DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, IIT ROPAR

Tutorial-1

CSL-471, Probability and Computing

Dr. S. R. S. Iyengar

September 5, 2016

1 INSTRUCTIONS

1. This tutorial sheet consists of two parts- i) Instructor picked questions. ii) TA picked questions. You are requested to attempt both the parts.
2. The tutorial will be discussed in the class on August 11, 15:20 - 16:10 and 17:10- 18:00 hrs.
3. In case of any doubt or clarification wrt any question, please open a thread on the google group csl471@iitrpr.ac.in and initiate a discusison.

2 INSTRUCTOR'S PICK

1. Obtain the closed form for the following expression

$$1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$$

(Rating : ***)

2. Assume a HR officer is to appoint a secretary for the Managing Director of the company. There are n number of applicants. The officer follows the following procedure:

   - Pick the first candidate from the applicants' queue (Please note that the applicants are randomly placed in the queue and are not sorted according to some criterion).
   - Hire this candidate and then interview the second applicant. If this applicant is no better than the currently hired secretary, she is ignored. But, if the next applicant is better than the current secretary, she is hired and the current secretary is fired.
   - In this way, the officer keeps interviewing all the prospective secretaries in queue, firing the current secretary on seeing a better option (Do you notice that in this scenario, the company will end up hiring the best candidate by the end of the queue).

   Find out the expected number of firings if one follows this procedure.

   (Rating : **)

3. During the world war II, the western allies wanted to estimate the number of tanks possessed by the German army. The tanks produced by the Germans were marked with consecutive numbers starting from 1 to n. The alias captured some of these German tanks and noted these numbers. The problem was to estimate the number n of actual tanks Germans possessed by looking at the sample of the passing by tanks.

   Simply stated in another form: Martha has n numbers, she gives you k of these numbers uniformly at random, without repetitions. By looking at these k numbers, can you find the expected value of n?

   We discussed a simple solution to this problem in the class. If the maximum of these n numbers happens to be a_k , we have proved that $E[a_k] = \frac{k}{k+1}(n+1)$.

   What is the standard deviation of a_k, i.e. $\sigma(a_k)$?

(Rating : Exp)

4. Recall the online hiring/ dating problem. The solution involves one to look at the first k candidates, reject all of them, while keeping a note of the best one from 1 to k. As soon as we find a person after $k+1$ who is better than the best seen between 1 and k, we hire this person and terminate the algorithm. We proved that the ideal k is $\frac{n}{e}$. This approach expects one to know the number of candidates n in advance. Give an algorithm to execute online hiring if the number of candidates n is not known in advance.

(Rating : *)

5. In the Monty Hall problem, there were 2 goats and 1 BMW car. Assume, there are k doors hiding goats and 1 door with the BMW car. We use the same strategy to play, i.e. swapping after seeing a door with a goat. What is the probability of us winning the BMW?

(Rating : *)

6. Consider a language having a large number of alphabets (By large number, we mean in the order of millions). Say $L = a_1, a_2, a_3, ...a_n$. Let probability of occurrence of an alphabet a_i, $pr(occurrence\ of\ a_i) = \frac{1}{2^i}$. If we randomly pick two alphabets from a very big book written with this alphabet set L (obeying the above mentioned frequency distribution), what is the probability that both given two random letters in the book are the same (In other words, what is the probability of a collision)?

(Rating : **)

7. Consider a variant to the above question. If instead of two alphabets, we pick 3 alphabets uniformly at random, what is the probability that all these three alphabets are the same?

(Rating : *)

8. Given a binary string of length n, what is the expected length of the longest streak of 0s that one can see?

(Rating : 3*)

9. a) What is the expected number of steps in an online hiring problem?
   b) What is the probability that a boy playing the game gets the a) The best girl b) Second best girl c) Third best girl

(Rating : 2*)

10. If a and n are relatively prime, then prove that $a, 2a, 3a.....(n-1)a$, are all distinct.

(Rating : 3*)

11. Assuming you have a function which gives you random numbers from 1 to n, devise an efficient algorithm to permute an array containing k elements.

(RAting : **)

12. In the one time pad algorithm discussed in the class, the key length was considered equal to the length of the plain text. Assume that the key length is $n/2$ where n is the length of the plaintext and we replicate the key twice to encrypt the plain text. Is this perfectly secure?

(Rating : **)

13. Consider the k-permutation cipher. Given a plain text, $p_1, p_2, p_3, p_4, p_5, p_6, ..., p_n$ of length n. We divide the plain text in blocks of size k. While encrypting, every block is permuted randomly.

    Assume $k = 4$ in the below example.

    Plain text : $p_1, p_2, p_3, p_4, |p_5, p_6, p_7, p_8, |.....|p_{n-3}, p_{n-2}, p_{n-1}, p_n$

    Cipher text: $p_3, p_1, p_4, p_2, |p_8, p_7, p_5, p_6, |.....|p_{n-1}, pn-3, p_{n-2}, p_n$

    Prove that this cipher is not perfectly secure.

(Rating : **)

3 TA PICKED QUESTIONS

1. Consider a game, where you throw a fair die. If you get a number from 1 to 5, you get the number of $ = The number that comes on the die. If die shows 6, you get 6 more $ and end the game. What is the expected amount of money you win? Also find the standard deviation.

(Rating : 2*)

2. A die is rolled and a coin is tossed alternately. If the coin shows head, the die throw continues else stops. What is the expected sum of the numbers which have appeared on die throughout the game? Also find the standard deviation. Assume the die as well as the coin to be unbiased.

(Rating : 2*)

3. Consider Caesar cipher. We know that it is breakable in a maximum of 26 attempts. Can one cipher text in the caesar cipher have 2 plain texts corresponding to it? What is the probability of this happening.

(Rating : 2*)

4. Answer the above question for substitution cipher.

(Rating : 3*)