Solutions to Tutorial-1

CSL-471 (Probability and Computing)

September 5, 2016

1 Solution:

Consider Figure 1

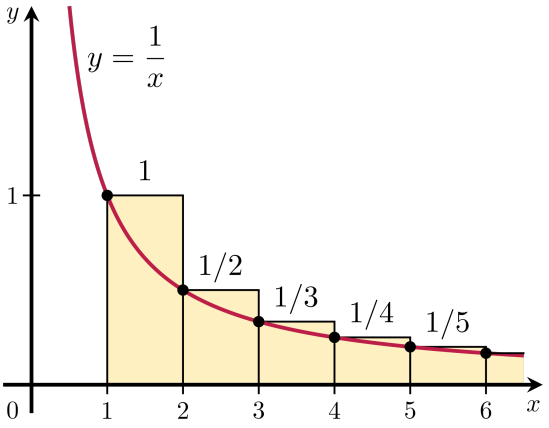

Figure 1: $f(x) = 1/x$

$$f(x) = \frac{1}{x}$$

$$\int_1^n \frac{1}{x} > \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ... + \frac{1}{n}$$

Again, from Figure 1,

$$\int_1^n \frac{1}{x} < 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ... + \frac{1}{n} \; = \; \alpha$$

say

$$\int_1^n \frac{1}{x} = |logx|_1^n = \log_e n - \log_e 1 = log_e n$$

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

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

So,

$$\alpha - 1 < \log n < \alpha$$

So, $\log n \approx \alpha$ (We can say, it can be calculated exactly also.)

Hence, $1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} = \mathcal{O}(\log_e n)$

2 Solution:

Let the expected number of firings be X. Also let X_i be indicator random variables.
$X_i = 1$ if the i_{th} person results in a firing of the already hired person, else 0.

$E[X_i]$=$P(X_i = 1)$

=$\frac{i}{i+1}(n+1)$

$E[X] = E[X_1] + E[X_2] + .. + E[X_n]$

=$\sum_{i=1}^{n} P(X_i = 1)$

=$\sum_{i=1}^{n} \frac{i}{i+1}(n+1) = \log n$

3 Solution:

$$\mathrm{E}[a_k\ ]=\frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} \binom{\alpha}{k}$$

Then we used a very interesting property to solve it.
$\sum_{\alpha=k}^{n} \binom{\alpha}{k} = \binom{n+1}{k+1}$

And got the following

$$\frac{k}{\binom{n}{k}} \times \binom{n+1}{k+1}$$

Let us look at the case of calculating standard deviation

$\sigma[a_k\ ]=\sum_{\alpha=k}^{n} \alpha^2\ \frac{\binom{\alpha-1}{k-1}}{\binom{n}{k}}$

$= \frac{1}{\binom{n}{k}} \sum_{\alpha=k}^{n} \alpha^2 \frac{(\alpha-1)!}{(k-1)!\times(\alpha-k)!}$

$=\frac{1}{\binom{n}{k}} \sum_{\alpha=k}^{n} \alpha^2 \times k \frac{(\alpha-1)!}{k\times(k-1)!\times(\alpha-k)!}$

$=\frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} \alpha \frac{\alpha!}{(\alpha-k)!k!}$

We play a small trick here

$=\frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} (\alpha+1-1) \frac{\alpha!}{(\alpha-k)!k!}$

$=\frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} (\alpha+1) \frac{\alpha!}{(\alpha-k)!k!} - \frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} \frac{\alpha!}{(\alpha-k)!k!}$

$=\frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} (\alpha+1) \frac{\alpha!}{(\alpha-k)!k!} \times \frac{k+1}{k+1} - \frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} \frac{\alpha!}{(\alpha-k)!k!}$

$=\frac{k(k+1)}{\binom{n}{k}} \sum_{\alpha=k}^{n} \frac{(\alpha+1)!}{(\alpha-k)!(k+1)!} - \frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} \frac{\alpha!}{(\alpha-k)!k!}$

$=\frac{k(k+1)}{\binom{n}{k}} \sum_{\alpha=k}^{n} \binom{\alpha+1}{k+1} - \frac{k}{\binom{n}{k}} \sum_{\alpha=k}^{n} \binom{\alpha}{k}$

Now we can use the property $\sum_{\alpha=k}^{n} \binom{\alpha}{k} = \binom{n+1}{k+1}$ to solve both the summations.

4 Solution:

When we do not know the total number of candidates, we can look at the starting few candidates and predict the number of candidates with the help of the german tank problem.

