Math 172 - HW 2

Michael Knopf

February 3, 2015

1. Let S be a set with special subsets $E_1, \dots, E_n$, as in the setup of inclusion-exclusion. Let f_k denote the number of elements in S that are in **exactly** k of the sets. Show that

$$f_k = \sum_{i=k}^{n} (-1)^{i-k} \binom{i}{k} h_i,$$

where

$$h_i = \sum_{\{a_1,\dots,a_i\} \subset [n]} |E_{a_1} \cap \cdots \cap E_{a_i}|.$$

Then give an analagous formula for f'_k, which is the number of elements in S which are in **at least** k of the sets.

Proof. Suppose $x \in S$ is in exactly $k+j$ of the sets. Then the number of sets $\{a_1, \dots, a_i\} \subset [n]$ (of i elements) for which $E_{a_1} \cap \cdots \cap E_{a_i}$ contains x is $\binom{k+j}{i}$, since we can count them by counting the number of ways to choose k of these $k+j$ sets that contain x. Thus, this is the contribution of x to h_i.

To count the contribution of x to the ith term of $\sum_{i=k}^{n} (-1)^{i-k} \binom{i}{k} h_i$, the product principle allows us to multiply its contribution to h_i by $(-1)^{i-k}\binom{i}{k}$. Its contribution to the ith term, then, is $(-1)^{i-k}\binom{i}{k}\binom{k+j}{i}$. Therefore, its overall contribution to the supposed expression for f_k is

$$\sum_{i=k}^{k+j} (-1)^{i-k} \binom{i}{k} \binom{k+j}{i} = \sum_{i=0}^{j} (-1)^{i} \binom{i+k}{k} \binom{k+j}{i+k},$$

where the upper index in the first expression is $k+j$ rather than n because the summand is 0 for all $i > k+j$. Note that, if $j < 0$, then this sum is 0, thus the overall contribution of x is 0. So for the following argument, assume $j \geq 0$.

Manipulating this expression gives

$$\begin{aligned}
\sum_{i=0}^{j}(-1)^i\frac{(i+k)!(k+j)!}{k!i!(j-i)!(i+k)!} &= \frac{(k+j)!}{k!}\sum_{i=1}^{j}(-1)^i\frac{1}{i!(j-i)!} \\
&= j!\frac{(k+j)!}{k!}\sum_{i=1}^{j}\binom{j}{i}1^{j-i}(-1)^i = j!\frac{(k+j)!}{k!}(1-1)^j \\
&= j!\frac{(k+j)!}{k!}0^j.
\end{aligned}$$

If x is in exactly k of the sets, then $j=0$, thus this expression reduces to $0!\frac{k!}{k!}0^0=1$. Otherwise, $j>0$, in which this case this expression is 0. Therefore,

$$\sum_{i=k}^{n}(-1)^{i-k}\binom{i}{k}h_i$$

$$\begin{aligned}
&= 1\cdot|\{x : x \text{ is in exactly k of the sets}\}| \\
&+ 0\cdot|\{x : x \text{ is not in exactly k of the sets}\}|
\end{aligned}$$

$$= f_k.$$

The number of elements in at least k sets is

$$\sum_{j=k}^{n} f_j = \sum_{j=k}^{n}\sum_{i=j}^{n}(-1)^{i-k}\binom{i}{k}h_i$$

We can group the terms according to which h_i they contain as a factor by expanding the above expression:

$$\begin{aligned}
&\binom{k}{k}h_k - \binom{k+1}{k}h_{k+1} + \binom{k+2}{k}h_{k+2} - \cdots + (-1)^{n-k-1}\binom{n-1}{k}h_{n-1} + (-1)^{n-k}\binom{n}{k}h_n \\
&\qquad \binom{k+1}{k+1}h_{k+1} - \binom{k+2}{k+1}h_{k+2} + \cdots + (-1)^{n-k-2}\binom{n-1}{k+1}h_{n-1} + (-1)^{n-k-1}\binom{n}{k+1}h_n \\
&\qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots \\
&\qquad\qquad\qquad\qquad\qquad\qquad + \binom{n-1}{n-1}h_{n-1} - \binom{n}{n-1}h_n \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad + \binom{n}{n}h_n.
\end{aligned}$$

