18.404/6.840 Michael Sipser
Theory of Computation
Due 2:30pm sharp, Thursday, November 8, 2018

Problem Set 4

Read all of Chapter 7.

1. Let $MODEXP = \{\langle a, b, c, p\rangle \mid a, b, c, p$ are positive binary integers such that $a^b \equiv c \pmod{p}\}$. Show that $MODEXP \in \text{P}$.

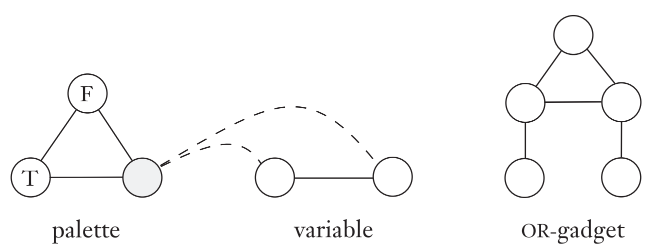
2. Let $SHUFFLE =$
$\{\langle w, x, y\rangle \mid w{=}a_1b_1 \cdots a_kb_k$ for $k \geq 0$ where $x{=}a_1a_2 \cdots a_k$ and $y{=}b_1b_2 \cdots b_k$, each $a_i, b_i \in \Sigma^*\}$. Note, the a_i and b_i may be strings, not just symbols. It is easily seen that $SHUFFLE \in \text{NP}$. Show that $SHUFFLE \in \text{P}$.

3. Show that if P = NP, then every language $A \in \text{P}$, except $A = \emptyset$ and $A = \Sigma^*$, is NP-complete.

4. Show that if P = NP, a polynomial time algorithm exists that produces a satisfying assignment when given a satisfiable Boolean formula. (Note: The algorithm you are asked to provide computes a function, and NP contains languages, not functions. The P = NP assumption implies that SAT is in P, so testing satisfiability is solvable in polynomial time. But the assumption doesn't say how this test is done, and the test may not reveal satisfying assignments. You must show that you can find them anyway. Hint: Use the satisfiability tester repeatedly to find the assignment bit-by-bit.)

5. Let $SET\text{-}SPLITTING = \{\langle S, C\rangle \mid S$ is a finite set and $C = \{C_1, \ldots, C_k\}$ is a collection of subsets of S, where the elements of S can be colored *red* or *blue* so every C_i has at least one red element and at least one blue element$\}$. Show that $SET\text{-}SPLITTING$ is NP-complete.

6. A ***coloring*** of a graph is an assignment of colors to its nodes so that no two adjacent nodes are assigned the same color. Let $3COLOR = \{\langle G\rangle \mid G$ is colorable with 3 colors$\}$. Show that $3COLOR$ is NP-complete. (Hint: Use the following three subgraphs.)



7.* (Optional) Let $A \subseteq \mathtt{1}^*$. Show that if A is NP-complete then P = NP.
(Hint: Consider a reduction from SAT to A, and consider formulas such as ϕ_{0100} which set the first 4 variables x_1, x_2, x_3, x_4 in ϕ to the values $0, 1, 0, 0$ respectively.)