(CS1.406) Advanced Algorithms (Spring 2024) Due: 18.01.2024

Problem Set 1

Instructions:

- Discussions amongst the students are not discouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring sources other than the lecture notes is discouraged as solutions to some of the problems can be found easily via a web search. But if you do use an outside source (eg., text books, other lecture notes, any material available online), do mention the same in your writeup. This will not affect your grades. However dishonesty of any sort when caught shall be heavily penalized.
- Be clear in your arguments. Vague arguments shall not be given full credit.

---

1. Let the events $E_1, E_2, \ldots, E_n$ be mutually independent. Then show that the events $\overline{E}_1, \overline{E}_2, \ldots, \overline{E}_n$ are also mutually independent.
2. Consider a set of integers $\{1, 2, \ldots, n\}$ (denoted by $[n]$). We generate a subset X of $[n]$ using the following random process – a two-sided and unbiased coin is flipped independently for each element a of the set $[n]$ and we add a to the set X if and only if the coin lands HEADS.
   (a) What is the probability distribution over all subsets of $[n]$ under this process.
   (b) Suppose two sets X and Y are chosen independently and uniformly at random from all the subsets of $[n]$, then determine
      i. the probability that X is a subset of Y, and
      ii. the probability that $X \cup Y = \{1, 2, \ldots, n\}$.
3. Let Y be a random variable assuming only non-negative values. Then show that for all $t \in \mathbb{R}_{\geqslant 0}$,
$$\mathbb{P}[X \geqslant t] \leqslant \frac{\mathbb{E}[X]}{t}.$$ **markov inequality**
4. Let X be a random variable with expectation μ_X and standard deviation σ_X. Then show that for any $t \in \mathbb{R}_{\geqslant 0}$,
$$\mathbb{P}[|X - \mu_X| \geqslant t \cdot \sigma_X] \leqslant \frac{1}{t^2}.$$ **chebyshev inequality**
   Similarly, show that for any $\nu \in \mathbb{R}_{\geqslant 0}$,
$$\mathbb{P}[|X - \mu_X| \geqslant \nu] \leqslant \frac{\mathrm{Var}[X]}{\nu^2}.$$

5. The weak law of large numbers states that if $X_1, X_2, X_3, \ldots$ are independent and identically distributed random variables with mean μ and standard deviation σ, then for any constant $\varepsilon > 0$ we have

$$\lim_{n\to\infty} \mathbb{P}\left[\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \mu\right| > \varepsilon\right] = 0.$$

Use the inequality from the previous problem to prove the weak law of large numbers.

6. Suppose we run a experiment E (with randomness) that succeeds with a probability p and fails with a probability $1 - p$. Suppose X is a random variable defined to be the number of trials needed for the experiment E to succeed. Then show that the following hold.

   (a) $\mathbb{P}[X = i] = (1-p)^{i} \cdot p$.

   (b) $\mathbb{P}[X \geqslant i] = (1-p)^{i-1}$.

   (c) $\mathbb{E}[X] = \frac{1}{p}$.

7. A function $f : \mathbb{R} \mapsto \mathbb{R}$ is said to be convex if for any x_1, x_2 and $0 \leqslant \lambda \leqslant 1$, the following inequality is satisfied.

$$f(\lambda x_1 + (1-\lambda)x_2) \leqslant \lambda \cdot f(x_1) + (1-\lambda) \cdot f(x_2).$$

Let Z be a random variable that assumes values in the interval $[0, 1]$ and let $p = \mathbb{E}[Z]$. Define a Bernoulli random variable X such that $\mathbb{P}[X = 1] = p$ and $\mathbb{P}[X = 0] = 1 - p$. Then show that for any convex function f, $\mathbb{E}[f(Z)] \leqslant \mathbb{E}[f(X)]$. Please do not invoke Jensen's Inequality directly. You could however prove it and use it. Page 27. Book

8. Suppose you pick a graph on n vertices by picking each edge with probability p independently of the others. What is the expected number of triangles in the graph. Linearity of Expectation

9. Consider the problem of deciding whether two integer multisets S_1 and S_2 are identical in the sense that each integer occurs the same number of times in both sets. The problem can be solved by sorting the two sets in $O(n \log n)$ time where n is the cardinality of the multisets. Suggest a way of representing this as a problem involving verification of polynomial identity and thereby obtain an efficient randomized algorithm.

