Assignment 2

Rachel Hwang
(discussed w/ Spencer Claxton)

October 23, 2013

1. *Give a closed form expression for the number of ordered pairs $\langle A, B\rangle$, where $A, B \subseteq [n]$ are such that $A \cup B = [n]$.*

   Let set $S \subseteq [n]$ be a binary string of length n, where each digit s_i in the string corresponds to one element i in $[n]$. If the $s_i = 1$, then $i \in A$, and if $s_i = 0$, then $i \notin A$. So a string of all 0's represents $\varnothing$ and all 1's represents $\{1, \ldots, n-1\}$.

   Let us imagine A and B as such strings. We want to count how many pairs of A and B exist such that $A|B = 1^n$ (equivalent to $A \cup B = [n]$).

   When $A = 1^n$, any value of B will satisfy $A|B = 1^n$. There are 2^n possible binary strings of length n, so in the case $A = 1^n$, there are 2^n viable values of B. However, when A has one 0 in the string, say $a_0 = 0$, then b_0 must be 1 to satisfy $A|B = 1^n$. The value of one digit is now set to 0 already, so there are 2^{n-1} viable values of B. But we must count possible values of B for every possible configuration of A as a string with n-1 1's and a single 0. We are counting the ways to place a single 0, so this value is $\binom{n}{1} = n$.

   This establishes a pattern. For the case A has k 0's in it (the rest are 1's), the number of possible configurations is $\binom{n}{k}$. For each of these A vales, we count the number of possible B values as 2^{n-k}, since k digits are already determined. This gives us:

$$\sum_{k=0}^{n-1} 2^{n-k} \binom{n}{k} = \text{ number of valid pairings}$$

2. *The Hamming weight of a binary string is the number of ones in it. Give a combinatorial bijection between the set of all binary stings of length n and even Hamming weight and the set of those that have the same length n and whose Hamming weight is odd.*

   Given a binary string b of length n,
   Let $\neg(b)$ be defined as taking b's logical complement (ie. $\neg(1001) = 0110$).
   Let $b \gg k$ be defined as logically left-shifting b by k bits (ie. $100 \gg 1 = 10$).
   Let $b \ll k$ be defined as logically right-shifting b by k bits (ie. $100 \ll 1 = 1000$).

Let b_1 & b_2 be defined as logical *and* (ie. 100 & 111 = 100).
Let $b_1|b_2$ be defined as logical *or* (ie. 100|111 = 111).

$$f(b) = \begin{cases} \neg b & \text{if } n \text{ is odd} \\ (f(b \gg 1)) \ll 1)|(b\&1) & \text{if } n \text{ is even} \end{cases}$$

This means if the length of b is odd, we return its logical complement, and if the length of b is even, we take the complement of all but the last bit, which remains as is.

Proof: f maps from n-length b-strings with odd hamming weight to n-length b-strings with even hamming weight.

Case 1: n is odd.
b has k ones where k is odd and $n-k$ zeros. Since n is odd and k is odd, $n-k$ must be even. By the definition of logical complement, for each digit of input binary string s, if $s_i = 0$ set $f(s)_i = 1$ and if $s_i = 1$ set $f(s)_i = 0$. Therefore, all k ones will be set to zero and all $n-k$ zeros will be set to one. Since we have already established that k is odd and $n-k$ is zero, f will output a number with an even number of ones and an odd number of zeros.

Case 2: n is even.
b has k ones where k is odd and $n-k$ zeros. Since n is even and k odd, $n-k$ must be odd.
If b_n, the last digit of b, is a one, $b \gg 1$ will give us a string of $n-1$ with $k-1$ ones and $n-k$ zeros. Since n is even, $n-1$ is odd, and so as proved above, taking $f(b \gg 1)$ will return a string with $k-1$ zeros and $n-k$ ones. Shifting this one place to the right and changing the last bit back to its original value will give us $k-1$ zeros and $n-k+1$ ones. This gives us an even number of ones and an odd number of zeros.
If b_n, the last digit of b, is a zero, $b \gg 1$ will give us a string of $n-1$ with k ones and $n-k-1$ zeros. Since n is even, $n-1$ is odd, and so as proved above, taking $f(b \gg 1)$ will return a string with k zeros and $n-k-1$ ones. Shifting this one place to the right and changing the last bit back to its original value will give us $k+1$ zeros and $n-k-1$ ones. This gives us an even number of ones and an odd number of zeros.