5 Solution:

$P(Success) = \frac{k}{k+1} \times \frac{1}{k-1}$
$=\frac{k}{k^2-1}$

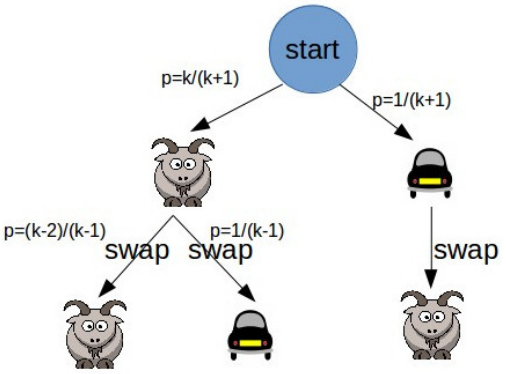

Figure 2: Modified Monty-Hall Problem

$P(Failure) = \frac{k}{k+1} \times \frac{k-2}{k-1} + \frac{1}{k+1}$
$= \frac{k^2-2k+k-1}{k^2-1}$
$= \frac{k^2-k-1}{k^2-1}$

6 Solution:

As we have seen in lecture 3 (cryptanalysis of Vigenere Cipher),

If the given text was to be random, instead of the massive text from English(or some other language), then all the f_is would be the same. In that case if we pick two letters from S, probability that they are same = $\sum_{i=1}^{L} {f_i}^2$

Given $f_i = \frac{1}{2^i}$

Hence, P(collision) = $\sum_{i=1}^{\infty} \frac{1}{2^{2i}}$

$= \frac{1}{2^2} + \frac{1}{2^4} + \frac{1}{2^6} + ...$

$= \frac{\frac{1}{2^2}}{1-\frac{1}{2^2}}$

$= \frac{1}{4} \times \frac{4}{3}$

$= \frac{1}{3}$

7 Solution:

As in the previous question,
$\sum_{i=1}^{L} {f_i}^3$

Given $f_i = \frac{1}{2^1}$

Hence, P(collision) = $\sum_{i=1}^{\infty} \frac{1}{2^{3i}}$

$= \frac{1}{2^3} + \frac{1}{2^6} + \frac{1}{2^9} + ...$

$= \frac{\frac{1}{2^2}}{1-\frac{1}{2^3}}$

$= \frac{1}{4} \times \frac{8}{7}$

$= \frac{2}{7}$

8 Solution:

Done in the class room, surf lecture notes.

9 Solution:

1. **Expected Number of steps in online hiring:**
   Let X be a random variable which represents the number of steps taken by the online hiring algorithm.
   In online hiring algorithm, we look for the first k boys, look at the best among them, and then look for the better than the best in rest of the candidates.
   We have seen in class that $k = n/e$.

   We know X can take values {k+1, k+2, ..., k+n-1, n}

   $E[X] = \sum_{i=1}^{n-k} i \times P(X = k + i)$

   For all the values of i, other than $n - k$, we have the following

   $P(X = k + i) = P$(Best boy from the locations 1 to $k + i - 1$ lie in the locations 1 to k and the boy at the location $k + i$ is better than all the boys seen before). It is because only in these conditions, this boy will be chosen and the algorithm will end in exactly $k + i$ steps.

$P(X = k + i) = \frac{k}{k+i-1} \times \frac{1}{k+i}$ ..... (1)

When $i = n - k$, i.e. the algorithm takes n steps:
Algorithm will take n steps in two cases: 1. When the boy at the location n is the best in the boys from locations 1 to n 2. When the best boy is in the first k locations.

$P(X = n) = (\frac{k}{n-1} \times \frac{1}{n}) + \frac{k}{n}$ .....(2)

Put in the formula for expected value and get the answer.

2. Probability of choosing second best boy = Probability of choosing 3rd best boy = Probability of choosing best boy = $\frac{k}{n}(\log n - \log k)$ and follows the same analysis as done in the class.

10 Solution:

11 Solution:

Algorithm:

1. Take first element in the array, swap it with an element randomly selected from the array. The place of the first element is fixed.
2. Take second element and swap it with the randomly selected element from the remaining $n - 1$ elements (since first element has been fixed).
3. Similarly, the i_{th} element is swapped with the randomly selected element from the remaining $n - i + 1$ elements.
4. Repeat the same process for all the elements.

Time Complexity : O(n), assuming that the random function takes O(1) time.

Proof that it is a random permutation:

P(a random permutation in n elements) = $\frac{1}{n!}$

Take a random permutation $i_1, i_2, ..., i_n$
P(i_1 is at the first position)= $\frac{1}{n}$, since this element was chosen uniformly at random and swapped with the first element.

P(i_2 is at the first position)= $\frac{1}{n-1}$, since this element was chosen uniformly at random from the $n - 1$ elements and swapped with the second element.

P(i_k is at the first position)= $\frac{1}{n-k+1}$, since this element was chosen uniformly at random from the $n-1$ elements and swapped with the second element.

P(This permutation) = $\frac{1}{n} \times \frac{1}{n-1} \times \frac{1}{n-2} \times ..... \times \frac{1}{n-(n+1)}$

= $\frac{1}{n!}$, which is same as randomly choosing one permutation out of the total $n!$ permutations

12 Solution:

If the key length = $n/2$, then the number of possible plaintexts corresponding to a given ciphertext= $2^{n/2}$.
In a perfectly secure encryption, the number of plaintexts possible should have been 2^n.

13 Solution:

In permutation cipher, number of plaintext corresponding to a given cipher text = $k!$, which is very less. Hence, it is not perfectly secure.