So the coefficient of h_i in the expansion is $\sum_{j=k}^{i}(-1)^{i-j}\binom{i}{j}$, which can be verified by collecting terms vertically. So an expression for the number of elements in at least k sets is

$$\sum_{i=k}^{n}\left(\sum_{j=k}^{i}(-1)^{i-j}\binom{i}{j}\right)h_i.$$

$\square$

2. Find the "best" estimate for the following (give a justification for each answer, but no need to prove why the answer you selected is better than the others):

(a) $\binom{n}{2}$;

(b)The sum of the first n positive integers;

(c)The number of ways to have a set of n total red, white, and blue indistinguishable balls.

Your answers should be "simple", such as $O(\log^k(n)$, $O(n^k)$, or $O(k^n)$ for specific k.

Proof. First, note that any degree k polynomial in n is $O(n^k)$. Let $p(n) = a_k n^k + a_{k-1}n^{k-1} + \cdots + a_1 n + a_0$, and let $a = \max\{a_0, \ldots, a_k\}$. Let $M = 2a$. Since

$$\frac{n^k}{n^{k-1} + n^{k-2} + \cdots + n + 1} \to \infty \quad \text{as} \quad n \to \infty$$

we know there is an $N > 0$ such that $\dfrac{n^k}{n^{k-1} + n^{k-2} + \cdots + n + 1} > 1$ for all $n > N$. Also, $\dfrac{a}{M-a} = \dfrac{a}{2a-a} = 1$. Therefore, for these choices of M and N,

$$\frac{a}{M-a} = 1 < \frac{n^k}{n^{k-1} + n^{k-2} + \cdots + n + 1}$$
$$\implies a_{k-1}n^{k-1} + \cdots + a_1 n + a_0 \le an^{k-1} + \cdots + an + a < (M-a)n^k \le Mn^k - a_k n^k$$
$$\implies p(n) = a_k n^k + a_{k-1}n^{k-1} + \cdots + a_1 n + a_0 < Mn^k$$

for all $n > N$. Thus $p(n) = O(n^k)$.

All three of these are $O(n^2)$. For part (a), we have $\binom{n}{2} = \dfrac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n = O(n^2)$. For part (b), we have $\sum_{i=1}^{n} i = \dfrac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n = O(n^2)$.

Part (c) is asking for the number of ways to place n indistinguishable balls into 3 distinguishable bins (assuming that it allows for us to have 0 balls in a bin). This number is $\binom{n+2}{2} = \dfrac{(n+2)(n+1)}{2} = \dfrac{n^2+3n+2}{2} = O(n^2)$.

If we insist there be at least 1 ball of each color, then we can arrange the n balls in a line are count the number of ways to place 2 dividers into the $n-1$ spaces between balls (without repetition). Each ball will be colored according to which of the 3 resulting sections it is part of. The number of ways to do this is $\binom{n-1}{2} = \dfrac{(n-1)(n-2)}{2} = \dfrac{n^2-3n+2}{2} = O(n^2)$.

$\square$

3. Show, **with combinatorics and not algebra /number theory**, Fermat's Little Theorem: that $a^p - a$ is divisible by p for any prime p and positive integer a. (hint: you probably want to create a set S with $a^p - a$ elements; also, think quotient principle.)

Proof. Let $S = [a]^p \setminus \bigcup_{i=1}^{a} \{i\}^p$, so that S is the set of all length p tuples, with entries from $[a]$, for which not all components are equal. So $|S| = |[a]^p| - |\bigcup_{i=1}^{a} \{i\}^p| = a^p - a$.

Define a relation $\sim$ on S by $x \sim y$ if y is a roation of x. Formally, we could denote by x_n the nth component of x (where the indices are taken modulo p, for convenience) and define $x \sim y$ if there is some integer k such that $y_n = x_{(n+k)}$ for all n. We may take k modulo p as well, since rotation by p is the identity on a tuple of length p.

