Assignment 1

2023-12675 박지호

EXERCISE 1.4

- Let A and B the name of the contestants
- Without loss of generallity, assume A wins the match
- In order B to have won k games when the match is over, a total of $n + k$ games must have been played
  - Within the first $n + k - 1$ games, A must have won $n - 1$ games, and B must have won k games
  - Also, A must have won the final game
  - The probability of this happening is $\binom{n+k-1}{k} \times \left(\frac{1}{2}\right)^{n+k}$
- We need to double this probability in order to account for cases that B wins
- The answer: $\binom{n+k-1}{k} \times \left(\frac{1}{2}\right)^{n+k-1}$

EXERCISE 1.6

- Let $a_{m,k}$ be the probability that there are k white balls in the bin once there are m total balls in the bin.
  - $\forall m, a_{m,0} = a_{m,m} = 0, a_{2,1} = 1$
  - $\forall k$ such that $1 \leq k, a_{m,k} = a_{m-1,k} \times \frac{m-1-k}{m-1} + a_{m-1,k-1} \times \frac{k-1}{m-1}$
- Proposition: $\forall k$ such that $1 \leq k \leq m - 1, a_{m,k} = \frac{1}{m-1}$
  - Proposition holds for $m = 2$
    - $a_{2,1} = \frac{1}{2-1}$
  - If the proposition holds for $m - 1$
    - $\forall k$ such that $2 \leq k \leq m - 2$
      - $$\begin{aligned} a_{m,k} &= a_{m-1,k} \times \frac{m-1-k}{m-1} + a_{m-1,k-1} \times \frac{k-1}{m-1} \\ &= \frac{1}{m-2} \times \frac{m-1-k}{m-1} + \frac{1}{m-2} \times \frac{k-1}{m-1} \\ &= \frac{1}{m-2} \times \frac{m-2}{m-1} = \frac{1}{m-1} \end{aligned}$$
    - $$\begin{aligned} a_{m,1} &= a_{m-1,1} \times \frac{m-2}{m-1} + a_{m-1,0} \times \frac{0}{m-1} \\ &= \frac{1}{m-2} \times \frac{m-2}{m-1} = \frac{1}{m-1} \end{aligned}$$
    - $$\begin{aligned} a_{m,m-1} &= a_{m-1,m-1} \times \frac{0}{m-1} + a_{m-1,m-2} \times \frac{m-2}{m-1} \\ &= \frac{1}{m-2} \times \frac{m-2}{m-1} = \frac{1}{m-1} \end{aligned}$$
    - The proposition holds for m

- By mathematical induction, the proposition holds for all m
- $\forall k$ such that $1 \leq k \leq n-1, a_{n,k} = \frac{1}{n-1}$
- Once there are n total balls in the bin, the number of white balls is equally likely to be any number between 1 and $n-1$

EXERCISE 1.8

- Let the event where the chosen number is divisible by k be E_k
- $$\begin{aligned}\Pr(E_4 \cup E_6 \cup E_9) &= \Pr(E_4) + \Pr(E_6) + \Pr(E_9) - \Pr(E_4 \cap E_6) - \Pr(E_4 \cap E_9) \\ &\quad - \Pr(E_6 \cap E_9) + \Pr(E_4 \cap E_6 \cap E_9) \\ &= \Pr(E_4) + \Pr(E_6) + \Pr(E_9) - \Pr(E_{12}) - \Pr(E_{36}) - \Pr(E_{18}) \\ &\quad + \Pr(E_{36}) \\ &= \Pr(E_4) + \Pr(E_6) + \Pr(E_9) - \Pr(E_{12}) - \Pr(E_{18}) \\ &= \frac{250000}{1000000} + \frac{166666}{1000000} + \frac{111111}{1000000} - \frac{83333}{1000000} - \frac{55555}{1000000} \\ &= \frac{388889}{1000000}\end{aligned}$$

EXERCISE 1.15

- After rolling nine of the ten dice, let x be the remainder when dividing the sum up to that point by 6
- In order for the sum of all ten dice to be divisible by 6, the last dice should be $6 - x$
  - The probability of this is $\frac{1}{6}$, regardless of the value of x
- The answer: $\frac{1}{6}$

