CS 70 Discrete Mathematics and Probability Theory
Fall 2013 Midterm #2

1. **(30 points) Short Answer. No justification necessary. Please write only the answer in the space provided after each question. Please do any calculations on the back of the page.**

   (a) (2 points) How many distinct polynomials of degree (at most) 3 are there modulo 11, such that the value at the points $x = 1,2,3,4$ lie in the set $\{1,2,3,4,5\}$?
   Solution: 5^4. 4 points uniquely determine a degree 3 polynomial and each of the 4 points have 5 possibilities.

   (b) (2 points) A bridge hand is a set of 13 cards from a standard 52-card deck. A bridge hand is called balanced if it has 4 cards from one suit and 3 each from the remaining three suits. How many distinct balanced bridge hands are there?
   Solution: $\binom{4}{1}\binom{13}{4}\binom{13}{3}^3$. Select one suit out of 4 to have 4 cards from that suit, and all other suits have 3 cards.

   (c) (2 points) Recall that an anagram of a word is a string made up from the letters of that word, in any order. (For instance, there are exactly three anagrams of BEE: namely EEB, EBE, and BEE. Note that by our definition anagrams need not form legal words.) How many anagrams are there of the word ANAGRAM?
   Solution: $\frac{7!}{3!}$. There are 7! ways to permute the letters, and 3! accounts for over counting for the A's.

   (d) (2 points) In an n dimensional hypercube, how many vertices are there at a distance of exactly 6 from a particular vertex?
   Solution: $\binom{n}{6}$. The vertex can be represented by an n-bit string and all vertices at a distance of exactly 6 differ in 6 bits - we just need to choose which 6 bits.

   (e) (2 points) If A, B, C are event such that $P[A] = .5$, $P[B] = .4$ and $P[C] = .3$, and such that $P[A \cap B] = .2$, $P[A \cap C] = .1$, $P[B \cap C] = .1$ and $P[A \cup B \cup C] = .9$. What is $P[A \cap B \cap C]$?
   Solution: .1. By the inclusion/exclusion principle, $\Pr[A \cup B \cup C] = \Pr[A] + \Pr[B] + \Pr[C] - \Pr[A \cap B] - \Pr[A \cap C] - \Pr[B \cap C] + \Pr[A \cap B \cap C]$.

   (f) (5 points) Pick two *non-zero* numbers x and y modulo 7 at random. Let $z = xy \bmod 7$. Let A be the event that $x = 3$, B that $y = 3$ and C that $z = 3$.
   Note: An alternate interpretation would be picking a random non-zero number and reducing it modulo 7, so you are picking from the set $\{0,\ldots,6\}$. This was also given full credit, and the solutions for this interpretation are included below. Of course if you used the alternative interpretation the solution to part v. was different.

      i. What is $\Pr[C]$?
      Solution: $\frac{1}{6}$. z can be any value other than zero.

Alternate interpretation: $\frac{6}{49}$. *Let x take on any non-zero value (6 possibilities) and y equal* $3x^{-1}$.

ii. What is $\Pr[A \cap B]$?
Solution: $\frac{1}{36}$. Both x and y are equal to 3 with probability $(\frac{1}{6})^2$.
Alternate interpretation: $\frac{1}{49}$. *Both x and y are equal to 3 with probability* $(\frac{1}{7})^2$.

iii. What is $\Pr[A \cap C]$?
Solution: $\frac{1}{36}$.This means that $x = 3$ and $y = 1$, which occurs with probability $(\frac{1}{6})^2$.
Alternate interpretation: $\frac{1}{49}$.*This means that* $x = 3$ *and* $y = 1$*, which occurs with probability* $(\frac{1}{7})^2$.

iv. What is $\Pr[B \cap C]$?
Solution: $\frac{1}{36}$. This means that $y = 3$ and $x = 1$, which occurs with probability $(\frac{1}{6})^2$.
Alternate interpretation: $\frac{1}{49}$. *This means that* $y = 3$ *and* $x = 1$*, which occurs with probability* $(\frac{1}{7})^2$.

v. Are A,B,C pairwise independent? **Yes** **No**
Are A,B,C pairwise independent? **Alternate interpretation:** **Yes** **No**

(g) (5 points) Suppose A and B are disjoint events such that $P[A] \neq 0$ and $P[B] \neq 0$.

i. What is $\Pr[A \cap B]$?
Solution: 0. The events are disjoint so their intersection is empty (it contains no sample points).

ii. Can A and B be independent? **Yes** **No**
Solution: $\Pr[A \cap B]$ is 0, but $\Pr[A] \times \Pr[B]$ cannot be 0 since both events have non zero probability.

(h) (5 points) Suppose Alice wants to send Bob a message consisting of $n = 3$ characters, and there can be $k = 2$ general errors during the transmission. So Alice uses an error correcting code and sends Bob $n + 2k = 7$ characters. Unfortunately, Bob doesn't receive one of the characters, so he now holds 6 characters. There are still k general errors among the remaining characters, but fortunately Alice managed to tell Bob where one of these general errors is. Since he can now throw away the character with an error, Bob holds only 5 characters. Can Bob still recover Alice's message? If so, does he need to use all 5 of his remaining characters, or can he use a smaller number?