Proof: f is 1-to-1
For binary strings a and b, if $a \neq b$, then for some digit number $i < n$, $a_i \neq b_i$. For binary strings, this means either (Case 1: $a_i = 0$ and $b_i = 1$) or (Case 2: $a_i = 1$ and $b_i = 0$). By the definition of logical complement, for each digit of input binary string s, if $s_i = 0$ set $f(s)_i = 1$ and if $s_i = 1$ set $f(s)_i = 0$. Therefore, after we take $f(a)$ and $f(b)$, in Case 1, we will have ($f(a)_i = 1$ and $f(b)_i = 0$) and in Case 2, we will have ($f(a)_i = 0$ and $f(b)_i = 1$). In either case, $f(a)_i \neq f(b)_i$, so $f(a) \neq f(b)$ if $a \neq b$.

Proof: f is onto
Let b be an n-length b-string with an even hamming weight.
If b is of odd length, we can take $\neg b$. Using the logic used in the first proof ("f maps from n-length b-strings...") for Case 1, this will return a binary string c of odd length with an odd hamming weight where $c = \neg b$. Since $f(c)$ will return $\neg c$, this returns $\neg\neg b = b$. So $\exists c$ such that $f(c) = b$.
If b is of even length, we can take $(f(b \gg 1)) \ll 1)|(b\&1)$. Using the logic used in the first proof ("f maps from n-length b-strings...") for Case 2, this will return a binary string c of

even length with an odd hamming weight where $c = (\neg(b \gg 1)) \ll 1)|(b\&1)$. $f(c)$ will return $(\neg(c \gg 1)) \ll 1)|(c\&1)$ Since $(b\&1) = (c\&1)$, this
$= (\neg((\neg(b \gg 1)) \ll 1)|(b\&1) \gg 1)) \ll 1)|(b\&1)$
$= (\neg\neg b \gg 1) \ll 1)|(b\&1)$
$= (b \gg 1) \ll 1)|(b\&1)$
$= b$
So $\exists c$ such that $f(c) = b$.

Since f is 1-to-1 and onto, f is a bijection.

3. *Which of the following binomial coefficients* $\binom{2013}{500}$ *and* $\binom{2013}{1500}$ *is larger?*

$$\binom{2013}{500} = \frac{2013!}{1513!(500!)} \text{ and } \binom{2013}{1500} = \frac{2013!}{513!(1500!)}$$

Since $1513!(500!) > 513!(1500!)$, the denominator of $\binom{2013}{500}$ is larger than the denominator $\binom{2013}{1500}$. Their numerators are the same. Therefore,

$$\binom{2013}{1500} > \binom{2013}{500}$$

4. *Prove that there are at least* $P(m, n-1) = \frac{m!}{(m-n+1)!}$ *surjective functions from* $[m]$ *to* $[n]$.

Let M = the set of all 1-1 mappings from from $[m]$ to $[n]$. Since a 1-1 mapping must start from a n-sized subset of $[m]$, to find $|M|$, we can first count all possible such subsets, which is $\binom{m}{n}$. For each of these subsets, we count every possible mapping to $[n]$, which is the same as the number of possible orderings of n elements. Thus,

$$|M| = \binom{m}{n} \cdot n! = \frac{m!}{(m-n)!} = P(m, n)$$

A surjective function $f : [m] \to [n]$ is defined as a mapping in which every element of $[n]$ must be mapped to by at least one element of $[m]$. By this definition, we know that for every such surjective function f, there must be some $m_i \subseteq [m]$ of size $[n]$ which has a 1-1 mapping to $[n]$.

We can think of this set of 1-1 mappings as the set n-tuples with unique elements of [m] where each position in the tuple corresponds to an element of [n]. The entry at each position corresponds to the element in [m] mapped to the element in [n] corresponding to the position of the entry. As an example consider the following tuple: (2,4,6,8). By our convention, this means: $f(2) = 0, f(4) = 1, f(6) = 2$ and $f(8) = 3$.

However, not all these tuples/1-1 mappings correspond to unique surjective functions. We are over counting. If $m = n$, the number of surjective functions $[m] \to [n]$ will be equal to the

number of tuples = $n!$. Otherwise, each tuple does not corresponds to a unique surjective f. Some of these mappings may be part of the same functions. For example, given sets [4] and [1] and surjective $f(m) = 1$ mapping between them, using our tuple scheme, (2) and (3) both correspond to f.