EXERCISE 1.18

Assumptions about the Evil Adversary

- For $x \in \{0, ..., n-1\}$, let $G(x)$ be the value in the lookup table that corresponds to x, after the Evil Adversary changed the values in the lookup table.
- We will assume that if the Evil Adversary changed the value of corresponding to x
  - $G(x) \neq F(x)$ (The Evil Adversary did change the value to a different value from original)
    - In other words, exactly $\frac{1}{5}$ of the values are different from original, $\Pr((G(x) \neq F(x))) = \frac{4}{5}$
  - $G(x) \in \{0, ..., m-1\}$ (The Evil Adversary made the value believable)

Randomized Algorithm

- For a given input z
  - Pick a random integer x from $\{0, ..., n-1\}$
  - Let $y = z - x \bmod n$

- Output $(G(x) + G(y)) \bmod m$

Success Probability of the Algorithm

- If $G(x) = F(x)$ and $G(y) = F(y)$, the algorithm outputs a correct value
  - The probability: $\frac{4}{5} \times \frac{4}{5} = \frac{16}{25}$
- If $G(x) = F(x) \wedge G(y) \neq F(y)$, or if $G(x) \neq F(x) \wedge G(y) = F(y)$, then $(G(x) + G(y)) \bmod m \neq (F(x) + F(y)) \bmod m = F(z)$, and the algorithm outputs an incorrect value
- If $F(x)$ and $F(y)$ has both been changed,
  - There are $m - 1$ values, from $\{0, ..., m - 1\} - \{F(y)\}$, that $F(y)$ can be after being changed
  - No matter what value $G(x)$ has, there is exactly one value that $G(y)$ can have that makes the output value correct
    - This value cannot be $F(y)$, because then $G(x) = F(x)$
  - $\therefore$ The probability: $\frac{1}{5} \times \frac{1}{5} \times \frac{1}{m-1}$
- The overall success probability: $\frac{16}{25} + \frac{1}{25} \times \frac{1}{m-1}$
  - Let this value be p_0

Repeating the Algorithm Three Times

- Let (a_1, a_2, a_3) be the three results of the algorithm, and let a_0 be the correct result of the algorithm
- The algorithm: if there is a value that happens twice or more, choose that value, otherwise, choose a_1
- No repeat value
  - In order for the overall algorithm to succeed,
    - The algorithm must have succeeded on the first try
    - Then failed twice resulting in different values
  - The probabilty: $p_0(1 - p_0)^2 \times \frac{m-2}{m-1}$
- Value repeated twice
  - In order for the overall algorithm to succeed,
    - The algorithm must have succeeded twice, and failed once, regardless of the order
  - The probability: $\binom{3}{1} p_0^2 (1 - p_0)$
- Value repeated thrice
  - In order for the ovrall algorithm to succeed,
    - The algorithm must have succeeded all three times
  - The probability: p_0^3
- The overall probability:

$$
\begin{aligned}
&p_0(1-p_0)^2 \times \frac{m-2}{m-1} + \binom{3}{1} p_0^2 (1-p_0) + p_0^3 \\
&= -p_0^3 + p_0^2 + p_0 - \frac{1}{m-1} p_0 (1-p_0)^2 \\
&= -\frac{639}{15625(m-1)} + \frac{184}{15625(m-1)^2} + \frac{1}{15625(m-1)^3} - \frac{1}{15625(m-1)^4} + \frac{12304}{15625}
\end{aligned}
$$

- Assuming $m \to \infty$, $\frac{12304}{15625} \approx 0.787$

EXERCISE 1.23

- Let $C_1, ..., C_m$ be every distinct min-cut sets of the graph
- Let E_i be the event where the randomized min-cut algorithm results in the cut set C_i
  - $\Pr(E_i) \geq \frac{2}{n(n-1)}$, according to the analysis of the algorithm
  - E_i are mutually disjoint events, since the cut sets C_i are distinct
- $m \times \frac{2}{n(n-1)} \leq \sum_{i=1}^{m} \Pr(E_i) \leq 1$
  - $\therefore m \leq \frac{n(n-1)}{2}$, there can be at most $\frac{n(n-1)}{2}$ min-cut sets for any graph