CPSC 421: Introduction to Theory of Computing
Practice Problem Set #4, Not to be handed in

Time hierarchy theorem

1. (Easy) We saw in homework that $TIME(1) = TIME(f(n))$ whenever $f(n) = o(n)$. Explain why this does not contradict the time hierarchy theorem.

2. (Easy) Prove the following statements.

   i. $TIME(2^n) = TIME(2^{n+1})$.
   ii. $TIME(2^n) \subsetneq TIME(2^{2n})$.

3. (Easy) Show that at least one of the following must be true. Either $\mathsf{P} \neq \mathsf{NP}$ or $\mathsf{NP} \neq \mathsf{EXP}$.

NP, NP-hardness, and NP-completeness

4. (Easy) Let X and Y be languages and suppose that $X \leq_P Y$. Which are the following are necessarily true? Briefly justify your answer.

   i. $\overline{X} \leq_P \overline{Y}$.
   ii. If Y is in NP then X is in NP.
   iii. If X is in P then Y is in P.
   iv. If Y is in P then X is in P.
   v. If Y is NP-complete then so is X.
   vi. If X is NP-complete then so is Y.
   vii. If Y is NP-complete and X is in NP then X is NP-complete.
   viii. If X is NP-complete and Y is in NP then Y is NP-complete.
   ix. X and Y cannot both be NP-complete.

5. (Easy) Is P closed under:

   a. union?
   b. concatenation?
   c. complement?
   d. intersection?

6. (Easy) Is NP closed under:

   a. union?
   b. concatenation?
   c. (Extremely Hard and Unsolved) complement?
   d. intersection?

7. (Medium) If $P = \mathsf{NP}$, then every language $A \in P$ (except $A = \emptyset$ and $A = \Sigma^*$) is NP-complete. Why can't $\emptyset$ and Σ^* be NP-complete?

8. (For this question, we are not assuming that $\mathsf{P} \neq \mathsf{NP}$. Also, it makes sense to understand the previous question before trying this one.)

   If A and B are NP-complete, show that:

   a. (Easy) $A \cap B$ need not be NP-complete.

   b. (Medium) $A \cup B$ need not be NP-complete.

9. Let $G = (V, E)$ and $G' = (V', E')$ be (undirected, simple) graphs. An isomorphism between G and G' is a bijection $\phi\colon V \to V'$ such that $(u, v) \in E$ if and only if $(\phi(u), \phi(v)) \in E'$ for every $u, v \in V$. We say that G and G' are *isomorphic* (denoted $G \simeq G'$) if there exists an isomorphism between G and G'. The graph isomorphism problem is the language $\mathsf{GI} = \{\ (G, G') : G \simeq G'\ \}$.

   i. (Easy) Show that $\mathsf{GI} \in \mathsf{NP}$.

   ii. (Open) Is GI NP-complete? Is GI in P?

10. (Easy/medium) Let

$$\mathsf{MODEXP} = \left\{\ (a, b, c, p) : a, b, c, p \text{ are binary integers such that } a^b \equiv c \pmod{p}\ \right\}.$$

    Show that MODEXP is in P.

    Hint: The naive algorithm will not work. Use exponential squaring. As a starting point, suppose b is a power of 2.

Reductions

11. (Easy) Let $U = \{\ \langle M, x, 1^t\rangle : \text{NTM } M \text{ accepts } x \text{ within } t \text{ steps on at least one branch}\ \}$. Show that U is NP-complete.

    Hint: Directly reduce every language $L \in \mathsf{NP}$ to U. It is not necessary to use the Cook-Levin Theorem here.

12. (Easy) Let $k \geq 3$ be a fixed constant. Show that $k\mathsf{SAT}$(the language of satisfiable CNFs where each clause is a disjunction of exactly k literals) is NP-complete.

13. (Easy) Let $\mathsf{DoubleSAT} = \{\ \phi : \phi \text{ has at least two satisfying assignments}\ \}$. Show that $\mathsf{DoubleSAT}$ is NP-complete.

14. (Easy) In this question, all graphs G are undirected. Let

$$\mathsf{SPATH} = \{\ (G, a, b, k) : G \text{ contains a simple path of length at most } k \text{ from } a \text{ to } b\ \}$$

    and

$$\mathsf{LPATH} = \{\ (G, a, b, k) : G \text{ contains a simple path of length at least } k \text{ from } a \text{ to } b\ \}.$$

    i. Show that SPATH is in P.

ii. Show that LPATH is NP-complete.

Hint: The language UHAMPATH $= \{ G : G$ contains a Hamilton path $\}$ is NP-complete. Recall that a Hamilton path in a graph is a path that uses each vertex exactly once. Equivalently, it is a simple path of length $n-1$ where n is the number of vertices in the graph G.

Hint 2: Note that the path in UHAMPATH can start anywhere but the path in LPATH has fixed endpoints so you need to make sure your reduction has some way to deal with this.

15. (Medium) Let Partition be the following language. Given inputs $x_1, \ldots, x_n \in \mathbb{N}$, determine if there is some $S \subseteq [n]$ such that $\sum_{i \in S} x_i = \sum_{i \notin S} x_i = \frac{1}{2} \sum_{i \in [n]} x_i$. Show that Partition is NP-complete.

16. (Medium) A dominating set in a graph $G = (V, E)$ is a set $S \subseteq V$ such that for all $v \in V$, either $v \in S$ or one of its neighbours is in S. Show that deciding if a graph G has a dominating set of size k is NP-complete.

17. (A puzzle game)

    i. (Medium) Consider the following puzzle. You are given a rectangle of dimension $A \times B$ and n smaller rectangles of size $a_1 \times b_1, \ldots, a_n \times b_n$. Your goal is to determine if we can fit all the small rectangles exactly into the big rectangle with no gaps. In other words, all the small rectangles are in the big rectangle and there is no extra space in the big rectangle. You may rotate the small rectangles by 90 degrees if you wish but no other rotations are allowed. Show that this puzzle game is NP-complete.

    Hint: Reduce from Partition. The Partition problem is as follows. Given a sequence of n positive integers $a_1, \ldots, a_n$, determine if there exists a subset $S \subseteq [n]$ such that $\sum_{i \in S} a_i = \sum_{i \in \overline{S}} a_i$.

    ii. (Medium/Hard) Same question as before but now the big rectangle is restricted to being a square.

    iii. (Hard) Same question as part (a) but now all rectangles are restricted to being squares.

Miscellaneous problems

18. (Easy/Medium) Let

    $U = \{ \langle M, x, t \rangle : t$ is in binary and NTM M accepts x within t steps on at least one branch $\}$.

    Show that U is NEXP-complete.

19. (Hard, but a great exercise on nondeterminism) Let PRIMES $= \{ p : p$ is in binary and p is prime $\}$. Show that PRIMES $\in$ NP.

    Hint: Use the following fact. A number p is prime if and only if the following holds. Let $p_1, \ldots, p_k$ be the prime factors of $p-1$. For some $a \in \{1, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$ but $a^{(p-1)/p_i} \not\equiv 1 \pmod{p}$ for all $1 \leq i \leq k$. (If you have taken undergraduate algebra, it might be helpful to think about the Chinese Remainder Theorem.)

20. (Tricky) Let $L = \{ M : M$ is a TM that halts in $O(n^2)$ time $\}$. Show that L is undecidable.