Yes, using 5 characters **No**

Solution: There are now $k - 1 = 1$ general errors and Alice wants to send a message of $n = 3$ characters, so $n + 2(k - 1) = 5$ characters are required.

(i) (5 points) A manufacturer claims that they have an excellent test for steroid use. A steroid user tests positive with probability p and non-users test *negative* with the same probability. It is widely known that the fraction of NCAA football players who use steroids is q. How effective is the test when applied to NCAA football players. i.e. what is the probability that a player uses

steroids if he tested positive? You do not need to simplify the expression - just write it in terms of p and q.

The probability is $\frac{pq}{pq+(1-p)(1-q)}$.

Solution: Let A be the event that an NCAA football player uses steroids. Let B be the event that the test result is positive. Then we are given:

$$\begin{aligned}\Pr[A] &= q \\ \Pr[B|A] &= p \\ \Pr[B|\bar{A}] &= 1-p\end{aligned}$$

We would like to find $\Pr[A|B]$. By the total probability rule:

$$\Pr[B] = \Pr[B|A]\Pr[A] + \Pr[B|\bar{A}]\Pr[\bar{A}] = pq + (1-p)(1-q).$$

And by Bayes' rule:

$$\Pr[A|B] = \frac{\Pr[B|A]\Pr[A]}{\Pr[B]} = \frac{pq}{pq+(1-p)(1-q)}.$$

2. **(15 points) Even or odd.** Suppose you flip a biased coin with $P[H] = p$. Let E_n be the event you get an even number of H's in n tosses of the coin. Prove by induction on n that $P[E_n] = \frac{1}{2} + \frac{(1-2p)^n}{2}$ for $n \geq 1$.

Solution:

Base Case: $n = 1$. E_1 is the event that you obtain tails on the first day. $\Pr[E_1] = 1 - p = \frac{1}{2} + \frac{1-2p}{2}$ as claimed.

Inductive Hypothesis: Assume that $\Pr[E_{n-1}] = \frac{1}{2} + \frac{(1-2p)^{n-1}}{2}$.

Inductive Step: Prove that $\Pr[E_n] = \frac{1}{2} + \frac{(1-2p)^n}{2}$.

We can use the total probability rule:

$$\Pr[E_n] = \Pr[E_n|E_{n-1}]\Pr[E_{n-1}] + \Pr[E_n|\bar{E}_{n-1}]\Pr[\bar{E}_{n-1}].$$

Observe that $\Pr[E_n|E_{n-1}]$ is the probability that the n-th flip was tails; this is because if we had an even number of heads on day $n-1$, we must obtain tails on day n to maintain an even number of heads. By the same reasoning, $\Pr[E_n|\bar{E}_{n-1}]$ is the probability that the n-th flip was heads. Plugging in the values and the inductive hypothesis we obtain:

$$\Pr[E_n] = (1-p)(\frac{1}{2} + \frac{(1-2p)^{n-1}}{2}) + p(1 - (\frac{1}{2} + \frac{(1-2p)^{n-1}}{2})).$$

After simplification, we find that:

$$\Pr[E_n] = \frac{1}{2} + \frac{(1-2p)^n}{2}.$$

Here is another way to think about this problem. To get an even number of heads in n tosses, you must have either an even number of heads in $n-1$ tosses (event E_{n-1}) followed by a tails in the n^{th} toss (event T) or an odd number of heads in $n-1$ tosses (event $\bar{E}_{n-1}$) followed by a heads in the n^{th} toss (event H). Note that these two possibilities are disjoint, so the total probability is the sum of the probabilities of each of the two. It follows that:

$$\Pr[E_n] = \Pr[E_{n-1}]\Pr[T] + \Pr[\bar{E}_{n-1}]\Pr[H]$$

Here we used the fact that the outcome of the n-th coin toss is independent of the outcomes of the first $n-1$ tosses. We apply the induction hypothesis as above to get:

$$\Pr[E_n] = (1-p)(\frac{1}{2} + \frac{(1-2p)^{n-1}}{2}) + p(1 - (\frac{1}{2} + \frac{(1-2p)^{n-1}}{2})) = \Pr[E_n] = \frac{1}{2} + \frac{(1-2p)^n}{2}.$$

3. **(15 points) Secret Sharing** Alice is part of a secret sharing scheme in which $n = 10$ people have shares of a secret (which you may think of as a random number modulo 11) such that any $k = 3$ of them can reconstruct the secret. This is implemented using a uniformly random polynomial over $GF(11)$ of degree (at most) 2. Suppose Alice's share of the secret, $P(5)$, is equal to 2. Suppose she happens to learn that Bob's share of the secret, which is $P(4)$, is not 10.
For reference: Property 1: Polynomial of degree d has at most d roots.
Property 2: There is a unique polynomial of degree d that goes through $d+1$ points.
Note: Please state explicitly where you use properties 1 and/or 2 in your solution

   (a) (5 points) Given her information, what is the probability that the secret $P(0)$ is equal to 3? Justify your answer (1 point for the correct answer without proper justification).

