CSM CS70 Fall 2018 Mock Midterm 2

Computer Science Mentors

October 28 2018

1. **True/False (2 points each)**

   (a) X is picked randomly variable over the set $\{0, 1, 2, 3, 4, 5, 6\}$, and A is a uniform random variable over the set $\{1, 2, 3, 4, 5, 6\}$. Define $Y = AX \pmod 7$. Then X and Y are identically distributed.

   (b) In GF(p), any polynomial of degree greater than p has an equal polynomial representation with degree less than p.

   (c) $(x_1 + x_2 + ... + x_n)^p \equiv x_1^p + x_2^p + ... + x_n^p \pmod p$ for a prime p

   (d) The set of all finite length strings consisting of characters from the English alphabet is uncountably infinite.

   (e) Say that you are working in GF(p) have a channel that will corrupt k packets, where $k > \frac{p}{2}$. It is still possible to communicate some length message over this channel.

   (f) We can construct a program $\mathcal{P}$ that, given another program $\mathcal{Q}$ and x as input, can determine if $\mathcal{Q}(x)$ halts in $3^{|x|}$ steps.

(g) The number of ways to rearrange n distinct letters is greater than the number of ways to choose $\frac{n}{2}$ letters from the first half with replacement.

(h) $\sum_{i=1}^{\frac{n}{2}} \binom{n}{i} = \sum_{i=\frac{n}{2}+1}^{n} \binom{n}{i}$, where $n \geq 2$ is even.

(i) $\sum_{i=0}^{n} \binom{n}{i} = n^2$

(j) Given a sample space Ω and event A, A and Ω are always independent.

(k) Take a deck of n cards where each card has a unique number in $1, ..., n$. You draw cards one by one without replacement. Let X_i be the number on the ith card you pick up. Then X_1 and X_2 are identically distributed.

(l) For disjoint events A and B, the $Pr(A \cap B) = Pr(A) \cdot Pr(B)$

(m) If Pr(A) $>$ 0 and Pr(B) $>$ 0, and A and B are disjoint then A and B are not independent.

(n) Given two events A and B with Pr(A) $>$ 0 and Pr(B) $>$ 0, if Pr(A|B) $>$ Pr(A), then Pr(B|A) $<$ Pr(B).

(o) If two events A and B are independent, then A^c and B^c are dependent.

2. **Short Answer: RSA (10 points)**
LeBron wants to send a RSA-encrypted message M to his friends Kevin and Chris. Kevin and Chris use public keys (N, e_1) and (N, e_2). Notice they use the same modulus, but different exponents. LeBron sends $C_1 = M^{e_1} \mod N$ to Kevin and $C_2 = M^{e_2} \mod N$ to Chris. You eavesdrop on LeBrons transmissions and learn C_1 and C_2.

   Show how you can recover M. You may assume that you know e_1, e_2 and N and that e_1 and e_2 are relatively prime.

3. **Short Answer: Polynomials and Error Correction (3 points each)**
   (a) A polynomial has 4 roots. What is the minimum degree?

   (b) Suppose $P(x)$ and $Q(x)$ are two distinct polynomials (of degree d_1 and d_2 respectively) which intersect in exactly 5 points. If the lowest degree polynomial that contains those five points has degree 3, what is the minimum value of $d_1 + d_2$?

   (c) Prove or disprove:
      i. The set of all polynomials of degree 3 that interpolate $(1, 1), (2, 4)$ and $(3, 10)$ is countably infinite.

      ii. Now, re-answer the problem above, but suppose we are working in $GF(p)$ for some prime $p \geq 11$.

(d) Suppose each point represents one character of a message, and that the ith letter in the alphabet is represented by the number i (so A = 1, B = 2, ...). Suppose we want to send the message outlined in part a) (that is, ADJ), but we know that 1 character of our message is going to be corrupted. Determine the number of extra points we need to send, and find those points. Use $GF(13)$ and the correct degree polynomial.

