*.

This is contrary to, say, the proof that there is a finite state automaton for the language $L(M_1) \cup L(M_2)$ where M_1 and M_2 are finite state automata. In Lecture 23, we did not only prove the existence of a finite state automaton. The proof of its existence was *constructive*, that is, we actually constructed a finite state automaton for the language $L(M_1) \cup L(M_2)$.

27.3 Combinatorial Arguments

As we mentioned at the beginning of lecture, combinatorial reasoning is a way of deriving identities or inequalities by counting a set in two different ways. We can think of it as another proof technique. This technique is best explained on examples.

We have actually seen a combinatorial argument before. In Lecture 19 we showed that the graph K_5 was not planar by counting the number of edge-face pairs (e, f) such that e is on the border of f in two different ways. First, we added up the numbers of edges on the border of each face, and then, for each edge, we added up the numbers of faces that have that edge on their border. This led to two different bounds on the number of the pairs in (e, f), and ultimately gave us a contradiction showing that the graph K_5 is not planar.

27.3.1 Equating Two Binomial Coefficients

Let's start with a simple example that illustrates the technique.

Proposition 27.2. *For all integers n and k, $\binom{n}{k} = \binom{n}{n-k}$.*

First let's see a proof without combinatorial reasoning.

First proof. By definition, $\binom{n}{k} = \frac{n!}{(n-k)!\cdot k!}$, and $\binom{n}{n-k} = \frac{n!}{(n-(n-k))!(n-k)!} = \frac{n!}{k!\cdot(n-k)!}$. We see that the expressions for the two binomial coefficients are the same. □

And now let's see a proof that uses combinatorial reasoning.

Second proof. Let S be the set of all k-element subsets of a set of n elements. We can describe this set by saying which k elements belong to it, and also by saying which $n-k$ elements are the ones that do not belong to it. For example, if $n=5$ and $k=2$, the statements "elements 1 and 3 belong to the subset" and "elements 2, 4 and 5 do not belong to the subset" describe the same subset of $\{1,\ldots,5\}$.

We have $\binom{n}{k}$ ways to pick the k elements that are in the subset, and we have $\binom{n}{n-k}$ ways to pick the $n-k$ elements that are not in the subset. This means that $\binom{n}{k} = \binom{n}{n-k}$. □

The second proof looks more complicated than the first one. Indeed, combinatorial reasoning is a little bit of an overkill for this problem. However, this example is good for illustrating the technique. Now we look at a more involved example.

27.3.2 Pascal's Identity

Pascal's identity is another relationship between binomial coefficients. It says the following.

Proposition 27.3 (Pascal's identity)**.** *For any integers n and k, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.*

Before we prove it, let's see an application that can be used to construct all binomial coefficients out of binomial coefficients where the "top" value is smaller. Let's arrange all the binomial coefficients in a triangle in the following way. One row of the triangle consists of the list $\binom{n-1}{0}, \binom{n-1}{1}, \ldots, \binom{n-1}{n}$. The next row contains the values of the binomial coefficients with the "top" entry n, again listed in order of the "bottom" entry: $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$. We write it so that $\binom{n}{k}$ is between $\binom{n-1}{k-1}$ and $\binom{n-1}{k}$. That is, the configuration of those three binomial coefficients is as shown in Figure 27.1a. We can see the first five rows of the triangle obtained this way in Figure 27.1b, and show the values of the coefficients in Figure 27.1c. In order to obtain the next row, we can write down ones at the beginning and the end of that row, and then compute the entries in between by adding up two entries from the row above.

The entries at the beginning and end of each row do not follow the pattern of Figure 27.1a. One of the coefficients in the row above $\binom{n}{0}$ is missing for $n \geq 1$. We treat that missing coefficient as zero. This makes sense because $\binom{n}{k}$ stands for the number of ways we can pick a subset of k elements out of an n-element set. There are zero ways to pick -1 elements out of n, and also zero ways to pick $n+1$ elements out of n. Thus, defining $\binom{n}{k}$ to be zero whenever $k < 0$ or $k > n$ makes sense.