   Solution: Assume Alice has both her share of the secret and Bob's share. By Property 2, a polynomial of degree 2 is uniquely defined by 3 points. Since Alice only has 2 points, the secret $P(0)$ can still take on any value. Since the polynomial is randomly chose, the probability that the secret $P(0)$ is equal to 3 is $\frac{1}{11}$. Since this is true for every possible value of Bob's share, it follows that $\Pr[P(0) = 3] = \frac{1}{11}$ even given Alice's partial knowledge of Bob's share.

   (b) (10 points) Suppose Alice also finds out that Carol's share, which is $P(2)$, is equal to 4. Given this additional new information, what is the probability that the secret is equal to 3. Justify your answer (2 points for the correct answer without proper justification).
   Note: A brute force answer will take you too long. There is an easy way to solve the problem.

   Solution: We'll first assume the secret is 3 and determine what Bob's share ($P(4)$) is in this case. If Bob's share is 10 in this case, we know that the probability that the secret is equal to 3 is 0 (because Bob's share cannot be 10). Otherwise, the probability that the secret is equal to 3 is $\frac{1}{10}$, since Bob's share can be any value in $GF(11)$ other than 10.

   To determine Bob's share given that the secret is 3, we use Property 1 and Lagrange interpolation. Property 1 tells us that P is uniquely determined by 3 points, which are $P(0) = 3$, $P(5) = 2$, and $P(2) = 4$ in this case. Lagrange interpolation (or a system of linear equations) allows us to find the polynomial $P(x) = 6x^2 + 5x + 3$. Then Bob's share, $P(4)$, is equal to 9. As we argued above, this means the probability that the secret is equal to 3 is $\frac{1}{10}$.

   Another way to prove this is by assuming that Bob's share is equal to 10, and then computing what the secret is (again using Property 1 and Lagrange interpolation). You'll find that the secret is 9 in this case, which means that when the secret is 3, Bob's share is not equal to 10. As in our solution above, this implies that the probability that the secret is equal to 3 is $\frac{1}{10}$.

   Both of these solutions implicitly make use of the following observation: since Alice already has 2 shares, Bob's share uniquely determines the value of the secret ($P(0)$). This means that there is a bijection between all possible values of Bob's share and all possible values of the secret. This is due to property 2: once 2 values of a degree 2 polynomial are known, the third point uniquely determines the polynomial.

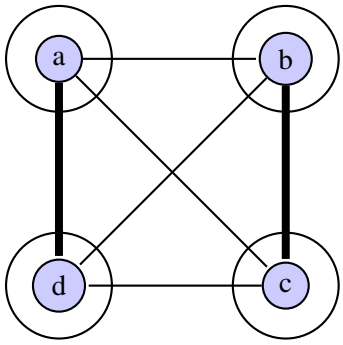
4. **(15 points) Euler.** One way to think of Eulerian tour is as follows: an Eulerian tour is a way of drawing the graph by tracing each edge exactly once and return to the starting point, without lifting the pencil. Now suppose we wish to draw a graph that does not have an Eulerian tour, but is connected and has exactly m vertices of odd degree (m must be even). It is still possible to draw the graph without lifting our pencil and return to our starting point, but now we must trace over some edges more than once.

   (a) (10 points) Prove that regardless of the graph, it is impossible to trace the graph without going over *at least* $\frac{m}{2}$ edges more than once. (Note that there are graphs for which the number of edges that must be traced more than once could be very large, and much larger than m.)

   Solution: During a tracing, each vertex must be entered as many times as it is exited. The only way to do this at an odd degree vertex is to retrace at least one edge. Each retraced edge is incident to at most two odd degree vertices, so there must be at least $\frac{m}{2}$ retraced edges in order to have one incident to each of m vertices.

   (b) (5 points) Give an example of a graph with $m = 4$ odd degree vertices which you can trace with exactly $\frac{m}{2}$ edges traced over more than once (twice). Clearly mark the $m = 4$ odd degree vertices and the $\frac{m}{2} = 2$ edges you trace twice.

   Solution: The odd degree vertices are circled, and the edges used twice are bolded.



5. **(1 point) Bonus Problem.** We play a game, where I shuffle a standard deck of cards and turn them over one at a time. At any time before the last card is turned up you say "Choose", and you win if the next card that I turn up is red. If you never say "Choose" then by default you are assumed to have chosen the last card. Your objective is to maximize the chance of choosing a red card, and you can follow any strategy you like (such as wait until the number of black cards showing is larger than the number of red cards). What is your optimal strategy and what is your chance of choosing a red card under that strategy? Of course, you must prove that your strategy is optimal.

   Solution: This will be provided in the solutions for homework 10.