Prerequisites Test

Cryptography and Security 2024

Exercise 1 Probability

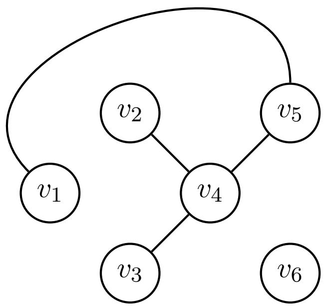

Figure 1: Example graph with 6 vertices ($V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$) and 4 edges ($E = \{\{v_1, v_5\}, \{v_2, v_4\}, \{v_3, v_4\}, \{v_4, v_5\}\}$) where v_6 is an isolated vertex.

A simple, undirected graph $G = (V, E)$ with vertex set V and edge set E is a graph without any self loops or multiedges, and whose edges have no direction. In other words, for any two vertices a and b, there is at most one edge $\{a, b\}$ (edge $(a, b) = (b, a)$) between them, and there is no edge if $a = b$. We say a vertex is isolated if there is no edge connected to it. See Figure 1 as an example.

Suppose for every two different vertices a and b, the edge $\{a, b\}$ appears with probability p. Moreover, the appearances of any two different edges are independent.

Question 1.1 Expectation

Given $|V| = n$, use the linearity of expectation to compute the expected number of isolated vertices.
Hint: Define a boolean random variable X_i that indicates whether vertex i is isolated.

Answer. Let X_i be a boolean random variable that indicates whether vertex i is isolated.Then $\Pr[X_i = 1] = (1-p)^{n-1}$ since there are at most $n-1$ edges that can connect to i, and each of them does not appear with probability $1-p$. Since X_i takes value in $\{0, 1\}$, $\mathrm{E}[X_i] = \Pr[X_i] = (1-p)^{n-1}$.

Let $X = \sum_i X_i$ be the random variable for the number of isolated vertices. By linearity of expectation, $\mathrm{E}[X] = \sum_i \mathrm{E}[X_i] = n \cdot (1-p)^{n-1}$

Question 1.2 Variance

Compute the variance of number of isolated vertices.

Answer. We know that $\mathrm{Var}[X] = \mathrm{E}[X^2] - \mathrm{E}[X]^2$ and $\mathrm{E}[X] = n \cdot (1-p)^{n-1}$ from the previous question. It suffices to compute $\mathrm{E}[X^2]$.

Again let $X = \sum_i X_i$. Then we compute

$$\begin{aligned} \mathrm{E}[(\sum_i X_i)^2] &= \sum_{i,j} \mathrm{E}[X_i X_j] \\ &= \sum_{i \neq j} \mathrm{E}[X_i X_j] + \sum_i \mathrm{E}[X_i^2] \end{aligned}$$

For the second term, notice that $X_i^2 = X_i$ for Bernoulli random variable. Then for n addends, $\sum_i \mathrm{E}[X_i^2] = n\mathrm{E}[X_i] = n \cdot (1-p)^{n-1}$.

For the first term, we need some extra care. Since $X_i X_j$ takes value in $\{0, 1\}$, it suffices to calculate $\Pr[X_i X_j]$. Also notice that $X_i X_j = 1$ iff both vertice i and j are isolated. We first ignore the edge $\{i, j\}$, the probability that vertex i does not have the remaining $n-2$ edges is $(1-p)^{n-2}$, same for vertex j. The probability that both vertex i and j are isolated except for edge $\{i, j\}$ is then $(1-p)^{2n-4}$. Finally, the probability that $\{i, j\}$ does not appear is $(1-p)$. Putting everything together, the probability that $X_i X_j = 1$ is $(1-p)^{2n-3}$.

To conclude, the variance is $n(1-p)^{n-1} + n(n-1)(1-p)^{2n-3} - n^2(1-p)^{2n-2}$.

Exercise 2 Algorithms

Question 2.1 Randomized Algorithms

In this exercise, we are going to analyze the expected number of iterations for a simple randomized search algorithm. Let $a_1, \ldots, a_N$ be N integers. Our goal is to search the index of a given target number T. Below is an algorithm $\mathsf{RandSearch}(a_1, \ldots, a_N, N, T)$ that takes a list of integers as $a_1, \ldots, a_N$, the number of integers as N and the target integer as T, outputs an index in $\{1, \ldots, N\}$ if T is found, 0 if not.

