International Institute of Information Technology Hyderabad

Modern Complexity Theory (CS1.405)

Assignment 4
Deadline: November 18, 2025 (Tuesday), 17:00 PM
Venue for Hard-copy Submission:
CSTAR, A3-110, Vindhya Block, IIIT Hyderabad
Total Marks: 100

NOTE: It is strongly recommended that no student is allowed to copy from others.
No assignment will be taken after the deadline.
Write the following while submitting ONLY HARDCOPY:

Modern Complexity Theory (CS1.405)
Assignment 4
Name:
Roll No.:

Questions

1. A deterministic polynomial-time oracle Turing machine M^{SAT} may make polynomially many queries to the SAT oracle while deciding a language L. Let the number of oracle queries on input x be $q(|x|)$, where q is polynomial.

   Define the class $P^{SAT[1]}$ as the set of languages decidable by a deterministic polynomial-time machine that is allowed to make *at most one* query to the SAT oracle.

   Prove that: ~~$\mathsf{P}^{SAT} = P^{SAT[1]} = NP$.~~

   $$NP = P^{SAT[1]} \subseteq P^{SAT}.$$

   [10+10]

2. Let ~~$CIRCUIT\text{-}MIN = \{\langle C, k\rangle \mid C$ is a Boolean circuit equivalent to some smaller circuit of size $\leq k\}$.~~
   $CIRCUIT - MIN = \{\langle C, k\rangle \mid$ there is NO circuit of size $\leq k$ equivalent to $C\}$.

   (a) Show that $CIRCUIT - MIN$ is in coNP.

   (b) Prove that $CIRCUIT - MIN$ is coNP-complete.

   Hint: Reduce from the $TAUTOLOGY$ problem. Construct a Boolean circuit whose minimal equivalent size reflects whether a given Boolean formula is always true. **[20]**

3. (a) Prove that
   $$\mathsf{BQP} \subseteq \mathsf{PP}.$$
   That is, show that any language decidable by a bounded-error quantum polynomial-time algorithm can also be decided by a probabilistic Turing machine in polynomial time with unbounded error.

   (b) Suppose it were the case that
   $$\mathsf{NP} \subseteq \mathsf{BQP}.$$
   Explain why this would have significant implications for classical cryptography. In particular, discuss how quantum algorithms such as Shor's algorithm for integer factorization challenge existing computational hardness assumptions, and why most researchers believe that $\mathsf{NP} \not\subseteq \mathsf{BQP}$.

   [10+10]

4. Prove that

$$\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}.$$

That is, show that the class of problems solvable by a zero-error probabilistic polynomial-time algorithm (ZPP) is exactly the intersection of the class of problems solvable by a one-sided error randomized polynomial-time algorithm (RP) and its complement (coRP).

Your proof should include both directions:

(a) Show that $\mathsf{ZPP} \subseteq \mathsf{RP} \cap \mathsf{coRP}$.

(b) Show that $\mathsf{RP} \cap \mathsf{coRP} \subseteq \mathsf{ZPP}$.

[10+10]

5. Consider the RSA cryptosystem where the modulus $n = p \times q$, with p and q being large primes.

(a) Prove that if an adversary can efficiently compute $\varphi(n) = (p-1)(q-1)$ without factoring n, then the adversary can also efficiently factor n.

(b) The RSA cryptosystem relies on the computational hardness of integer factorization.

(i) Explain how Shor's quantum algorithm violates this assumption and describe the general steps by which it factors a composite number $n = pq$.

(ii) Using Shor's algorithm, demonstrate the factorization of $n = 21$ as a numerical example. Clearly show the period-finding process for the function $f(x) = a^x \bmod n$ and how the period r leads to discovering the prime factors of n.

[5+15]

All the best!!!