MT2 Practice

This worksheet contains problems for every section covered on your midterm 2. Vivek and Alvin wrote these problems from scratch, keeping in mind what has and has not been covered this Fall 2016 semester.

- Modular Arithmetic
- Bijections and RSA
- Polynomials
- Error Correcting Codes
- Infinity and Uncountability
- Self-Reference and Uncomputability
- Counting
- Introduction to Discrete Probability
- Conditional Probability

Note that problems here were designed to challenge you and to exercise your knowledge of these topics. In some cases, several topics were drawn upon to create the question. We recommend selectively working on topics where you feel weakest.

The concentration of questions in this review do not correspond to the concentration of questions on the exam.

1. **Piazza**

   Between the CS70 and CS170 piazzas, if there are exactly 8 unresolved questions total, Sinho will resolve all of them (This means there can never be more than 8 unresolved questions). Let us pretend that Sinho can resolve questions instantaneously and he does not tend to Piazza if there are fewer than 8 unresolved questions. Sinho tells you that there are a total of 3 unresolved questions.

   (a) Is it possible for CS70 to have as many unresolved posts as CS170?

   (b) Is it possible for CS170 to have twice as many unresolved posts as CS70?

2. **Random Uniqueness**

   Consider the following scenarios, where we apply probability to polynomials. We generate a new polynomial Q in GF(7), by randomly picking 6 numbers in (mod 7), for a polynomial of the form.

$$a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

The first number we pick is a_5, the second number is a_4 etc.

(a) What is the probability that the polynomial has degree at least 4?

(b) What is probability we have a unique polynomial of degree less than 4?

(c) Now, consider only degree 5 polynomials that were randomly generated using the scheme described above. What is the probability that the sum of its coefficients is equal to 6?

3. **Maybe Lossy Maybe Not**

Let us say that Alice would like to send a message to Bob, over some channel. Alice has a message of length 4 and sends 5 packets.

(a) Packets are dropped with probability p. What is probability that Bob can successfully reconstruct Alice's message?

(b) Again, packets can be dropped with probability p. The channel may additionally corrupt 1 packet. Alice realizes this and sends 3 additional packets. What is the probability that Bob receives enough packets to successfully reconstruct Alice's message?

(c) Again, packets can be dropped with probability p. This time, packets may be corrupted with probability q. Consider the original scenario where Alice sends 5 packets for a message of length 4. What is probability that Bob can successfully reconstruct Alice's message?

4. **Hilbert's Paradox of the Grand Hotel**

Consider a magical hotel with a countably infinite number of rooms numbered according to the natural numbers where all the rooms are currently occupied. Assume guests don't mind being moved out of their current room as long as they can get to their new room in a finite amount of time.

(a) Suppose one new guest arrived in their car, how would you shuffle guests around to accommodate them? What if k guests arrived, where k is a constant positive integer?

(b) Suppose a countably infinite number of guests arrived in an infinite length bus with seat numbers according to the natural numbers, how would you accommodate them?

(c) Suppose a countably infinite number of infinite length buses arrive carrying countably infinite guests each, how would you accommodate them? (Hint: There are infinitely many prime numbers)

5. **Impossible Programs**

Show that none of the following programs can exist.

(a) Consider a program P that takes in any program F, input x and output y and returns true if $F(x)$ outputs y and returns false otherwise.

(b) Consider a program P that takes in any program F and returns true if $F(F)$ halts and returns false if it doesn't halt.

(c) Consider a program P that takes in any programs F and G and returns true if F and G halt on all the same inputs and returns false otherwise.

6. **Kolmogorov Complexity**
Compression of a bit string x of length n involves creating a program shorter than n bits that returns x. The Kolmogorov complexity of a string $K(x)$ is the length of shortest program that returns x (i.e. the length of a maximally compressed version of x).

(a) Explain why "the smallest positive integer not definable in under 100 characters" is paradoxical.

(b) Prove that for any length n, there must be at least one bit string that cannot be compressed.

(c) Imagine you had the program K, which outputs the Kolmogorov complexity of string. Design a program P that when given integer n outputs the bit string of length n with the highest Kolmogorov complexity. If there are multiple strings with the highest complexity, output the lexicographically first (i.e. the one that would come first in a dictionary).

(d) Suppose the program P you just wrote can be written in m bits. Show that P and by extension, K, cannot exist, for a sufficiently large input n.

(e) Consider the program I, which can be written in m bits, that when given any input string x returns true if x is incompressible and returns false otherwise. Show that such a program cannot exist.

7. **Binomial Theorem**
The binomial theorem states the following:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Prove this theorem using a combinatorial proof.

8. **Crazy Balls and Bins**
Imagine you had 5 distinct bins and randomly threw 7 identical balls into the bins with uniform probability.

(a) What is likelihood that the first bin has at least 3 balls in it?

(b) What is likelihood that the first bin has exactly 3 balls in it?

(c) What is likelihood that at least one bin has exactly 3 balls in it?

(d) What is likelihood that the at least one bin has at least 3 balls in it?

9. **Teams and Leaders**
Prove the following identities using a combinatorial proof.

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

(b) $\sum_{k=1}^{n} k\binom{n}{k}^2 = n\binom{2n-1}{n-1}$

10. **Finicky Bins**

If a bin has at least 5 balls in a bin, the 5 balls will fall out and not be counted (e.g., 6 balls in a bin is the same as 1). Compute the number of ways to distribute 7 indistinguishable balls among 4 bins.

11. **Bag of Coins**

Your friend Forest has a bag of n coins. You know that k are biased with probability p (i.e., These coins have probability p of being heads). Let F be the event that Forest picks a fair coin, and let B be the event that Forest picks a biased coin.. Forest draws three coins from the bag, but he does not know which are biased and which are fair.

(a) What is the probability of FFH?

(b) What is the probability of picking at least two fair coins?

(c) Given that Forest flips the second coin and sees heads, what is the probability that this coin is biased?