Note that $\sim$ is an equivalence relation. For every $x \in S$, we have $x \sim x$ since $x_n = x_{n+0}$ for all n. If $x \sim y$, then $y_n = x_{n+k}$. So $x_n = y_{n-k}$ for all n, thus $y \sim x$. If $x \sim y$ and $y \sim z$, then $y_n = x_{n+j}$ and $z_n = y_{n+k}$. So $z_n = x_{n+j+k}$ for all n, thus $x \sim z$. Therefore, $\sim$ induces a partition on S, so we wish to count the number of distinct elements in each equivalence class.

There are at most p elements in each class, since there are p possible choices for k. Rotations by $i, j \in \mathbb{Z}_p$ are equivalent if and only if rotation by $i - j$ is the identity. So let $x \in S$, and assume, for a contradiciton, that rotation by some nonzero $k \in \mathbb{Z}_p$ is the identity on x.

This means that $x_n = x_{n+k}$ for all n, which inductively gives that $x_n = x_{n+ck}$ for all c. Therefore, the first string of k components of x are repeated throughout the tuple. For example, if $k = 3$, then x could be $(1, 3, 4, 1, 3, 4, ..., 1, 3, 4)$. This means that x is a concatenation of strings of size k, thus $k \mid p$. Because we are taking k modulo p, the only possibility is $k = 1$. However, this means that $x_0 = x_1 = \cdots = x_{p-1}$, a contradiction because S does not include tuples for which every entry is the same.

Therefore, each $k \in \mathbb{Z}_p$ induces a unique rotation on x, meaning each equivalence class contains exactly p elements. Thus, the number of equivalence classes is $\dfrac{|S|}{p} = \dfrac{a^p - a}{p}$, which implies that $p \mid a^p - a$ (since there must be an integral number of equivalence classes).

$\square$

4. Show that **both** of the following are $O(\log(n))$, where the base of the logarithm can be taken to be any number (say e for natural log):

(a) The number of digits of n written in base 10.

(b) The number of digits of n written in base 2.

Proof. Let b be the base, so $b = 10$ for part (a) and $b = 2$ for part (b). Every integer n can be written as ab^k such that $b^{-1} \leq a < b^0$, so that $-1 \leq \log_b(a)$ and k is the number of digits in the base b expansion of n.

Solving for k gives $k = \log_b n - \log_b a$. From the inequality in the previous paragraph, we obtain

$$\log_b n - \log_b a \leq \log_b n + 1.$$

For all $n > b$, we have $1 < \log_b n$, so

$$k = \log_b n - \log_b a \leq \log_b n + 1 < \log_b n + \log_b n = 2 \log_b n.$$

Thus $k = O(\log_b n)$. $\square$

5. (VLW 10D) Define $\mu(d)$ to be

(a)1 if d is a product of an even number of **distinct** primes,

(b)-1 if it is a product of an odd number of distinct primes, and

(c)0 otherwise (in particular, if the square of any prime divides d, you should get 0).

The Reimmann ζ-function is defined as $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Show that

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \mu(n) n^{-s}.$$

Hints: you don't need to touch s at all (which is actually a complex number!). Just figure out how to make sense of what the question **means**. You are also free to use the following result without proof: $\sum_{d|n} \mu(d) = 1$ if $n = 1$ and 0 otherwise. (this is Theorem 10.3 in VLW, which is short and easy. Optional: try to prove it without looking).

Proof. First, we will show that $\sum_{d|n} \mu(d) = 1$ if $n = 1$ and 0 otherwise. It is trivial that $\sum_{d|1} \mu(d) = \mu(1) = 1$ because 1 has 0 distinct prime factors, and 0 is even.

Now, assume $n > 1$. Let $S = \{p_1, \ldots, p_k\}$ be the set of prime factors of n. The nonzero terms in the sum are the terms $\mu(d)$ where $d = \prod_{p \in T} p$ for some $T \subseteq S$. If T has even cardinality, then $\mu(d) = 1$. Otherwise, $\mu(d) = -1$. Thus there is a bijection between the positive terms and the even-sized subsets of S, and there is a bijection between the negative terms and the odd-sized subsets of S. We will show, by induction on the size k of S, that S has the same number of even-sized and odd-sized subsets, thus giving the result.