Advanced questions

1. Let $\{x_{i,j} \mid 1 \leqslant i, j \leqslant n\}$ be a set of n^2 many distinct variables (also called indeterminates). For a given graph $G = (V, E)$ (which is not necessarily bipartite) with $V = \{v_1, \ldots, v_n\}$, we define a $n \times n$ skew-symmetric[1] matrix T_G corresponding to it as follows.

$$\text{For all } 1 \leqslant i, j \leqslant n, \qquad (T_G)_{i,j} = \begin{cases} x_{i,j} & \text{if } (v_i, v_j) \in E \text{ and } i < j, \\ -x_{j,i} & \text{if } (v_i, v_j) \in E \text{ and } i > j, \\ 0 & \text{otherwise.} \end{cases}$$

Let $A_\sigma = \prod_{i=1}^{n} (T_G)_{i,\sigma(i)}$.

[1] $A^T = -A$.

(a) Show that if a permutation σ has an odd cycle then there exists another permutation σ' such that

$$\text{sign}(\sigma) \cdot A_\sigma + \text{sign}(\sigma') \cdot A_{\sigma'} = 0\,.$$

(b) Show that G has a perfect matching if and only if there exists a permutation σ with all even cycles such that $A_\sigma \neq 0$.

(c) Show that G has a perfect matching if and only if $\text{Det}(T_G) \not\equiv 0$.

2. A cloud storage provider CSP has a file x corresponding to the file y on user's device. CSP wants to ensure that x is consistent with y. Towards this CSP converts x and y to bit strings, picks a prime p uniformly at random in $[1, \ell^2]$ (where ℓ is the length of bit encoding of x and y), and sends p and $x \bmod p$ to the user's device. The device checks if $x \equiv y \mod p$ and if not, initiates syncing. Show that the probability that this algorithm makes an error in asserting $x \equiv y \mod p$, bounded on the above by $\frac{3 \ln \ell}{\ell}$. (**Hint:** There are about $\frac{t}{\ln t}$ many primes between 1 and t.)

Name: Aaryan Ajay Sharma
Roll no: 2022121001
Date: 17/01/2024

Solution to Problem Set 1

1. Let the events $E_1, E_2, \ldots, E_n$ be mutually independent. Then show that the events $\overline{E}_1, \overline{E}_2, \ldots, \overline{E}_n$ are also mutually independent.

Let $P(n)$ be the statement:

The set of events $A = \{E_i \mid 1 \le i \le n\}$ are mutually independent $(\Rightarrow)$ implies

The set of events $B = \{\overline{E}_i \mid 1 \le i \le n\}$ are mutually independent.

We can use strong induction to prove $P(n)$.

Base case: $n = 2$

$P(2)$: E_1 & E_2 are mutually independent $\Rightarrow$ $\overline{E}_1$ and $\overline{E}_2$ are mutually independent

We have,

$$P(E_1 \cap E_2) = P(E_1)P(E_2)$$

$$\Rightarrow P(\overline{\overline{E}_1 \cup \overline{E}_2}) = P(\overline{E}_1)P(\overline{E}_2)$$

$$\Rightarrow 1 - P(\overline{E}_1 \cup \overline{E}_2) = (1 - P(\overline{E}_1))(1 - P(\overline{E}_2))$$

$$\Rightarrow 1 - (P(\overline{E}_1) + P(\overline{E}_2) - P(\overline{E}_1 \cap \overline{E}_2)) = 1 - (P(\overline{E}_1) + P(\overline{E}_2)) + P(\overline{E}_1)P(\overline{E}_2)$$

$$\Rightarrow 1 - (P(\overline{E}_1) + P(\overline{E}_2)) + P(\overline{E}_1 \cap \overline{E}_2) = 1 - (P(\overline{E}_1) + P(\overline{E}_2)) + P(\overline{E}_1)P(\overline{E}_2)$$

$$\Rightarrow P(\overline{E}_1 \cap \overline{E}_2) = P(\overline{E}_1)P(\overline{E}_2)$$

$\therefore$ $P(2)$ is true.

Now, let $P(2), P(3), \ldots, P(m)$ be true.

