CS 1010 Lecture 15
P, NP, and NP-completeness
10/25

Language definitions:
- \( \text{Path} = \{ (G, s, t) \mid G \text{ is a directed graph}, s, t \in V(G), \text{there is a path from } s \text{ to } t \text{ in } G \} \)
- \( \text{RelPrime} = \{ (a, b) \mid a, b \in \mathbb{Z} \text{ and } \gcd(a, b) = 1 \} \)
- \( \text{HAMPATH} = \{ (G, s, t) \mid G \text{ is a directed graph}, s, t \in V(G) \text{ and } \exists \text{ a path from } s \text{ to } t \text{ visiting each vertex } v \in V(G) \text{ exactly once.} \} \)
- \( \text{PrefixOfFactorization} = \{ (p, f) \mid p \text{ is an int, } \text{in binary } f \text{ is a binary string starting } 0, s, t \text{ is a prime } p, p | n \text{ and } f \text{ is a prefix of } p \} \)

Recap:
- \( \text{Time}(t(n), \text{NTime}(t(n)) \)

Def:
- \( D = \bigcup_{k=0}^{\infty} \text{Time}(n^k) \)
- Interesting b/c:
  - "efficiently" decidable languages are in \( D \)
  - model-independent: polytime on a TM is also polytime on a multi-tape turing machine or a RAM.
  - Languages not in \( D \) are interesting b/c not efficiently decidable.

Def:
- \( \text{NP} = \bigcup_{k=0}^{\infty} \text{NTime}(n^k) \)

Example: \( \text{HAMPath} \in \text{NP} \) b/c
  - on input \( (G, s, t) \)
    - non-deterministically pick a sequence of vertices \( u_1, \ldots, u_k \) where \( k \leq |V(G)| \)
    - Check that \( u_1, \ldots, u_k \) is a Hamiltonian path:
      - \( u_1 = s, u_k = t \)
      - \( (u_i, u_{i+1}) \in E(G) \) for \( 1 \leq i < k \)
      - and each vertex in the path is unique.
    - If so, accept; else, reject.
Let $A$ be a language. A verifier $V$ for $A$ is a TM $s.t.$
$A = \{w \mid \text{some } c \text{ s.t. } V \text{ accepts } \langle w, c \rangle \}$

$V$ is a poly-time verifier if its runtime is polynomial in $|w|$.

DEF: $NP_2 = \{ L \mid L \text{ has a poly-time verifier} \}$

THM: $NP_1 \subseteq NP_2$

PF: $NP \subseteq NP_2$ b/c

Let $N$ be a poly-time NTM deciding $L$.

Verifier for $L$:

"on input $\langle w, c \rangle$"
- Simulate $N$ on $w$ using $c$ to pick the transitions on every step
- If $N$ accepts, accept. Else, reject.

$NP \subseteq NP_2$

Suppose $V$ is a poly-time verifier for $L$. Then there is an NTM for $L$:

"on input $w$"
- Non-det. Pick a length $p(|w|)$ certificate $c$.
- Run $V(w, c)$. Accept if $V$ accepts, reject otherwise.

From now on $NP$ and $NP_2$ will be called $NP$.

Observation: $P \subseteq NP$.

Prefix (off)factorization: Verifier:

"on input $\langle (w, f), p \rangle$"
- Check that $p = 2$ and $p \mid N$
- If so, check that $f$ is a prefix of $p$.
- If so, accept. Else reject.

Thus, prefix (off)factorization $\in NP$.

Conjecture: $P \not\subseteq NP$ (If it were, we could factor in poly-time, which hasn't been done).
P=NP?  open problem
CS religion: P \neq NP, but has not been proven.

Two possibilities:

- P=NP
- P \neq NP, but has not been proven.

More definitions:

- Def: A \leq_P B if \exists a polynomial-time computable f s.t. \forall x, f(x) \in B \iff f(x) \in A

- Def: A is NP-hard if \forall \text{LENP}, L \leq_P A
- Def: A is NP-complete if \text{ACNP} and \text{ACNP} \leq_P A

Some examples:

- Let G be an undirected graph: G=(V,E)
  - K-clique in G is a subset C \subseteq V s.t.
    \forall u, v \in C, (u,v) \in E, |C|=k
  - K-independent set: I \subseteq V s.t. |I|=k and \forall u, v \in I, (u,v) \notin E
  - K-vertex cover: C \subseteq V, |C|=k, s.t. \forall (u,v) \in E, (u,v) \in C or (v,u) \in C

Their languages:

- CLIQUE = \{ \langle G, k \rangle | G \text{ is undirected graph, w/a K-clique} \}
- INDEPENDENT-SET = \{ \langle G, k \rangle | \text{w/a K-independent set} \}
- VERTEX-COVER = \{ \langle G, k \rangle | \text{w/a K-vertex cover} \}

Claim: CLIQUE \leq_P INDEPENDENT-SET
Be: reduction f:

- On input \langle G, k \rangle
  - G' = (V',E') where \n    V' = V
    E' = \{(u,v) | (u,v) \in E\}
    K' = k

Output \langle G', k' \rangle

Analysis: Let C be a K-clique in G, then X = \{(u,v) \in V_{K} \times V_{K} | (u,v) \in E\}

\forall (u,v) \in X, (u,v) \in E, (u,v) \in E' \iff (v,u) \in E' \iff (v,u) \in E

\forall (u,v) \in X, (v,u) \notin E \iff (v,u) \notin E' \iff (v,u) \notin E'

\forall (u,v) \in X, (u,v) \in E \iff (u,v) \in E'

\forall (u,v) \in X, (u,v) \notin E \iff (u,v) \notin E'

Symmetry for the reverse.
Claim: \text{Indep. Set} \leq_p \text{Vertex Cover}

Proof: Reduction \textit{f}:

on input \( \langle G, K \rangle \)

output \( \langle G', |V(G)| - K \rangle \)

Analysis: Let \( I \) be \( \text{Indep. Set} \) of \( G \). Then any edge \((u,v) \in E(G)\) must have either \( u \in V \setminus I \) or \( v \in V \setminus I \).

Therefore, \( V \setminus I \) is a \((|V(G)| - K)\)-vertex cover.

Other direction similar.

Similar reductions show \( \text{Indep. Set} \leq_p \text{Clique} \)

and \( \text{Vertex Cover} \leq_p \text{Indep. Set} \).