CSM 70 Discrete Mathematics and Probability Theory

Spring 2016

Midterm 2 Review

I. Mod/Bijections/FLT/RSA

1. Finding Bijections

Which of the following functions are bijections from $\mathbf{Z}_8$ to $\mathbf{Z}_8$

a. f(x) = 3x

b. f(x) = 3x-2

c. f(x) = 4x

2. Mapping Mods

Why can't we have a surjection from $\mathbf{Z}_8$ to $\mathbf{Z}_{16}$? Why can't we have an injection from $\mathbf{Z}_8$ to $\mathbf{Z}_4$?

3. Mod Math

What is 3^{453} mod 11? What principle/theorem do you use to solve this?

4. **Really Secret Algebra**
   Alex is sending a message to Bob with RSA. If he uses the public key e = 7, N = 33, what is the value of d that Bob must use to decrypt the message?

5. **Three is Prime**
   If p and p^2+2 are prime, prove that p must be 3.

6. **Wilson's World**
   Prove Wilson's Theorem using Fermat's Little Theorem: Let p be a prime integer. Then $(p-1)! \equiv -1 \pmod{p}$.

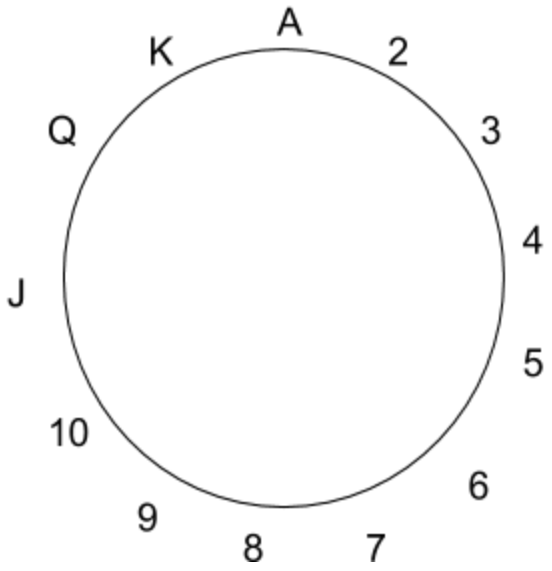
7. **Bijective Magic**

Let's learn a new card trick. You can perform this trick with an assistant, who asks a member of the audience to choose five cards while you face the other way. The assistant then places four of those cards face up on the table and one of them face down. You make a grand entrance and looking at the four cards on the table, correctly guess the one that is face down. How'd you do it?

There are two things you need to guess correctly: the suit and the denomination.
Let's start with the suit.

a. Say the five suits were H, D, H, S, C. Your assistant will place H, D, S, C on the table (in that order) and will place the other H face down. If the chosen cards were D, S, C, C, H your assistant will place C, D, S, H on the table (in that order) and will place the other C face down. Do you see the pattern? What mathematical principle is at play here? Write a strategy you and your assistant can use so that you will always know the suit of the hidden card.

Now we need to figure out how to guess the denomination.
Arrange the denominations in a circle.



We define smaller clockwise distance between denominations X and Y as the smallest of the following distances: from X to Y in the clockwise direction or Y to X in the clockwise direction.

b. What is the smaller clockwise distance between 8 and J? Between 3 and K?

c. What are all of the possible smaller clockwise distances? In other words, if I choose X and Y arbitrarily, what could the smaller clockwise distance be?

How can the assistant use this information to help you guess the hidden card? The assistant has two cards in the same suit. For now assume that the assistant has a secret way of telling you what the smaller clockwise distance between them is.

d. What card should the assistant hide and what card should they place face up on the table?

Now we need to somehow encode the smaller clockwise distance. Recall that the assistant places four cards face up. The one of the left tells us the suit and where to start counting. There are three other cards that the assistant can use to let you know what the smaller clockwise distance is.

e. How can the assistant use the suits and denominations of the other three cards to encode the information from part c?

II. Error Correcting Polynomials

1. Call Me On My Solomon Reed Phone

Alice wants to send Bob a message of length 2 in GF(7)over a noisy channel. She knows that at most 1 character will get corrupted when she sends her message. So, she pads her message with 2 extra characters before sending it. (Using standard interpolation-based 0-indexed Reed Solomon codes.)

This is what Bob receives: A A E G

What was Alice trying to tell him?