We need to prove $P(m+1)$.

$P(m+1)$:

The set of events $A = \{E_i \mid 1 \le i \le m+1\}$ are mutually independent $\Rightarrow$

The set of events $B = \{\overline{E}_i \mid 1 \le i \le m+1\}$ are mutually independent.

$$\therefore P(E_1 \cap E_2 \cdots E_{m+1}) = P(E_1)P(E_2)P(E_3)\cdots P(E_{m+1})$$

$$\Rightarrow P(\overline{\bar{E}_1 \cup \bar{E}_2 \cdots \bar{E}_{m+1}}) = P(\bar{E}_1)P(\bar{E}_2)\cdots P(\bar{E}_{m+1})$$

$$\Rightarrow 1 - P(\bar{E}_1 \cup \bar{E}_2 \cup \cdots \cup \bar{E}_{m+1}) = (1-P(\bar{E}_1))(1-P(\bar{E}_2))\cdots(1-P(\bar{E}_{m+1}))$$

(from inclusion-exclusion principle)

$$\Rightarrow 1 - \left\{ \sum_{i=1}^{m+1} P(\bar{E}_i) - \left[\sum_{1\le i<j\le m+1} P(\bar{E}_i \cap \bar{E}_j) \right] + \sum_{1\le i<j<k\le m+1} P(\bar{E}_i \cap \bar{E}_j \cap \bar{E}_k) - \cdots + (-1)^{m+1} P(\bar{E}_1 \cap \bar{E}_2 \cdots \bar{E}_{m+1}) \right\}$$

$$= 1 - \sum_{i=1}^{m+1} P(\bar{E}_i) + \left[\sum_{1\le i<j\le m+1} P(\bar{E}_i)P(\bar{E}_j) \right] - \sum_{1\le i<j<k\le m+1} P(\bar{E}_i)P(\bar{E}_j)P(\bar{E}_k) + \cdots + (-1)^{m+1} P(\bar{E}_1)P(\bar{E}_2)\cdots P(\bar{E}_{m+1}) \quad (Eq.1)$$

Now, since $P(K)$ is true for $\forall\ 2 \le K \le m$ from strong induction

$$\therefore \sum_{1\le a_1<a_2<\cdots<a_K\le m+1} P(\bar{E}_{a_1} \cap \bar{E}_{a_2} \cdots \bar{E}_{a_K}) = \sum_{1\le a_1<a_2<\cdots<a_K\le m+1} P(\bar{E}_{a_1})P(\bar{E}_{a_2})\cdots P(\bar{E}_{a_K}) \quad \forall\ 2 \le K \le m \quad (Eq.2)$$

Using (Eq.2) in (Eq.1), we get:

$$1 - \sum_{i=1}^{m+1} P(\bar{E}_i) + \left[\sum_{1\le i<j\le m+1} P(\bar{E}_i)P(\bar{E}_j) \right] - \sum_{1\le i<j<k\le m+1} P(\bar{E}_i)P(\bar{E}_j)P(\bar{E}_k) + \cdots + (-1)^{m+1} P(\bar{E}_1 \cap \bar{E}_2 \cdots \bar{E}_{m+1})$$

$$= 1 - \sum_{i=1}^{m+1} P(\bar{E}_i) + \left[\sum_{1\le i<j\le m+1} P(\bar{E}_i)P(\bar{E}_j) \right] - \sum_{1\le i<j<k\le m+1} P(\bar{E}_i)P(\bar{E}_j)P(\bar{E}_k) + \cdots + (-1)^{m+1} P(\bar{E}_1)P(\bar{E}_2)\cdots P(\bar{E}_{m+1})$$

$$\therefore P(\bar{E}_1 \cap \bar{E}_2 \cdots \bar{E}_{m+1}) = P(\bar{E}_1)P(\bar{E}_2)\cdots P(\bar{E}_{m+1})$$

$\therefore P(m+1)$ is true.

$\therefore$ The statement $P(n)$:

The set of events $A = \{E_i \mid 1 \le i \le n\}$ are mutually independent $\Rightarrow$ The set of events $B = \{\bar{E}_i \mid 1 \le i \le n\}$ are mutually independent.

is proved.

