Review

- PCP is undecidable
- Gödel's Incompleteness Theorem
- Hilbert 10^{th} Problem

Computational Complexity

- **Given a decision problem, understand the resources required to solve it. Resources include time, space, randomness, parallelism, etc.**
- Understand the relation between various problems is mainly by **reduction**.

P

Def 5.1 **Let $T:\mathbb{N}\to\mathbb{N}$, language $L\in DTIME(T(n))\Leftrightarrow$ there exists a (multitape) TM that runs in time $O(T(n))$ and decides L.**

Def 5.2

$$P=\cup_{c\geq 1}DTIME(n^c)$$
$$EXP=\cup_{c\geq 1}DTIME(2^{n^c})$$

Examples:

1. *Shortest Path Problem*: $O(|v|^2),O(|E|+|v|\log|v|)$
2. *Minimum Spanning Tree Problem*: $O(|E|\log|v|),O(|E|+|v|\log|v|)$
3. *Maximum Flow Problem*:
   - *Edmond's*: $O(|v||E|^2)$
   - *Push-Relabel*: $O(|v|^3)$
   - *CKLPGS*: $O(|E|^{1+O(1)})$
4. *Linear Programming*: $\tilde{O}((n^\omega+n^{2.5-\frac{\alpha}{2}}+n^{2+\frac{1}{6}})\cdot L)$, $O(n^{2.5})$
5. *BFS/DFS*: $O(|v|+|E|)$
6. *String Matching Problem*: $O(n)$

Thm 5.3 **Let** $PATH=\{\langle G,s,t\rangle | G\ is\ a\ directed\ graph,\ and\ there\ is\ a\ path\ from\ s\ to\ t\}$. $PATH\in P$.

Thm 5.4 **Let** $RELPRIME=\{\langle x,y\rangle | x\ and\ y\ are\ relatively\ prime\}$. $RELPRIME\in P$.

Proof: Use $Euclid\ GCD(x,y)$. Let $x>y$.

1. While $y>0$, $x\leftarrow x\ mod\ y$
2. Swap x,y
3. When loop ends, return x

Obviously, x drops at least by half every 2 iterations. #iterations $= O(\log_2 x) = O(\log_2 2^{O(l)}) = O(l) = O(n)$. In each iteration, mod takes $O(n^2)$. In total, it takes $O(n^3)$.

Thm 5.5 **Let $PRIME = \{x | x\ is\ a\ prime\ number\}$. $PRIME \in EXP$.**

Proof: #iterations$\leq 2^n$, each iteration takes $O(2^n)$. In total, it takes about $O(2^{O(n)})$.

Thm 5.6 $PRIME \in P$

NP

- **NP stands for Non-deterministic Polynomial.**

Def 5.7 **Language $L \subseteq \{0,1\}^*$ is in NP if there exists a polynomial $P: \mathbb{N} \to \mathbb{N}$ and a polynomial-time TM M called the verifier for L, s.t. for every $x \in \{0,1\}^*, x \in L \Leftrightarrow \exists w \in \{0,1\}^{P(|x|)}$ s.t. $M(x,w) = 1$.**

- Such w is called a **certificate** or **witness** for x.

Example 5.8 $Graph\ Isomorphism \in NP$.

- $Graph\ Isomorphism = \{\langle G, H\rangle | Undirected\ graph\ G\ and\ H\ are\ isomorphic\}$

Example 5.9 $CLIQUE \in NP$.

- $CLIQUE = \{\langle G, k\rangle | G\ contains\ K_k\ subgraph\}$

Example 5.10 $Travelling\ Salesman \in NP$.

- $Travelling\ Salesman$: Given a set of n nodes, use $d_{i,j}$ to denote the distance between node i and j, and for a number k, decide if there exists a closed tour that visits every node exactly once and the total length $\leq k$.

Examples 5.11 5.12 5.13 **Below are also some NP problems:**

- Given N, l, u, decide if N has a prime factor in $[l, u]$.
- (*0/1 Integer Programming*) Given m linear inequalities with integral coefficients over n variables $u_1, u_2, \ldots, u_n$. Decide if there is an assignment of $0s$ and $1s$ to $u_1, u_2, \ldots, u_n$, which satisfies the inequalities.
- (*Subset Sum*) Given a set of n integers $A = \{A_1, A_2, \ldots, A_n\}$, and a number T. Decide if there is a subset of A that sums up to T.

Examples 5.14 5.15 **Below are conjectured not in NP:**

- (*Graph Non-isomorphism*) $\{\langle G, H\rangle | G \ncong H\}$.
- (*NoClique*) $\{\langle G, k\rangle | G\ does\ not\ have\ a\ K_k\ subgraph\}$.

Theorem 5.16 $P \subseteq NP \subseteq EXP$.