If $k = 1$, then the only subsets of S are $\emptyset$, which has even size, and $S = \{p_1\}$, which has odd size. Now, suppose $|S| > 1$ and let $p \in \mathcal{P}(S)$. By the inductive hypothesis, we may assume that $\mathcal{P}(S \setminus \{p\})$ has the same number of even-sized and odd-sized subsets. The remaining subsets of S are all sets of the form $T \cup \{p\}$ for some $T \in \mathcal{P}(S \setminus \{p\})$. Furthermore, $T \cup \{p\}$ has even size if and only if T has odd size. Thus we have formed two bijections: one between the even-sized subsets of S which do not contain p and the odd-sized subsets of S which do contain p, and one between the odd-sized subsets of S which do not contain p and the even-sized subsets of S which do contain p. Thus S has an equal number of odd and even-sized subsets.

Now, we wish to show that $\zeta(s) \sum_{n=1}^{\infty} \mu(n) n^{-s} = 1$, so express the left-hand side as

$$(1^{-s} + 2^{-s} + 3^{-s} + 4^{-s} + \cdots)(1^{-s}\mu(1) + 2^{-s}\mu(2) + 3^{-s}\mu(3) + 4^{-s}\mu(4) + \cdots).$$

The expansion of this product is formed by summing all pairwise products of terms from these two factors. We may group the terms in this expansion according to their coefficient n^{-s}, since every term will be of the form $n^{-s}u_n$, where u_n is a sum of the images of some numbers under the Möbius function.

To determine u_n for a given n, we must identify all possible ways to choose two terms – one from the left factor, of the form c^{-s}; and one from the right factor, of the form $d^{-s}\mu(d)$ – such that $cd = n$. u_n will be the sum of all $\mu(d)$ for which such terms exists. Since both factors contain every divisor of n, the expansion contains the term $c^{-s}d^{-s}\mu(b)$, such that $cd = n$, for every divisor d of n. This gives us the following expression for u_n:

$$u_n = \sum_{d|n} \mu(d).$$

Therefore,

$$\zeta(s) \sum_{n=1}^{\infty} \mu(n) n^{-s} = \sum_{n=1}^{\infty} n^{-s} u_n$$

$$= \sum_{n=1}^{\infty} n^{-s} \sum_{d|n} \mu(d) = 1^{-s} \sum_{d|1} \mu(d) + \sum_{n=2}^{\infty} n^{-s} \sum_{d|n} \mu(d)$$

$$= 1 + \sum_{n=2}^{\infty} n^{-s} \cdot 0 = 1.$$

So $\dfrac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \mu(n) n^{-s}$.

□

6. The rules of "172 Craps" is similar to Craps, but slightly different: you have 2 normal 6-sided dice, and you roll. If you get a 2, 3, 11, or 12, you lose immediately. If you roll a 7 you win. After this first turn, you remember the results of your first roll (which must not be a 7 otherwise you would have won already) and continue to roll until you get a 7 (in which case you **lose**) or your first roll (in which case you win). What is your probability of winning? (Hint: it is really useful to understand the following baby situation: suppose $p_1 + p_2 + p_3 = 1$ and you have a game where you win with probability p_1, lose with probability p_2, and replay the game with probability p_3. What is the probability that you win?)

Proof. First, we need to calculate the probability of rolling these numbers. Consider the outcome space to be all possible outcomes from rolling two 6-sided dice, where order is accounted for. So the size of the outcome space is $6^2 = 36$. Let X be the sum of the two rolls. The size of the event $X^{-1}(n)$ is the number of ways to write n as a sum of two integers integers between 1 and 6, where again order matters.

n	2	3	4	5	6	7	8	9	10	11	12
$\lvert X^{-1}(n)\rvert$	1	2	3	4	5	6	5	4	3	2	1
$\mathbb{P}(X = n)$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

First, we will derive the result, called *Craps Principle*, for the situation given in the hint. Suppose $p_1 + p_2 + p_3 = 1$ and you have a game where you win with probability p_1, lose with probability p_2, and replay the game with probability p_3.