Note: Here, assume that letters correspond to numbers as follows:A=0, B=1, C=2, D=3, E=4, F=5, G=6

2. Can't Read This

Consider the alphabet A = 0, B = 1, C = 2, D = 3, E = 4. Suppose a message of length 3 is sent using the erasure error correction scheme over GF(5), with no more than one erasure. If you receive the following packets, what was the original message? The points are 1-indexed.

(a) C _ A A

(b) _ A C C

(c) C E _ C

3. **100% Successful Decoding Guaranteed**
   You would like to send a message of length n over a channel. You know that at most k packets may be dropped along the way, and of the packets that are not dropped, at most j may be corrupted. How many packets should you send to guarantee successful decoding? Why?

4. **Noise Channels**
   You would like to send a message of length $n > 0$ over a lossy channel that drops (erases) packets. If up to a fraction 1/4 of the total number of packets you send get erased, how many extra packets do you need to send (as a function of n)?

5. **Secret Polynomials**
   The code to open your secret club's treasure chest is 15. Your club has 4 other members, named John, Paul, George and Ringo. What information can you give each of them so that any 3 of them can discover that the secret is 15, but if only 2 of them share their information, they cannot discover the secret?

6. **Secret Groups**
   Consider the following variant of the secret sharing problem. We wish to share a secret among twenty-one people, divided into three groups of seven, so that the following condition is satisfied. A subset of the twenty-one people can recover the secret if and only if it contains majorities (at least four out of seven) of at least two of the groups. How would you modify the standard secret sharing scheme to achieve this condition?

7. **Polynomial Problem**
   Suppose p is a prime number, P(x) is a polynomial with degree d, and $0 < d < p/2$. Prove that there are less than $2d+1$ distinct values of x such that $P(x)^2 - P(x) + 1 \equiv 0 \pmod{p}$.

8. **Code Breaker**
   You are spiteful for having to study over Spring Break, and so you want to cut off secret communications between your course staff. For each message, what percentage of a message being sent would you have to corrupt to make that message unrecoverable no matter how many extra packets are sent?

III. Countability

1. Consider the set of all pairs of rational numbers: $T_1 = \{(x, y) \mid x,y \text{ rationals}\}$
   Is T_1 finite, countably infinite, or uncountably infinite? Explain.

2. Consider the set of pairs where $T_2 = \{(x,y) \mid x \text{ is a natural number, } y \text{ is a real number}\}$
   Is T_2 finite, countably infinite, or uncountably infinite? Explain.

3. Consider the set of pairs where $T_3 = \{(x,y) \mid x,y \text{ are bit strings of length } k\}$
   Is T_3 finite, countably infinite, or uncountably infinite? Explain.

4. Consider the set of triples where $T_4 = \{ (x,y,z) \mid x,y,x \text{ are rational numbers}\}$
   Is T_4 finite, countably infinite, or uncountably infinite? Explain.

5. Consider the set of lists of length k, for positive integer k, where $T_5 = \{(x_1, ..., x_k) \mid x_i \in S_i$ such that $S_i \neq \varnothing \}$
   If any of S are uncountably infinite, what is the cardinality of T_5?

   If all of S are finite, is T_5 finite, countably infinite, or uncountably infinite?

   If none of S are uncountably infinite and at least one is infinite, what is the cardinality of T_5?

IV. Counting

1. A professor designed his final exam as follows: There will be three sections in the exam. Each section has five questions. Students have to pick any two sections to answer, in any order. Within each section, they must choose any three questions. In how many possible ways can a student choose which questions to answer?

2. A committee of five people is to be chosen from a club that has ten scientists and eight engineers. How many ways can the committee be formed if it has to contain at least two scientists and at least one engineer?

3. How many five card hands have at least one card from each suit?

4. You've been hired by the local phone company. They're concerned, because all the local taxi companies have started demanding phone numbers made up of exactly 2 different digits. (For instance, "555-5556" and "811-1881" are acceptable, but "111-1111" and "123-4567" are not.) Your job is to help the phone company figure out how long they've got before they run out of acceptable phone numbers. How many 7-digit numbers are there that contain exactly 2 different digits?

5. How many triangles does a complete graph with n nodes have?

6. How many different sequences of the numbers {0,1,2} of length 10 do not contain any of the subsequences 12, 23, or 31? 3222132111 is such a sequence.

7. A decimal number is called “increasing” if each digit is nonzero and is greater than the previous one (e.g. 24589 is one). How many 5 digit increasing numbers are there?