2. Consider a set of integers $\{1, 2, \ldots, n\}$ (denoted by $[n]$). We generate a subset X of $[n]$ using the following random process – a two-sided and unbiased coin is flipped independently for each element a of the set $[n]$ and we add a to the set X if and only if the coin lands HEADS.

   (a) What is the probability distribution over all subsets of $[n]$ under this process.

   (b) Suppose two sets X and Y are chosen independently and uniformly at random from all the subsets of $[n]$, then determine

      i. the probability that X is a subset of Y, and

      ii. the probability that $X \cup Y = \{1, 2, \ldots, n\}$.

(a) For each element a in $[n]$, there are two possibilities – either it is included in the subset (if coin lands HEADS) or it is not included in the set (if the coin lands TAILS). Since coin flips are independent, there are 2^n possible outcome, each corresponding to a different subset of $[n]$. The probability of each subset is $1/2^n$ because all the 2^n subsets are equally likely outcomes.

So, the probability distribution over all subsets of $[n]$ is a uniform distribution, where each subset has probability of $1/2^n$

(b) i) There are 4 distinct possibilities for an element a when X and Y are independently chosen: i) $a \notin X$, $a \notin Y$
ii) $a \notin X$, $a \in Y$
iii) $a \in X$, $a \notin Y$
iv) $a \in X$, $a \in Y$

For $X \subseteq Y$, only i), ii) and iv) should be true. Since all of these can happen with equal probability of $1/4$, the probability $X \subseteq Y$ will be $(\frac{1}{4}+\frac{1}{4}+\frac{1}{4})^n = (\frac{3}{4})^n$

ii) For $X \cup Y$ to be equal to $[n]$, every element in $[n]$ must be in either X or Y or both. The probability for each element to be in either X or Y (or both) is $1/2 + 1/2 - \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$. Since this is true for each element in $[n]$, the overall probability that $X \cup Y = [n]$ is $\left(\frac{3}{4}\right)^n$, where n is the size of $[n]$.

3. Let Y be a random variable assuming only non-negative values. Then show that for all $t \in \mathbb{R}_{\geqslant 0}$,

$$\mathbb{P}[X \geqslant t] \leqslant \frac{\mathbb{E}[X]}{t}.$$

Let $\mathbb{I}$ be an indicator random variable s.t.

$$\mathbb{I} = \begin{cases} 1 & \text{if } X \geq t \\ 0 & \text{otherwise} \end{cases}$$

$\therefore E(\mathbb{I}) = 1 \cdot P(X \geq t) + 0 \cdot P(X < t)$

$= P(X \geq t)$

Also, $\mathbb{I} \leq \frac{X}{t}$ since for $X \in [t, \infty)$ $\mathbb{I} = 1$ and $\frac{X}{t} \in [1, \infty)$

and for $X \in [0, t)$, $\mathbb{I} = 0$ and $\frac{X}{t} \in [0, 1)$

$\therefore E(\mathbb{I}) \leq E(\frac{X}{t})$

$\Rightarrow P(X \geq t) \leq \frac{E(X)}{t}$

Reference: Mitzenmacher, upfal - Probabilistic Computing, Page 47.

4. Let X be a random variable with expectation μ_X and standard deviation σ_X. Then show that for any $t \in \mathbb{R}_{\geqslant 0}$,

$$\mathbb{P}\left[|X - \mu_X| \geqslant t \cdot \sigma_X\right] \leqslant \frac{1}{t^2}.$$

Similarly, show that for any $\nu \in \mathbb{R}_{\geqslant 0}$,

$$\mathbb{P}\left[|X - \mu_X| \geqslant \nu\right] \leqslant \frac{\mathrm{Var}[X]}{\nu^2}.$$

we will use the results we got in Q.3

We know that $P(X \geq t) \leq \frac{E(X)}{t}$

Now, substitute X with $|X - \mu_X|$ (since X is non-negative)

$\therefore P(|X-\mu_X| \geq t) \Rightarrow P(|X-\mu_X|^2 \geq t^2) \leq \frac{E(|X-\mu_X|^2)}{t^2}$

