Prerequisites Test

Cryptography and Security 2024

Name: ______________________________

SCIPER: ______________________________

- ◇ This document contains **3** independent exercises.
- ◇ **Do NOT open this document until the beginning of the exam**.
- ◇ Duration: **105 minutes** (one hour and forty-five minutes).
- ◇ **This is a closed book exam. No extra sheet is allowed**.
- ◇ Allowed Material: blue or black pen (avoid pencils), eraser. Except for a basic pocket calculator or a non-connected clock, any other kind of electronic device is forbidden.
- ◇ Food and water are allowed but should not disturb the exam when consumed.
- ◇ If needed, additional scrap paper will be provided.
- ◇ **Only answers directly written on the exam sheet will be corrected**.
- ◇ Each answer must be written in English in the dedicated box. If the answer is put at the end, **clearly** indicate which exercise it refers to. In particular, properly separate scrap text from answers to be corrected.
- ◇ Non-trivial statements must be **cleanly and formally justified**.
- ◇ Questions about the (technical) content of the exam will not be answered.
- ◇ **Prepare the CAMPIRO card or an official ID paper for the identity check**.

Exercise 1 Probability

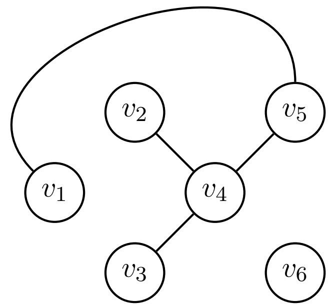

Figure 1: Example graph with 6 vertices ($V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$) and 4 edges ($E = \{\{v_1, v_5\}, \{v_2, v_4\}, \{v_3, v_4\}, \{v_4, v_5\}\}$) where v_6 is an isolated vertex.

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.

Question 1.2 Variance

Compute the variance of number of isolated vertices.

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 $\mathsf{RandSearch}$ algorithm.

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 $o(g)$.

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

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

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

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.