Proof of Proposition 27.3. Let S be the set of all sets of k elements from $\{1,\ldots,n\}$. The left-hand side, $\binom{n}{k}$, counts the cardinality of S the obvious way.

There is another way to find the cardinality of S. Write S as the disjoint union $S = S_{n^{\text{in}}} \dot\cup S_{n^{\text{out}}}$ where $S_{n^{\text{in}}}$ is the subset of S consisting of all sets that contain the last element n, and $S_{n^{\text{in}}}$ is the subset of S consisting of all sets that don't contain that element.

Since all sets in $S_{n^{\text{in}}}$ contain a total of k elements and n is one of them, we have to pick the remaining $k-1$ elements out of the elements 1 through $n-1$. This can be done $\binom{n-1}{k-1}$ ways, so $|S_{n^{\text{in}}}| = \binom{n-1}{k-1}$.

Now sets in $S_{n^{\text{out}}}$ consist of k elements and don't contain n. Thus, all their elements come from $\{1,\ldots,n-1\}$, which means that $|S_{n^{\text{out}}}| = \binom{n-1}{k}$.

$$\begin{array}{cc} \binom{n-1}{k-1} & \binom{n-1}{k} \\ \multicolumn{2}{c}{\binom{n}{k}} \end{array}$$

(a) Configuration of the coefficients related by Pascal's identity.

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}$$

(b) Binomial coefficients in the first five rows of Pascal's triangle.

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

(c) The values in the first five rows of Pascal's triangle. Each entry is the sum of the two entries above it in the previous row. If one of the entries is missing, we treat it as zero.

Figure 27.1: Pascal's triangle

The sum rule now tells us that $|S| = \binom{n-1}{k-1} + \binom{n-1}{k}$, and the proof is complete. □

27.3.3 Vandermonde's Identity

Now let's look at an expression that looks a little more scary.

Proposition 27.4 (Vandermonde's identity)**.** *For any integers n and k, $\binom{2n}{k} = \sum_{\ell=0}^{k} \binom{n}{\ell}\binom{n}{k-\ell}$.*

Proof. Let S be the set of all k-element subsets of the set $\{1, \ldots, 2n\}$. The left-hand side, $\binom{2n}{k}$, counts $|S|$ in the obvious way.

There is another way to count the elements of S. Think of a subset as a binary string of length $2n$ that has k ones in it. Some of the positions we pick for the k ones lie in the first half of the string, and the rest lie in the second half. In particular, if ℓ lie in the first half, $k - \ell$ lie in the second half. Let S_ℓ be the set of all strings of length $2n$ that contain k ones, ℓ of which are in positions 1 through n (and $k - \ell$ of which are in positions $n + 1$ through $2n$). Since we can place any number of ones between 0 and k in the first half of the string, we have S as the disjoint union $S = \dot{\bigcup}_{0 \leq \ell \leq k} S_\ell$.

A string with ℓ ones in positions 1 through n and $k - \ell$ ones in positions $n + 1$ through $2n$ corresponds to a subset of $\{1, \ldots, 2n\}$ consisting of ℓ elements from $\{1, \ldots, n\}$ and $k - \ell$ elements from $\{n + 1, \ldots, 2n\}$. We can pick ℓ elements out of $\{1, \ldots, n\}$ $\binom{n}{\ell}$ ways, and we can pick $k - \ell$ elements out of $\{n + 1, \ldots, 2n\}$ ways. We can combine the two choices any way we want, so the product rule implies that we can pick an element of S_ℓ $\binom{n}{\ell}\binom{n}{k-\ell}$ ways. The sum rule then implies that $|S| = \sum_{\ell=0}^{k} \binom{n}{\ell}\binom{n}{k-\ell}$. □