$\mathsf{RandSearch}(a_1, \ldots, a_N, N, T)$

1 : pick a uniformly random permuation of σ of $a_1, \ldots, a_N$
2 : **for** $i = 1$ to N :
3 :   **if** $a_{\sigma(i)} = T$:
4 :   **return** $\sigma(i)$
5 : **return** 0

1. Compute the expected number of iterations of the for loop in line 2 of the RandSearch algorithm.

   Answer. **Assuming** a_i are distinct and there exists $i, 1 \leq i \leq N$ s.t. $T = a_i$. The grading was a bit relaxed due to this assumption being announced mid exam and each question was graded based on its own assumption.

   Note: Albeit being simple, this analysis appears quite often in the course while analyzing the complexity of brute force attacks.
   Let X be the random variable for the number of iterations of the RandSearch algorithm. We have

   $$E[X] = \sum_{i=1}^{N} E[Pr[C = a_{\sigma(i)}]] \cdot i$$

   Since σ is a uniformly random permutation, we have

   $$E[Pr[C = a_{\sigma(i)}]] = \frac{1}{N}$$

   for all i Hence, we have

   $$E[X] = \sum_{i=1}^{N} \frac{1}{N} \cdot i = \frac{N+1}{2}$$

   Common mistake: X is not a geometric distribution, it would be the case if we were sampling an element from $\{a_1, \ldots, a_N\}$ at each iteration. However, in our case we are iterating over these elements meaning that we only visit them once in a random order.

Question 2.2 Asymptotic Notation

Assume that $f(n)$ and $g(n)$ are two positive functions.

Definition 1 ($O(.)$)**.** We write $f(n) = O(g(n))$ if and only if there exist constants $N > 0$ and $C > 0$ such that for all $n \geq N$, $f(n) \leq C \cdot g(n)$.

Definition 2 ($\Omega(.)$)**.** We write $f(n) = \Omega(g(n))$ if and only if there exist constants $N > 0$ and $C > 0$ such that for all $n \geq N$, $f(n) \geq C \cdot g(n)$.

Definition 3 ($\Theta(.)$)**.** We write $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

Definition 4 ($o(.)$)**.** We write $f(n) = o(g(n))$ if and only if for all constants $C > 0$ there exists $N > 0$ such that for all $n \geq N$, $f(n) < C \cdot g(n)$.

1. Show that if $f = \Omega(g)$ then f is not in $o(g)$.

   Answer. Assume the contrary that $f = \Omega(g)$ and $f = o(g)$, we have the following:

   (a) by definition of o, for all constants $c > 0$ there exists $N_1 > 0$ such that for all $n \geq N_1$ we have
   $$f(n) < c \cdot g(n)$$

   (b) by definition of Ω, there exists constants $c_2 > 0$ and $N_2 > 0$ such that for all $n \geq N_2$ we have
   $$f(n) \geq c_2 \cdot g(n)$$

   Note that since the first condition holds for all positive constants, it holds for c_2 as well. Moreover, both conditions when n is greater than N_1 and N_2. Hence, we obtain a contradiction as required.

2. Show that if $f(n) + g(n) = \Theta(max\{f(n), g(n)\})$.

   Answer. By definition, we need to show that $f(n) + g(n) = O(max\{f(n), g(n)\})$ and $f(n) + g(n) = \Omega(max\{f(n), g(n)\})$. Note that both f and g are positive functions. Hence, for a fixed for any $n > 0$ we have $f(n) > 0$ and $g(n) > 0$.

   - Due to the positiveness of f and g we have $f(n) + g(n) > 1 \cdot max\{f(n), g(n)\}$ so $f(n) + g(n) = \Omega(max\{f(n), g(n)\})$ with $C = 1$.
   - Again, due to positiveness, we have $f(n) + g(n) \leq 2 \cdot max\{f(n), g(n)\}$ so $f(n) + g(n) = O(max\{f(n), g(n)\})$ with $C = 2$.

