EECS 70 Discrete Mathematics and Probability Theory
Spring 2013 Anant Sahai

Practice final

Straightforward questions (50%)

Knowing the material in this section well is essential to getting a good grade on the final.

1. **I**f randomly arranging 8 letters {S, t, a, n, f, o, r, d}, what is the probability that the result is "Stanford"? If randomly arranging 8 letters {B, e, r, k, e, l, e, y}, what is the probability that the result is "Berkeley"?
2. **T**here are two pairs of red socks and one pair of white socks in a box, i.e., there are totally 4 red socks and 2 white socks. If randomly drawing 4 socks from the box, what is the probability that they can form two pairs given that you have at least 1 white sock and 1 red sock?
3. **P**rove by induction that the sum of the first n positive integers is $\frac{n(n+1)}{2}$.
4. **L**et $p = 43, q = 23, e = 8$. Using RSA, encode the message $m = 5$ and then show how it would be decoded to check your work. (Errata: 8 is not a valid choice for e. Explain why not, then use $e = 5$.)
5. **L**et $\Pr(A) = 0.7, \Pr(B|A) = 0.2, \Pr(B|A^c) = 0.5$. What is the probability of A given B?
6. **L**et X be a discrete random variable taking values on set of integers $\mathbb{Z}$, with expectation 13 and variance 6. Find a lower bound on $Pr(8 \leq X \leq 18)$.
7. **S**uppose you have a biased 6-sided die such that the probability of getting some number on the die is inversely proportional to the number itself, i.e $P[\text{Rolling } n] \propto \frac{1}{n}$. What is the expectation and variance of the number you get from rolling the die once?
8. **QUESTION DELETED BECAUSE IT HAS TO DO WITH CONTINUOUS PROBABILITY**
9. **P**rove that there are the same number of positive odd numbers as positive integers.
10. **T**he standard polynomial secret sharing is being used and we are working mod 5. Three shares are required to determine the secret, encoded as $P(0)$. We have the following shares: $P(1) = 1, P(2) = 1, P(4) = 2$. What is the secret?

True/false (15%)

The actual final would have only 2-3 of these questions.

1. **C**onsider n cities which are possibly connected to each other by roads. Cities may be isolated (have no roads connecting them to other cities). Note that if city A is connected to city B, then city B is also connected to city A.

   Is the following statement true or false? If true, prove it. If false, give a counterexample.

   "At least two cities have the same number of connections (not necessarily to the same cities).

2. **L**et X_i, $1 \leq i \leq n$ be identically distributed random variables with $E(X_i) = 0$ and $\text{Var}(X_i) = 1$. Then, $Pr(|\sum_{i=1}^{n} X_i| \geq k) \leq \frac{n}{k^2}$.

3. **S**uppose that there are men A, B, C and women $1, 2, 3$. There exist preferences such that the following conditions are both satisfied:

   - No man/woman is matched with his/her first choice.
   - The following pairing will be produced when the traditional propose-and-reject algorithm is run: $(A,1),(B,2),(C,3)$.

   Is the statement above true or false? Prove your answer.

4. **T**he set of all probability mass functions for Bernoulli random variables is countable.

The long hard road (35%)

All of these questions are on the harder side – the actual questions on the final will not be this hard and you won't be expected to spend as much time on this section. We do expect that many students will struggle with this section.

1. **Self grading** There are about $n = 300$ self-graded question parts (e.g. problem 1.1 on HW13) in this iteration of CS 70. On each of them, a student assigns a grade S_i. For each homework, readers randomly grade a subset of the problems. Assume that $n/5 = 60$ of the question parts are graded by the readers (chosen uniformly over all the problem parts) and the readers assign grades R_i. Assume that an honest grade S_i may deviate from R_i according to the following distribution: $S_i = R_i$ with probability $1/2$, $S_i = R_i + 1$ with probability $1/4$, and $S_i = R_i - 1$ with probability $1/4$.

   1. We do the following check: we add up all of the $S_i - R_i$ for a particular student (for the subset of problems graded by readers only). If the result is too high, we suspect that a student might be inflating their grades. What threshold T should we choose so that $\sum(S_i - R_i) \leq T$ for 95% of honest students?
   2. Assume a mediocre student (who never truly deserves full points on any question part) is inflating their self-grades S_i by adding 1 point to a question part with probability 1/2. What is their risk of being caught (i.e. above the threshold T)?
   3. If a student is willing to accept a 50% chance of being caught cheating and expelled from the university, by how much can they inflate their grade? Assume that they can inflate by no more than 3 points per question part.
   4. Is it worth it to inflate your own scores? (Remember: homework is worth only 15% of your grade!)

   Use the most appropriate and best tools that you have to answer the questions above and argue why they are an appropriate choice.

2. **Crazy Crusade: Loathsome Lord Needs a Systematic Strategy**

   Note: correction in bold below.

   1. You-Know-Who has a secret that he wants to share with his Death Eaters. He's not very good at math and wants to use small integers so he picks a polynomial $P(x)$ **of degree 3** in GF(7). He then chooses x_i uniformly at random gives a point $(x_i, P(x_i))$ to each Death Eaters i. However, he doesn't have his Quick Quotes Quill$^{\text{TM}}$ to write down which values he gives to each of the Death Eaters and he's too

lazy to try to find it. As a result, some Death Eaters may end up with the same information (point). What is the probability that a random subset of s Death Eaters can recover his secret for $s = 3, 4, 5$?

2. You-Know-Who's legion of Death Eaters has recently expanded due to popularity. He now has n Death Eaters at his disposal as well as a bookkeeper. The bookkeeper ensures that each of the Death Eaters has a distinct point. He also helps You-Know-Who with his math so they can use a sufficiently large field and a new polynomial with degree $d = n/3 - 1$ (don't worry about fractions—there's a magical solution for those). Unfortunately (for You-Know-Who), each of the Death Eaters has a 50% chance of dying before You-Know-Who secures his control over Magical Britain (or Dumbledore prevails). When the war is over (one way or another), what is the probability that the Death Eaters can recover You-Know-Who's secret if they all work together? How many Death Eaters are needed (initially) so that they can recover the secret with a 90% probability?
3. Unfortunately, the bookkeeper died of old age during the first war. You-Know-Who has risen again with his m remaining Death Eaters. Since his bookkeeper is dead, he goes back to his old scheme of randomly assigning points (as was done in part 1). However, he found time to take some math classes while in hiding so now he'll use a degree-$(m/4 - 1)$ polynomial with coefficients from a finite field of size m. Being a Death Eater is very risky and each Death Eater still has a 50% chance of dying in this new war. Assuming You-Know-Who waited until he had many Death Eaters to start the war (i.e. m is large), would the Death Eaters have a reasonable chance of being able to recover his secret if You-Know-Who is defeated? Argue convincingly with math.

3. QUESTION DELETED BECAUSE IT HAS TO DO WITH CONTINUOUS PROBABILITY