Given some surjective $f : [m] \to [n]$, since we know all $e_i \in [m]$ maps to some $n_i \in [n]$, if $m > n$, once we choose some 1-1 mapping tuple t under f, by the pigeonhole principle for every $e_i \in [m], e_i \notin t$ there is some $e_j \in t$ such that $f(e_i) = f(e_j) = n_i$. Therefore, exchanging e_i for e_j in our tuple (swapping one element in t for an element not in t that maps to the same n_i) will create a different 1-1 mapping tuple that also corresponds to f. The size of $\{e_i \notin m_i\} = m - n$, so for every surjective f, there are therefore at least (m-n) different tuples all differing from our original t by 1. Let each set of these tuples corresponding to the same surjective function be called S_i for some i, where $S_i \in M$ and $|S_i|$ = m-n+1. Now there are at least

$$\frac{P(m,n)}{m-n+1} = \frac{m!}{(m-n+1)!} = P(m, n-1)$$

unique such subsets S_i, and thus at least that many surjective functions from $[m]$ to $[n]$.

Proof: Let S refer to the set containing all S_i. Suppose $|S| < P(m, n-1) = \frac{|M|}{|S_i|}$. If so, there exists some 1-1 mapping tuple t_k that does not belong to any of the unique subsets S_i. If all possible tuples already appears in S, then $|S| \geq \frac{|M|}{|S_i|}$, since either $|M|$ is partitioned by the subsets so $|S| = \frac{|M|}{|S_i|}$ or else some tuples occur in multiple subsets and $|S| > \frac{|M|}{|S_i|}$.

So if $\exists t_k$ that does not occur in any of our $m - n + 1$ element subsets, $|S| \geq \frac{|M|}{|S_i|}$ then we can create such a subset for it by pairing it with the m-n tuples that differs from it by one element. We will always be able to do this for some t_k since for every tuple in our 1-1 mappings, there are m-n tuples that differ from it by one (again, pigeonhole principle). This can done for any such tuple that is not in a unique subset to begin with and consequently, all tuples can be placed in at least one unique subset S_i and the number of such subsets must be greater than or equal to $\frac{|M|}{|S_i|} = \frac{P(m,n)}{m-n+1} = \frac{m!}{(m-n+1)!} = P(m, n-1)$

5. *For how many integers n between 1 and $6 \cdot 10^6$ there exists at least one pair of integers (x, y) such that $xn + 60y = 1$?*

By Bezout's Theorem, if $gcd(n, 60) = 1$, then $\exists(x, y)$ such that $xn + 60y = 1$. So we are looking for all the numbers that share no prime factors (2, 3, 5) with 60. So we want to count the multiples of those numbers: (mtpl. of 2) $\cup$ (mtpl. of 3) $\cup$ (mtpl. of 5).

$$6 \cdot 10^6/2 = 3 \cdot 10^6 \text{ multiples of 2.}$$
$$6 \cdot 10^6/3 = 2 \cdot 10^6 \text{ multiples of 3.}$$
$$6 \cdot 10^6/5 = 1.2 \cdot 10^6 \text{ multiples of 5.}$$
$$Total = 6.2 \cdot 10^6 \text{ multiples of single factors}$$

However, we are double-counting numbers which are multiples of pairs of these numbers, and triple counting numbers which are multiples of all three. So we count numbers which are

multiples of each pair of our factors: (mtpl. 2) $\cap$ (mtpl. 3), (mtpl. 2) $\cap$ (mtpl. 5), (mtpl. 3) $\cap$ (mtpl. 5).

$$\begin{aligned} 6 \cdot 10^6/(2 \cdot 3) &= 10^6 \text{ multiples of 6.} \\ 6 \cdot 10^6/(2 \cdot 5) &= 6 \cdot 10^5 \text{ multiples of 10.} \\ 6 \cdot 10^6/(3 \cdot 5) &= 4 \cdot 10^5 \text{ multiples of 15.} \\ Total &= 2 \cdot 10^6 \text{ multiples of pairs of factors} \end{aligned}$$

But now we have overcounted the numbers that we are subtracting from the first number (multiples of single factors) since we count the numbers which are multiples of all three factors three times. We count those numbers: (mtpl. 2) $\cap$ (mtpl. 3) $\cap$ (mtpl. 5).

$$6 \cdot 10^6/(2 \cdot 3 \cdot 5) = 2 \cdot 10^5 \text{ mulitples of 30}$$

Our final count of numbers that are relatively prime with $6 \cdot 10^6$ is (numbers in range)-((multiples of single factors)-(multiples of pairs of factors)+(multiples of all three factors)) which is

$$6 \cdot 10^6 - (6.2 \cdot 10^6 - 2 \cdot 10^6 + .2 \cdot 10^6) = 1.6 \cdot 10^6$$