CSCI 5454: Algorithms: Homework 4

Ashutosh Gandhi

March 8, 2023

Problem 1

1.1 Part A

The probability of Alice winning would be the sum of
- Alice gets heads in the 1st toss
- Alice gets tails, Bob gets heads, Alice gets heads on 3 tosses
- Alice gets tails, Bob gets heads, Alice gets tails, Bob gets heads, Alice gets heads on 5 tosses and so on. Thus we get the equation

$P = 1/2 + 1/2 * 1/2 * 1/2 + 1/2 * 1/2 * 1/2 * 1/2 * 1/2 + ...$
$P = 1/2 + 1/2^3 + 1/2^5 + ... --> ①$
$4P = 2 + 1/2 + 1/2^3 + 1/2^5 ...... --> ②$
subtracting ② - ① we get
$3P = 2$ # All other terms cancel out each other
$P = 2/3$
The probability that Alice wins is 2/3

Let X denote a random variable representing the number of tosses until a player wins.
Then $E(X) = E(X_1 + X_2 + X_3 + ...)$
X_1 represents tossing 1 coin, X_2 2 coin tosses
$E(X) = E(X_1) + E(X_2) + E(X_3) + ...)$
$E(X) = 1*(1/2)+2*(1/2^2)+3*(1/2^3)+4*(1/2^4)+....--> ①$ $E(X) = \sum xP(X = x)$
For one toss Alice gets head, for 2 tosses Alice gets tails and Bob gets tails,
for 3 tosses Alice gets tails, Bob gets heads, Alice gets heads
$(1/2)E(X) = 1/2^2 + 2/2^3 + 3/2^4 + ...-> ②$
subtracting ① - ② we get
$(1/2)E(X) = 1/2 + 1/2^2 + 1/2^3 + 1/2^4 + ...$
This is an infinite GP with a=1/2 and r=1/2 so sum=a/1-r
$(1/2)E(X) = (1/2)/(1 - 1/2)$
$(1/2)E(X) = 1$
$E(X) = 2$
The expected number of coin tosses is 2

1.2 Part B

Consider a game G1 such that:

- Alice tosses a coin, if it is head Alice wins, else bob gets a turn
- Bob tosses a coin, if it is tails Bob wins, else
- Alice wins

The probability of Bob winning in G1 is Alice getting a tail and then Bob getting a tail $P = 1/2 * 1/2 = 1/4$

Consider a game G2 such that:

- Toss 5 coins, If all 5 are tails then Bob wins, else Alice wins

The probability of Bob winning in G2 is if all the coin tosses flip as tails. $P = 1/32$

Next, consider the composite game:

- Toss 2 coins, If they are both tails then Bob wins, if they are both heads then play the game G1, else play the game G2.

The probability of Bob winning the composite game is, he either gets 2 tails or wins at game G1 or wins at game G2.
$P = 1/4 + (1/4 * 1/4) + (1/2 * 1/32)$
$P = 1/4 + 1/16 + 1/64$
$P = (16 + 4 + 1)/64$
$P = 21/64$

2.1 Part A

Considering the 3 separate cases for 1, n, and 2....n-1

- For 1 to be a leaf node, the element just right to 1 should be picked first.
Proving this by contradiction: in case, 1 was picked before 2 then 2 would definitely be the right child of 1, so 2 must be picked before 1. Next, if any other $k > 2$ is picked it would always go in the right sub-tree of 2 leaving only 1 in the left sub-tree.
Using the probability formula in the question with i=2 and j=1 (2 being chosen before 1 and being its ancestor) we get the probability that 1 is a leaf node as $1/((2-1)+1) = 1/2$