$\Rightarrow P(|X-\mu_X|^2 \geq t^2) \leq \frac{Var(X)}{t^2}$

this is valid for any $t = \nu \in \mathbb{R}_{\geq 0}$

$\therefore P(|X-\mu_X| \geq \nu) \leq \frac{Var(X)}{\nu^2}$

replacing $\nu = t \cdot \sigma_X$, where σ_X is the standard deviation, we get:

$$P(|X-\mu_X| \geq \sigma_X \cdot t) \leq \frac{Var(X)}{\sigma_X^2 \cdot t^2} = \frac{1}{t^2}.$$

$\therefore P(|X-\mu_X| \geq \sigma_X t) \leq \frac{1}{t^2}$

5. The weak law of large numbers states that if $X_1, X_2, X_3, \ldots$ are independent and identically distributed random variables with mean μ and standard deviation σ, then for any constant $\varepsilon > 0$ we have

$$\lim_{n\to\infty} \mathbb{P}\left[\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \mu\right| > \varepsilon\right] = 0.$$

We know the inequility :

$$P(|X - \mu_X| \geq t) \leq \frac{Var(X)}{t^2}$$

substituting X with $\frac{X_1 + X_2 + \ldots X_n}{n}$, we get

$$Var\left(\frac{X_1 + X_2 + \ldots + X_n}{n}\right) = \frac{n \cdot \sigma^2}{n^2} \leq \frac{\sigma^2}{n}$$

$$\therefore P\left(\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \mu\right| > \varepsilon\right) \leq \frac{\frac{\sigma^2}{n}}{\varepsilon^2}$$

$$\Rightarrow P\left(\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \mu\right| > \varepsilon\right) \leq \frac{\sigma^2}{n\varepsilon^2}$$

As $\lim_{n\to\infty}$, $\frac{\sigma^2}{n\varepsilon^2} \to 0$

$$\therefore \lim_{n\to\infty} P\left(\left|\frac{X_1 + X_2 + \ldots + X_n}{n} - \mu\right| > \varepsilon\right) = 0$$

6. Suppose we run a experiment E (with randomness) that succeeds with a probability p and fails with a probability $1-p$. Suppose X is a random variable defined to be the number of trials needed for the experiment E to succeed. Then show that the following hold.

   (a) $\mathbb{P}[X = i] = (1-p)^{i} \cdot p$.

   (b) $\mathbb{P}[X \geqslant i] = (1-p)^{i-1}$.

   (c) $\mathbb{E}[X] = \frac{1}{p}$.

(a) $X = i \Rightarrow$ the experiment succeeds in i trails, meaning the i^{th} trial was a success and the $(i-1)$ trials were all fails.

$\therefore P(X=i) = (1-p)^{i-1} \cdot p.$

(b) $P(X \geq i) = \sum_{k=i}^{\infty} P(X=k)$

$= \sum_{k=i}^{\infty} (1-p)^{k-1} \cdot p$

$= p \cdot \frac{(1-p)^{i-1}}{1-(1-p)}$

$= \frac{p}{p} \cdot (1-p)^{i-1}$

$= (1-p)^{i-1}$

(c) $E(X) = \sum_{i=1}^{\infty} i P(X=i)$

$= \sum_{i=1}^{\infty} i \cdot (1-p)^{i-1} \cdot p$

$= \frac{1}{p}$.

$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$

$\sum_{i=1}^{\infty} i \cdot x^{i-1} = \frac{1}{(1-x)^2}$ (derivative w.r.t x)

$\sum_{i=1}^{\infty} i \cdot x^{i-1}(1-x) = \frac{1}{1-x}$

$\sum_{i=1}^{\infty} i(1-p)^{i-1} p = \frac{1}{p}$ (let $x = 1-p$)

7. A function $f : \mathbb{R} \mapsto \mathbb{R}$ is said to be convex if for any x_1, x_2 and $0 \leqslant \lambda \leqslant 1$, the following inequality is satisfied.

$$f(\lambda x_1 + (1-\lambda)x_2) \leqslant \lambda \cdot f(x_1) + (1-\lambda) \cdot f(x_2).$$

Let Z be a random variable that assumes values in the interval $[0, 1]$ and let $p = \mathbb{E}[Z]$. Define a Bernoulli random variable X such that $\mathbb{P}[X = 1] = p$ and $\mathbb{P}[X = 0] = 1 - p$. Then show that for any convex function f, $\mathbb{E}[f(Z)] \leqslant \mathbb{E}[f(X)]$. Please do not invoke Jensen's Inequality directly. You could however prove it and use it.