(e) Consider an erasure channel through which you want to send a message of length n.

i. If $\frac{1}{4}$ of your packets are going to be dropped, how many total packets must you send?

ii. Now suppose $\frac{1}{4}$ of your packets are going to be corrupted instead of dropped. How many total packets must you send to combat this error?

4. **Short Answer: Countability**

(a) Let A and B be two countable sets. Define $A \times B = \{(a, b) : a \in A, b \in B\}$. Show that $A \times B$ is countable.

(b) Show that the set $\mathbb{N}^k = \{(a_1, a_2, ..., a_k) : a_i \in \mathbb{N}\ \forall i = 1, ..., k\}$ is countable.

(c) Let P_d be the set of integer co-efficient polynomials of degree at most d. Show that P_d is countable for some fixed d.

(d) Show that the set P of all integer coefficient polynomials of finite degree is countable. (Hint: Can you write P in terms of the sets P_d?)

(e) An algebraic number is a real number that can be written as the root of an integer coefficient polynomial. Show that the set of algebraic numbers is countable.

5. **Short Answer: Secret-Sharing (5 points)**

(a) In a secret-sharing scheme in $GF(p)$ where k is the minimum number of people required to recover the secret, is successful secret recovery more probable when $k-1$ people collaborate compared to random guessing? Explain your answer.

6. **Short Answer: Self-reference/Uncomputability (10 points)**

(a) Suppose you are given a program $\mathcal{P}$ which, if run forever, eventually prints every input to another program $\mathcal{Q}$ that halts in finite time. Does this exist? If so, describe the program. If not, expain why.

7. **Short Answer: Counting (3 points each)**

(a) Suppose we have a set of ordered items: $a_1 < a_2 < \ldots < a_n$.

i. How many sets have a contiguous set of items: a set where every element is either the minimum item, the maximum item, or for a given a_i, both a_{i-1} and a_{i+1} are in the set?

ii. Now suppose that an item $a_i, i \in \{1, \ldots, n\}$ must be included in each set. How many sets are there?

(b) How many permutations exist of the word "BERKELEY" with "BRK" appearing together, but not necessarily in that order?

(c) Determine:

i. The number of simple undirected (and possibly disconnected) graphs on n vertices, with the vertices labelled $1, 2, 3, ...n$. Justify your answer.

ii. The number of simple directed (and possibly disconnected) graph on n vertices, with the vertices labelled as above. Justify your answer.

8. **Short Answer: Probability (3 points each)**

(a) Suppose your local McChipotle's ice cream machine is broken on any given day with probability p, independent of other days. What is the probability that April 5th is the second day in April that the machine works?

(b) You have a coin that turns up heads with p probability and one that does so with q probability. You flip each one n times and you mark each pair of flips as a success if one of the two coins was heads. What is the expected number of successes?

(c) Jane is flipping coins!

i. First, Jane flips 9 fair coins. What is the probability that she gets an even number of heads? Justify your answer. *Hint: use a counting argument*

ii. Now Jane flips 10 coins. What is the probability that she gets an even number of heads? What about if she flips n coins? Justify your answers.

iii. Suppose Jane flips n **unfair** coins (where $P(H) \neq 1/2$), along with a single fair coin. What is the probability that she gets an even number of heads after flipping these $n+1$ coins? Justify your answer.

(d) Pick a random integer n in the range from 0 to 999,999 each with equal probability.

i. What is the probability that the decimal digits of n add up to 8?

ii. What is the probability that the decimal digits of n add up to 10?

(e) A particle sits on the real number line, starting at the origin (0). At each timestep, we flip a fair coin and move the particle as follows:

- If we see heads, we move the particle one unit to the left
- If we see tails, we move the particle one unit to the right

Let X_n be the position of the particle at time-step n, and assume $X_0 = 0$.

i. Find $P(X_{1000} = 0)$.

ii. What is the most likely position for the particle at time $t = 2k$, where k is a non-negative integer? *Hint: Think about the symmetry of Pascal's triangle.*

iii. In general, what is $P(X_n = 0|X_0 = 0)$ in terms of n?