- For n to be a leaf node, the element just left to n should be picked first.
Proving this by contradiction: in case, n is picked first and later n-1 is picked the n-1 would be in the left child of n, so n-1 must be picked before n. Next, if any $k < n-1$ is picked it would go in the left sub-tree of n-1 leaving the right sub-tree with only n.
Using the probability formula in the question with i=n-1 and j=n then we get the probability

that n is a leaf node is $1/(n-(n-1)+1) = 1/2$

- For any element k in [2, n-1], k can only be a leaf node if it is picked after both its left and right neighbors are picked.
Proving this by contradiction: in case, k is picked before k-1 then k-1 and any other element less than k-1 till 1 can go in the left sub-tree of k, moreover, any remaining element k+1 to n would go in its right sub-tree. Similarly, if k is picked before k+1 then k+1 and any element more than k+1 till n can go to the right sub-tree of k, moreover, any remaining element k-1 to 1 would go into its left sub-tree. So for k to be a leaf node it has to be picked only after k+1 and k-1 are picked.
So out of k-1, k, k+1 we have 6 possible ways of picking them, out of which only 2 have k being selected after k-1 and k+1. So the probability would be 2/6 or 1/3.

2.2 Part B

Let X denote an indicator variable which takes the value 1 if node i is a leaf node or 0 if i is not a leaf node
number of leaf nodes = $\sum_{i=1}^{n}$[i is a leaf node]
Excepted number of leaf nodes E(X) = $\sum_{i=1}^{n} P$(i is a leaf node)
$E(X) = 1/2 + \sum_{2}^{n-1} 1/3 + 1/2$ (from 2a P(x=1,n)=1/2 and P(x=2...n-1)=1/3)
$E(X) = 1 + ((n-2)/3)$
$E(X) = (n+1)/3$

Thus the expected number of leaf nodes is (n+1)/3

3.1 Part A

To have $Hx = Hy$ we can say $Hx \oplus Hy = 0$ based on the $\oplus$ truth table.
or $H.(x \oplus y) = 0$
Since it is given that x and y only differ in i^{th} bit, $x \oplus y$ would be 0 for all the bits in x and y except the i^{th} bit which would be 1.
The n bit $x \oplus y$ would be multiplied with the m*n H matrix. So the i^{th} bit in $x \oplus y$ is multiplied with the i^{th} column in H. So if we have the i^{th} column in H as all 0, then the Boolean matrix multiplication would also be all 0, since $0\&1 = 0$, $0\&0 = 0$ and $0 \oplus 0 = 0$

Thus, the condition to have $Hx = Hy$ with the i^{th} bit differing in x and y, is to have the i^{th} column in H be all zeros.

3.2 Part B

To have the 2 keys x and y collide for a random matrix H we need to have $Hx = Hy$ or $H.(x \oplus y) = 0$

$x \oplus y$ would be a vector of zeros except at the bits where x and y are different. Now to get $H.(x \oplus y) = 0$ the XOR of those columns(the bits where x and y differ) in H must be 0. For example, let $V_6, V_8, V_{13}, V_{19}, V_{45}$ be some 5 columns in the matrix H and 6,8,13,19 and 45 be the bits at which x and y differ, then $V_6 \oplus V_8 \oplus V_{13} \oplus V_{19} \oplus V_{45}$ is a m bit vector of zeros. $V_6, V_8, V_{13}, V_{19}, V_{45}$ is m bit vector/columns in H and let b denote the bit in the 1st row of each of these vectors, then the probability of $b_6 \oplus b_8 \oplus b_{13} \oplus b_{19} \oplus b_{45} = 0$ being would be 1/2, in fact, for any k such additions it would 1/2.

To prove $P(b_1 \oplus b_2 \oplus b_3 \oplus ..... \oplus b_k = 0) = 1/2$.
If we fix k-1 bits then they would all, either XOR to a 0 or 1, and the k^{th} bit would also be either 0 or 1. So both of them would match at 2 out of the 4 possible outcomes and at those 2 matches the XOR would be 0. Thus the probability of getting the above XOR sum to 0 is 1/2.

Since The matrix H is of dimension m*n we would be doing the above XOR operation for each of the m rows, and the probability for each row having an XOR sum of 0 is 1/2. So the overall probability of having $H.(x \oplus y) = 0$ is $(1/2)^m$.

Thus to have a collision of keys x and y the condition $H.(x \oplus y) = 0$ must be true and the probability of that happening is $1/2^m$ as proved above.