Exercise 3 Number Theory & Algebra

The goal of this exercise is to demonstrate the connection between two mathematical concepts: Mersenne primes and perfect numbers.

Definition 5 (Mersenne primes)**.** A prime number q is called a Mersenne prime if $q = 2^n - 1$ for some $n \in \mathbb{N}$.

For example, $7 = 2^3 - 1$ and $31 = 2^5 - 1$ are Mersenne primes. Note that q being prime implies n is prime but not all numbers of the form $2^p - 1$ are Mersenne primes. For instance, $2^{11} - 1 = 2047 = 23 \times 89$.

Definition 6 (Perfect numbers)**.** A number $n \in \mathbb{N}$ is called *perfect* if the sum of all its positive divisors equals $2n$.

For example, 6 is the smallest perfect number, as its divisors are $1, 2, 3$ and 6 and their sum is equal to 12.

To link both concepts, we use *Euler's σ function*, which is similar to Euler's totient function. It is defined as follows:

$$\sigma : \mathbb{N} \to \mathbb{N}$$
$$\sigma(n) = \sum_{d|n, d>0} d$$

Question 3.1 Perfect Numbers

Here are some calculations to reinforce your understanding in those notions:

- Are 28 and 42 perfect numbers? Show why.
- What is the value of $\sigma(p^n)$, where p is prime and $n \in \mathbb{N}$?
- Show that σ is *multiplicative*, i.e., for $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$, we have

$$\sigma(a \cdot b) = \sigma(a)\sigma(b)$$

Answer.

- 28 is a perfect number. Since $28 = 7 \times 4$, we have

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \times 28.$$

However, 42 is not perfect. Since $42 = 2 \times 3 \times 7$, we have

$$\sigma(42) = 1 + 2 + 3 + 6 + 7 + 14 + 21 + 42 = 96 \neq 84 = 2 \times 42.$$

- Since divisors of p^n are of the form p^m with $0 \leq m \leq n$, we have

$$\sigma(p^n) = \sum_{i=0}^{n} p^i = \frac{p^{n+1} - 1}{p - 1}.$$

- Since a and b are coprime, all divisor d of ab can be uniquely writen as $d = d_a d_b$ with $d_a | a$ and $d_b | b$. Therefore,

$$\sigma(ab) = \sum_{d|ab} d = \sum_{d_a|a, d_b|b} d_a d_b = \sum_{d_a|a} \sum_{d_b|b} d_a d_b = \left(\sum_{d_a|a} d_a \right) \left(\sum_{d_b|b} d_b \right) = \sigma(a)\sigma(b).$$

Question 3.2 Euclid-Euler Theorem

Prove the following equivalence, known as the Euclid-Euler Theorem:

$$n = 2^{p-1}(2^p - 1) \text{ with } 2^p - 1 \text{ a Mersenne prime } \iff n \text{ is an even perfect number.}$$

Hint: Let $n = 2^k x$ with x odd and n perfect, show that x and $\frac{x}{2^{k+1}-1}$ muss be the only divisors of x.

Answer.

Let $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ prime. Then,

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p - 1}{2 - 1}(2^p - 1 + 1) = (2^p - 1)(2^p) = 2n.$$

Thus, n is a perfect number.

Now, suppose $n = 2^k x$ with x odd, and n is perfect. Then,

$$2^{k+1}x = 2n = \sigma(n) = (2^{k+1} - 1)\sigma(x).$$

Since $2^{k+1} - 1$ is odd, it must divide x. Hence, $\frac{x}{2^{k+1}-1}$ must be a divisor of x. Therefore,

$$\frac{2^{k+1}x}{2^{k+1} - 1} = \sigma(x) = x + \frac{x}{2^{k+1} - 1} + \underbrace{\cdots}_{\text{other divisors}}.$$

The equality holds only if x has no other divisors, meaning x is prime. Additionally, $1 = \frac{x}{2^{k+1}-1}$ implies $x = 2^{k+1} - 1$, which shows x is a Mersenne prime.