Probability, Bayes, Midterm Review

1 Counting

1. Let p, q be prime. How many numbers are there among $1, 2, \ldots (pq)^2$ that are relatively prime to pq?

2. Give a combinatorial proof of $\binom{k+n-1}{n-1} = \sum_{i=0}^{k} \binom{k-i+n-2}{n-2}$.

2 Probability

1. Let A represent the event that someone has cancer. Let B be the event that they test for cancer and it comes positive. Assume that the probability that the test is positive is 90% if they have cancer and 10% if not, and that the overall percentage of people with cancer is 10%.

   (a) Write out all information we know in terms of $Pr()$ expressions.

   (b) What is the probability that someone has cancer if they tested positive?

   (c) Say that the probability that someone dies if they have cancer is 2%, *and* this doesn't depend whether the test came back positive. Call the event that someone dies from cancer C, note that $P(C|\bar{A}) = 0$. Now say that the probability someone dies if they have surgery is p, but they are cured if they have surgery. At what p would it be a bad idea to have surgery if someone received a positive result on the test?

2. Suppose $P(B|A) = P(B|\bar{A})$ where $\bar{A}$ is the complement of A. Prove that it must be the case that B is independent of A.

3. True/False? For any events A,B,C in some probability space, $P(A \cap B \cap C) = P(A|B)P(B|C)P(C)$.

4. True/False? If events A and B are independent, so are $\bar{A}$ and B. Justify your answer with proof or counterexample.

5. You flip a fair coin repeatedly. What is the probability that the first head you see is on the sixth flip?

6. You flip a fair coin repeatedly. What is the probability that the second head you see is on the sixth flip?

7. Suppose 100 people stand in a line, in some random order, where Alice, Bob, and Chris are three of those people. If each permutation is equally likely, what is the probability that Bob is between Alice and Chris but not necessarily standing exactly next to them?

8. Say we have a class of 30 people, and the probability that any two of them are friends on Facebook is 1/20. Give an upper bound for the probability that there are 5 students that are all friends with each other on Facebook.

3 Midterm Review

1. Alice wants to send Bob a message of n symbols (over $GF(p)$,where p is a prime) over a channel. The channel corrupts each symbol independently with probability q. Alice and Bob decide to use a Reed-Solomon code with Alice sending (n + m) symbols over the channel, and Bob using the Berlekamp-Welch decoding algorithm. If the probability that Bob cannot correctly decode Alice's message is to be kept at most α, then write an inequality (it can involve summations) that solves for the smallest value of m needed for this to be accomplished. (You can leave the equation in raw form but you must clearly express the dependencies on the parameters of the problem.)

2. If I have a set T of k-bit strings, where $|T| = k$, give a procedure that looks at only one bit of each string and constructs a k-bit string that is not in the list. You can do things like let me look at the third bit of string 1, or the first bit of string 5.

3. Recall the following statement of the CRT: given k congruencies $x = a_i \pmod{n_i}$ where $a_i \neq 0$ and $gcd(n_i, n_j) = 1$ for $i \neq j$, there is exactly one $x \pmod{N}$ that satisfies all k congruencies for $N = \prod_i n_i$.

   (a) Consider that all the n_i are prime. Argue in this case that $x^{-1} \pmod{\prod_i n_i}$ exists.

   (b) Give an example where n_i may not be prime, where x does not have an inverse $\pmod{N}$.

   (c) Consider the case where every n_i is prime and we have $y = x^{-1} \pmod{N}$. What is $y \pmod{n_i}$? Justify this.

4. Consider the equation $(a_3x^3 + a_2x^2 + a_1x + a_0)(x_2 + b_1x + b_0) = F(x)(x_2 + b_1x + b_0)$, where $F(x)$ is some arbitrary function.

   (a) Let $F(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ on all but k points. What is the maximum value of k such that one can set b_1 and b_0 to "zero out" the equation?

   (b) For how many values of x do we need to know $F(x)$ to fully find a_3, a_2, a_1, a_0, b_1, and b_0, assuming that $F(x)$ differs from $a_3x^3 + a_2x^2 + a_1x + a_0$ on k points as found in the last problem?

5. Consider the equation $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 70$, where each x_i is a non-negative integer.

   (a) How many solutions to this equation are there?

   (b) What if $x_1 \geq 30$ and $x_2 \geq 30$?

   (c) What if we require that either $x_1 \geq 30$ or $x_2 \geq 30$ or both?