CSE 431 Winter 2022
Assignment #7

Due: Thursday March 3, 2022, 11:59 PM

Reading assignment: Read Sections 8.1-8.5.

Problems:

1. (20 points) Define

$$THIRD\text{-}CLIQUE = \{\langle G\rangle \mid G \text{ is an undirected graph with } n = 3\ell \text{ nodes for some integer } \ell \text{ and } G \text{ has a clique on } \ell \text{ nodes}\}.$$

   Prove that $THIRD\text{-}CLIQUE$ is NP-complete.
   (Hint: Use the fact the $CLIQUE$ is NP-complete.)

2. (20 points) We noted (but did not prove) that $PRIMES = \{\langle N\rangle \mid N \in \mathbb{N} \text{ is prime}\} \in P$. Let $PRIME\text{-}FACTOR = \{\langle N, k, \ell\rangle \mid N \in \mathbb{N} \text{ has a prime factor } p \text{ with } k \leq p \leq \ell\}$.

   (a) Prove that $PRIME\text{-}FACTOR \in NP \cap coNP$. (You can use the fact that $PRIMES \in P$ though the proof of this inclusion only requires that $PRIMES \in NP$.)

   (b) Show that if $NP \cap coNP = P$ then there is a polynomial-time algorithm that on input, $\langle N\rangle$, the binary representation of an integer N, computes the complete prime factorization of N. (This would break the RSA cryptosystem and systems security methods like TLS that depend on the security of RSA.)

3. (20 points) Many systems can be modelled in terms of interacting finite state machines, which may need to be nondeterministic to encode the fact that we may not precisely control their behavior. Algorithms for the following language turn out to be important for that understanding these systems:

$$A = \{\langle N_1, \ldots, N_k\rangle \mid k \in \mathbb{N},\ N_1, \ldots, N_k \text{ are NFAs with alphabet } \Sigma, \text{ and } \exists w \in \Sigma^* \text{s.t. } w \in L(N_1) \cap \ldots \cap L(N_k)\}.$$

   Show that A is in PSPACE.

4. (20 points) Prove that if every NP-hard language is $PSPACE$-hard then $NP = PSPACE$.

5. (20 points) Let $A_{LBA} = \{\langle M, w\rangle \mid M \text{ is an LBA that accepts input } w\}$. Show that A_{LBA} is PSPACE-complete.

6. (Extra Credit) Define the function MAJORITY:$\{0,1\}^* \to \{0,1\}$ by MAJORITY$(x) = 1$ iff $\geq 1/2$ the bits in x are 1. Let $C_{\text{MAJORITY}} : \mathbb{N} \to \mathbb{N}$ be the smallest function such that for every $n \in \mathbb{N}$, there is a circuit C_n of size at most $C_{\text{MAJORITY}}(n)$ that computes MAJORITY on all strings $x \in \{0,1\}^n$.

   (a) Show that $C_{\text{MAJORITY}}(n)$ is $O(n^2)$.

   (b) Show how to compute the sum of the bits of x using divide and conquer and use this to show that $C_{\text{MAJORITY}}(n)$ is $O(n \log n)$.

   (c) Find another clever idea to show that $C_{\text{MAJORITY}}(n)$ is $O(n)$.