Advanced Algorithms & Complexity (CS G526) Comprehensive Exam, 2022

There are 5 questions in all and total marks are $5 \times 7 = 35$. *This is an open book exam. You can use any printed or handwritten material. Please show all steps of your solution and give full derivation of your results.*

1. The following DTM computes a function $f : \mathbb{N} \to \mathbb{N}$. Find the function f and the *average time-complexity* of the DTM. For computing $f(x)$, the DTM is started in the initial state q_0, scanning the start symbol $\triangleright$, which precedes x written in binary. q_h is the halting state.

$$\begin{aligned}
\delta(q_0, \triangleright) &= (q_1, \triangleright, R) \\
\delta(q_1, 0) &= (q_2, 0, R) \\
\delta(q_1, 1) &= (q_1, 1, R) \\
\delta(q_1, B) &= (q_3, 0, L) \\
\delta(q_2, 0) &= (q_2, 0, R) \\
\delta(q_2, 1) &= (q_2, 1, R) \\
\delta(q_2, B) &= (q_4, B, L) \\
\delta(q_3, 1) &= (q_3, 0, L) \\
\delta(q_3, \triangleright) &= (q_5, \triangleright, R) \\
\delta(q_4, 0) &= (q_h, 1, L) \\
\delta(q_4, 1) &= (q_4, 0, L) \\
\delta(q_5, 0) &= (q_h, 1, L)
\end{aligned}$$

2. In the *RSA Cryptosystem*, an $n-$bit integer N is chosen so that

$$N = pq,$$

where p and q are $\frac{n}{2}$-bit prime numbers. The public key (known to everyone) is (N, e), where e is chosen so that

$$(e, \phi(N)) = 1.$$

The private key (known only to Alice) is (N, d), where d is chosen so that

$$ed \equiv 1(\bmod \phi(N)).$$

To send a plaintext P to Alice, Bob computes and sends the ciphertext C to Alice:

$$C \equiv P^e(\bmod N).$$

To get back the plaintext P, Alice performs the following computation:

$$P \equiv C^d(\bmod N).$$

Prove that Eve can recover P from C in polynomial-time if she has oracle access to the following language:

$$\text{FACTORING } = \{\, (N, L, U) \mid N \text{ has a prime factor } p \text{ in the interval } [L, U] \,\}.$$

3. Let X and Y be numbers that are chosen independently and uniformly at random from $\{0, 1, \ldots, n\}$. Let Z be their sum modulo $n + 1$. Show that X, Y, and Z are pairwise independent but not independent.

4. Let $\psi(x, y) = \exists x \forall y (\overline{x} \vee y) \wedge (x \vee \overline{y})$. Taking the prime $p = 11$, use the efficient arithmetization algorithm (using the $\exists$, $\forall$, and L operators) to arithmetize $\psi(x, y)$.

5. Suppose that you are given a graph G and a number K, and are told that either (i) the smallest vertex cover of G is of size at most K or (ii) it is of size at least $3K$. Show a polynomial-time algorithm that can distinguish between these two cases. Can you do it with a smaller constant than 3? Since VERTEX COVER is `NP-Hard`, why does this algorithm not show that `P = NP`?