First, we will prove Jensen's Inequality which is as follows:

For a random variable X, and convex function f, the following inequality holds:

$$E(f(x)) \geq f(E(x))$$

Assuming that f is twice differentiable, we will use another well-known definition of convex function as follows:

For a twice differentiable function f, it is convex if and only if

$$f''(x) \geq 0$$

We will also use Taylor's theorem which is as follows: * Reference given at the end of the answer

Suppose that f is defined on some interval I around a and suppose $f^{N+1}(x)$ exists on this interval. Then for each $x \neq a$ in I there is a value z between x and a such that

$$f(x) = \sum_{n=0}^{N} \frac{f^{(n)}(a)}{n!}(x-a)^n + \frac{f^{(N+1)}(z)}{(N+1)!}(x-a)^{N+1}$$

Now, since we assumed the second derivative of f exist, we can expand f using Taylor's Theorem as follows:

$$f(x) = f(u) + f'(u)(x-u) + \frac{f''(a)(x-u)^2}{2!}, \text{ for some } a \in (x, u)$$

since $f(x)$ is convex $\forall x \in \mathbb{R}$, $\therefore f''(a) \geq 0$

$\therefore f(x) = f(u) + f'(u)(x-u) + \underline{\frac{f''(a)(x-u)^2}{2!}} \geq f(u) + f'(u)(x-u)$

$\therefore f(X) \geq f(u) + f'(u)\cdot(X-u)$

$\therefore E(f(X)) \geq E(f(u)) + f'(u)(E(X)-u)$ (Taking expectation on both sides)

Now, since $E(X) = u$, we get:

$$E(f(X)) \geq f(E(X)) + f'(u)(u-u)$$

$$\Rightarrow E(f(X)) \geq f(E(X))$$ (Jensen's Inequality)

Now, since f is convex, the following inequality holds:

$$f(\lambda x_1 + (1-\lambda)x_2) \leq \lambda f(x_1) + (1-\lambda) f(x_2)$$

Given $p = E(z)$, we can write p as follows:

$p = \int_0^1 z \, dF(z)$, where $F(z)$ is the cdf of the continuous RV z.

Also, the expected value of $f(z)$ will be

$E(f(z)) = \int_0^1 f(z) \, dF(z)$

The expected value of $f(x)$ will be

$$E(f(x)) = pf(1) + (1-p)f(0)$$

Applying $x_1 = 1$, $x_2 = 0$, $\lambda = z$ (for $z \in [0,1]$), we get:

$f(z) = f(z\cdot 1 + (1-z)\cdot 0) \leq z \cdot f(1) + (1-z) f(0)$

$\Rightarrow f(z) \leq z \cdot f(1) + (1-z) f(0)$

$$\therefore \quad E(f(Z)) = \int_0^1 f(z) \cdot dF(z)$$

$$\leq \int_0^1 [z f(1) + (1-z) f(0)] \, dF(z)$$

$$= f(1)\left[\int_0^1 z \, dF(z)\right] + \left(1 - \left[\int_0^1 z \, dF(z)\right]\right) f(0)$$

$$= f(1) \cdot p + (1-p) f(0)$$

$$= E(f(X))$$

$$\therefore \quad E(f(Z)) \leq E(f(X))$$

---

* **Reference:** https://www.whitman.edu/mathematics/calculus_online/section11.11.html

↳ I ended up not using Jensen's Inequality at all in the end, but kept the proof just because I already wrote it before I came up with the proof. Sorry for the inconvenience. (T_T)

8. Suppose you pick a graph on n vertices by picking each edge with probability p independently of the others. What is the expected number of triangles in the graph.

