15-251: Great Theoretical Ideas In Computer Science

Recitation 9 : P and NP

New Phrases

- We say a problem is in **NP** if there exists a polynomial time verifier TM V and a constant $k > 0$ such that for all $x \in \Sigma^*$:

  if $x \in L$, then there exists a certificate u with $|u| \leq |x|^k$ such that $V(x, u)$ accepts.

  if $x \notin L$, then for all $u \in \Sigma^*$, $V(x, u)$ rejects.

- We say there is a **polynomial-time many-one reduction** from A to B if there is a **polynomial-time** computable function $f : \Sigma^* \to \Sigma^*$ such that $x \in A$ if and only if $f(x) \in B$. We write this as $A \leq_m^P B$. (We also refer to these reductions as Karp reductions.)

- A problem Y is **NP-hard** if for every problem $X \in$ **NP**, $X \leq_m^P Y$.

- A problem is **NP-complete** if it is both in **NP** and **NP-hard**.

No Privacy

DOUBLE-CLIQUE: Given a graph $G = (V, E)$ and a natural number k, does G contain two vertex-disjoint cliques of size k each?

Show DOUBLE-CLIQUE is **NP-Complete**.

No Peeking

A vertex covering of a graph is a subset of the vertices such that each edge in the graph is incident to at least one vertex in the subset. A subset of the vertices of a graph is called an independent set if there is no edge between any two vertices in the subset.

VERTEX-COVER: $\{\langle G, k\rangle : G \text{ is a graph}, k \in \mathbb{N}^+, G \text{ contain a vertex covering of size } k\}$

IND-SET: $\{\langle G, k\rangle : G \text{ is a graph}, k \in \mathbb{N}^+, G \text{ contains an independent set of size } k\}$

Show that VERTEX-COVER Karp reduces to IND-SET

(Extra) Never Pausing

Prove that the Halting Problem is **NP-hard**.