Let E_n be the event in which you win on the nth play. In order to win on the nth play, you must roll a "play again" on all previous plays, then win. By the product rule, this probability is $p_3^{n-1} p_1$. Thus, by the sum rule, the probability of winning is

$$\sum_{n=1}^{\infty} \mathbb{P}(E_n) = \sum_{n=1}^{\infty} p_3^{n-1} p_1 = p_1 \sum_{n=0}^{\infty} p_3^n = \frac{p_1}{1-p_3} = \frac{p_1}{p_1+p_2}.$$

Now, let X_i be the sum of the two rolls on the ith play (given that there is an ith play, otherwise we can let it be 0 if we like) in a game of "172 Craps". Let E be the event that you win. By the Craps Principle, $\mathbb{P}(E|X_1 = k)$ for some $k \in \{4, 5, 6, 8, 9, 10\}$ is $\dfrac{\mathbb{P}(X_i = k)}{\mathbb{P}(X_i = k) + \mathbb{P}(X_i = 7)}$, where i is any positive integer, since the choice of i does not affect the probability.

$$\begin{aligned}
\mathbb{P}(E) &= \mathbb{P}(X_1 = 7) + \sum_{k=4}^{6} \mathbb{P}(E|X_1 = k)\mathbb{P}(X_1 = k) + \sum_{k=8}^{10} \mathbb{P}(E|X_1 = k)\mathbb{P}(X_1 = k) \\
&= \mathbb{P}(X_1 = 7) + 2\sum_{k=4}^{6} \mathbb{P}(E|X_1 = k)\mathbb{P}(X_1 = k) \\
&= \mathbb{P}(X_1 = 7) + 2\left(\frac{\mathbb{P}(X_i = 4)^2}{\mathbb{P}(X_i = 4) + \mathbb{P}(X_i = 7)} + \frac{\mathbb{P}(X_i = 5)^2}{\mathbb{P}(X_i = 5) + \mathbb{P}(X_i = 7)} + \frac{\mathbb{P}(X_i = 6)^2}{\mathbb{P}(X_i = 6) + \mathbb{P}(X_i = 7)} \right) \\
&= \frac{6}{36} + 2\left(\frac{\left(\frac{3}{36}\right)^2}{\frac{3}{36} + \frac{6}{36}} + \frac{\left(\frac{4}{36}\right)^2}{\frac{4}{36} + \frac{6}{36}} + \frac{\left(\frac{5}{36}\right)^2}{\frac{5}{36} + \frac{6}{36}} \right) = \frac{433}{990}.
\end{aligned}$$

$\square$

7. (optional) What does Inclusion-Exclusion look like for multi-sets (sets where an identical element can occur multiple times)? Design your theorem.

A multiset is a structure (S, m_S) where S is a set and $m_S : S \to \mathbb{N}$. We will call $m_S(s)$ the *multiplicity* of s in S. Also, define

$$(S, m_S) \cup (T, m_T) = (S \cup T, \max(m_S, m_T))$$
$$(S, m_S) \cap (T, m_T) = (S \cap T, \min(m_S, m_T)).$$

Finally, define the size of (S, m_S) to be $|S(m)| = \sum_{s \in S} m_S(s)$.

Inclusion-Exclusion is the same for multi-sets as it is for sets:

Let $E_1, \dots, E_n$ be multisets. Then

$$\left| \bigcup_{i=1}^{n} E_i \right| = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \le i_1 < \cdots < i_k \le n} |E_{i_1} \cap \cdots \cap E_{i_k}| \right).$$

Proof. For each i, let A_i be a set (not a multiset) defined by

$$A_i = \bigcup_{s \in E_i} \{(s, 1), s(s, 2), \dots, (s, (m_S(s))\}.$$

Any intersection of some collection of the E_i has the same size as the intersection of the corresponding collection of A_i, and similarly for any unions. Therefore, the stated formula simply reduces to the standard inclusion-exclusion formula for sets, applied to the A_i.

$\square$

8. How much time did you spend on this problem set? What comments do you have on the problems? (difficulty, type, enjoyment, fairness, etc.)

I spent a lot of time on this, but it was worth it. The problems were very interesting. My favorites were 2 and 5. I think it's cool that Fermat's Little Theorem can be shown in so many different ways, but I had never thought of it combinatorially before. It was also nice to get to look into the Riemann zeta function. I know the proof that establishes its inverse using the Euler product formula, so I wanted to try to prove it without using that formula.

I found 1 and 5 pretty challenging. On question 3, I knew exactly what I wanted to say, but had a hard time expressing it. It was tough trying to write a correct proof without being too technical.