Let X be the total triangles in a graph,

Let $X = X_1 + X_2 + \dots + X_N$

where N = maximum possible triangle in the graph and $X_i \rightarrow$ where the i^{th} triangle actually is within the graph.

$$\therefore X_i = \begin{cases} 1 & \text{if } i^{th} \text{ triangle present} \\ 0 & \text{otherwise} \end{cases}$$

Now, the probability that $X_i = 1$ is the probability that the i^{th} triangle is present in the graph, which is simply $p \times p \times p = p^3$ since edge is picked with probability p independently of each other.

$$\therefore P(X_i = 1) = p^3$$

$$\therefore E(X_i) = 1 \cdot P(X_i = 1) + 0 \cdot P(X_i = 0)$$

$$= P(X_i = 1) = p^3$$

$$\therefore E(X) = E(X_1 + X_2 + \dots + X_N)$$

$$= E(X_1) + E(X_2) + \dots + E(X_N) \quad \text{(linearity of Expectation)}$$

$$= p^3 + p^3 + \dots + p^3 = Np^3$$

Here, N = max. possible triangles in a graph = ${}^nC_3$, where n = no. of vertices in a graph.

$$\therefore E(X) = {}^nC_3 \cdot p^3$$

9. Consider the problem of deciding whether two integer multisets S_1 and S_2 are identical in the sense that each integer occurs the same number of times in both sets. The problem can be solved by sorting the two sets in $O(n \log n)$ time where n is the cardinality of the multisets. Suggest a way of representing this as a problem involving verification of polynomial identity and thereby obtain an efficient randomized algorithm.

We can represent an integer multiset as polynomial by representing an arbitrary integer of the multiset a and its frequency f as a term in the polynomial whose power is a and whose coefficient is f i.e. $f \cdot x^a$.

∴ The algorithm for constructing polynomial from multisets is as follows:

CONSTRUCT-POLYNOMIAL(S) : (S → multiset)

1. Initialize $P \leftarrow \Phi$
2. For each $a \in S$:
2.1. P.add(S.a.value, S.a.frequency)
3. Return P

Here we consider:

S → multiset containing objects as element

S.a → object representing an arbitrary element of the multiset

S.a.value → value of the integer that the object represents in the integer multiset

S.a.frequency → frequency of the integer represented by a.

P → Polynomial, initialized 0 at the beginning

P.add(m,n) → A method to add a term with power m and frequency n to P

Now that we can convert our two multisets S_1 and S_2 (say) to P_1 and P_2 (say), our problem has been reduced to verifying whether the two polynomials P_1 and P_2 are equal or not.

This can be done via Schwartz-Zippel lemma* which is as follows:

Let $Q(x_1, x_2, \ldots, x_n)$ be a non-zero multivariate polynomial of total degree d defined over the field $F[x_1, x_2, \ldots, x_n]$.

Fix any set $S \subseteq F$ and let $r_1, r_2 \ldots, r_n$ be chosen independently and uniformly at random from S. Then

$$Pr[\, Q(r_1, r_2, \ldots, r_n) = 0 \mid Q(x_1, x_2, \ldots x_n) \not\equiv 0 \,] \leq \frac{d}{|S|}$$

*Reference: Motwani, Raghvan, Prabhakar - Randomized Algorithms Page: 165

The lemma/theorem can be proved via induction.

∴ our final algorithm for verification is as follows:

VERIFY-EQUAL(S_1, S_2):

1. $P_1 \leftarrow$ CONSTRUCT-POLYNOMIAL(S_1)
2. $P_2 \leftarrow$ CONSTRUCT-POLYNOMIAL(S_2)
3. Sample $r_1, r_2, \ldots, r_n$ independently and uniformly at random from $S \subseteq F$, with $|S|$ being sufficiently large
4. Compute $P_1(r_1, r_2, \ldots, r_n)$ and $P_2(r_1, \ldots, r_n)$

5. If $P_1(r_1, r_2 \ldots, r_n) \neq P_2(r_1, r_2, \ldots r_n)$:
RETURN $P_1 \not\equiv P_2$

else:
RETURN $P_1 \equiv P_2$ with probability $> 1 - \frac{d}{|S|}$.

We can reduce our error probability by taking an arbitrarily large S or by repeating the algorithm K more times which would make our error probability $\left(\frac{d}{|S|}\right)^K$ since trials are independent from each other.

Complexity:

- The polynomial construction takes $O(n)$ time since each element in the multiset contributes one term to the polynomial.
- The evaluation of the polynomial at a point can be efficiently done in $O(n)$.
- Therefore, the overall complexity will be $O(n)$, which more efficient than the $O(n \log n)$ time required for sorting based approach.