CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

MT2 Review

1 RSA for Your Midterm Score

Alice wants to tell Bob her midterm score, m, which is an integer between 0 and 100 inclusive. She wants to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know Alice's midterm score.

(a) Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's midterm score is. How did she do it?

(b) Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm, encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r. How can she figure out m?

2 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.

1. 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?
2. 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?
3. 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.)

3 Computability

Decide whether the following statements are true or false. Please justify your answers.

(a) The problem of determining whether a program halts in time 2^{n^2} on an input of size n is undecidable.

(b) There is no computer program `Line` which takes a program P, an input x, and a line number L, and determines whether the L^{th} line of code is executed when the program P is run on the input x.

4 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.

5 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.

6 Box of Marbles

You are given two boxes: one of them containing 900 red marbles and 100 blue marbles, the other one contains 500 red marbles and 500 blue marbles.

1. If we pick one of the boxes randomly, and pick a marble what is the probability that it is blue?
2. If we see that the marble is blue, what is the probability that it is chosen from box 1?
3. Suppose we pick one marble from box 1 and without looking at its color we put it aside. Then we pick another marble from box 1. What is the probability that the second marble is blue?

7 Diversify Your Hand

You are dealt 13 cards from a standard 52 card deck. Let X be the number of distinct values in your hand (The 13 possible values are Ace, 2, 3, 4, ..., Jack, Queen, King). For instance, the hand (A, A, A, 2, 3, 4, 4, 5, 7, 9, 10, J, J) has 9 distinct values.

Calculate $E[X]$.