8. How many license plates with 3 digits followed by 3 letters do not contain both the number 0 and the letter O?

9. How many different even integers ≥ 4000 and < 7000 have four different digits?

10. A deck of forty cards consists of four 1's, four 2's, …, and four 10's. One matching pair of cards is removed from the deck. Two cards are now drawn at random from the deck. What is the probability they form a pair?

11. Ten points are marked on a circle. How many distinct convex polygons can be drawn using some (or all) of the ten points as vertices?

12. Plain Jane has 5 identical narrow rings that she likes to wear. She can wear them on any of her 8 fingers (but not her thumbs), and they are narrow enough that she can fit all 5 on one finger if she chooses to. How many different ways can Jane wear her rings? (note that Jane's rings may be plain, but she can tell her fingers apart). If she puts at most one ring on each finger, how many ways are there for her to wear her rings? Suppose Jane is tired of being plain and paints her rings five different colors so she can tell them apart. How does this change your answers above?

V. Halting

Undecidability Here we use reductions to prove that certain problems are undecidable.
1. The totality problem is defined as follows: A program F is said to be total if F(x) is defined for all x. Assume there exists a procedure TOTAL that takes an input program P and outputs 'Yes' if P halts on all inputs and 'No' otherwise. Argue that this means we could solve the halting problem.

2. What does this mean about our assumption that TOTAL exists? Is the totality problem decidable?

3. The equivalence problem is defined as follows: Given two programs P and Q, do they compute the same function? (is $P(x) = Q(x)$ for all x?). Prove that the equivalence problem is undecidable by reducing the totality problem to it. In other words, show that you can solve the totality problem using the equivalence problem.

VI. Probability

1. Probably 61A

You want to teach 61A! You will apply for some position every semester after taking the class. Once you have first finished the class, you have an 80% chance to be hired as a Lab Assistant, a 10% chance of being hired as a Tutor, and a 10% chance of being hired as a TA. Once you have been a Lab Assistant, you have a 30% chance of being rehired as a Lab Assistant, a 50% chance of being hired as a Tutor, and a 20% chance of being hired as a TA. Once you have been a Tutor, you have a 60% chance of being rehired as a Tutor, and a 40% chance of being hired as a TA. TAs are guaranteed to stay TAs forever when they are hired.

a. What is the chance of being a reader on your second semester after finishing the class? (So you were either a Lab Assistant or a Tutor for one semester already)

b. What is the chance that you stay a Lab Assistant for all 7 semesters after taking the class?

c. Given you were hired as a Lab Assistant the first semester after taking the class, what is the chance that you stay a Tutor for all 6 remaining semesters?

d. What is the chance that you are hired as a Tutor exactly 3 times in 5 semesters?

e. What is your chance of being a TA at least once in your first 3 semesters?

2. Independent Dice

Consider rolling 2 normal 6-sided dice. Let A be the event that the first die comes up as an odd number. Let B be the event that the second die comes up as an odd number. Let C be the event that the sum of the dice values is odd. Intuitively, are A,B,C pairwise independent? That is, are any pair of these events independent? What are the probabilities of each event? Of each pair?

3. Mutually Independent Dice

Continuing from Part 2, are the events A,B,C mutually independent? In other words, is each one independent from the other two? What is the probability of all 3 of them happening together?

VII. Combinatorial Proofs

Use a combinatorial argument to prove the following identities.

1. $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$

2. $1+2+\cdots+n = \frac{n(n+1)}{2}$

3. Hockey Stick (from Worksheet 8)

   a. Prove the Hockey Stick Theorem:

$$\sum_{t=k}^{n} \binom{t}{k} = \binom{n+1}{k+1}$$ where n, t are natural numbers and $n > t$

   Use a combinatorial argument!

b. Let S be the set {1, 2, 3, … 2015}. Look at all 1000 element subsets of S. Find the average of all smallest elements of the subsets.

VIII. Random Var./Distributions/Expectations/Collisions

1. The Life of Die

Consider a single roll of two dice, one red and one blue.

(a) Let R be the value of the red die. What is the distribution of R? What is the expectation of R?

(b) Let M be the maximum of the numbers on the two dice. What is the distribution of M? What is the expectation of M?

2. **Hashbrown tables**
   Let there by a hashtable of size N. If k items are hashed, what is the expected number of collisions?