Reduction & completeness group problems together

NP vs. P
Completeness + Reduction

Language: a family of sets
input size $n$
For a fixed $n$, $L(n) \subseteq \{0,1\}^n$
e.g. $x \in \{0,1\}^n$ means $x = (x_1, \ldots, x_n)$ where $x_i \in \{0,1\}$

Decision
Membership Problem
given $y \in \{0,1\}^n$ (given an instance, tell if it
decide if $y \in L(n)$ belongs to a language)
e.g. Prime $= \{0,1\}^*$
$x \in \text{Prime}$ if $x$ is a prime $\neq 2$ bits
$5 \in (101)_2 \in \text{Prime}$ (3)
$6 \in 110$ does not belong to Prime

Decision Problem for Language $L$ is a unary relation

$m+n$ Binary relations $\times \{0,1\}^{m+n}$
$(x, y)$ where $x \in \{0,1\}^n$
y $\in \{0,1\}^m$

$B \in \{0,1\}^n \times \{0,1\}^m$ 1st component 2nd component
$= B \in \{0,1\}^{n+m}$
What is P?

**Polynomial function**

\( f(n) \) is a polynomial fn. in \( n \) if \( \exists \) a constant \( c \) such that \( f(n) = O(n^c) \)

- \( c \) cannot depend on \( n \) but it could be 1000
- \( n^{\log n} \) is not polynomial in \( n \)
  \[ \log f(n) = \Theta(\log n) \]

So what is \( P \? 
\( L \) is in \( P \) if \( \exists \) an algorithm \( A \) whose running time is polynomial in \( n \) to determine the decision problem for language \( L \)

What is NP?

A binary relation \( B \subset \{0,1\}^* \times \{0,1\}^* \) is in \( P \) if \( m \) is in polynomial in \( n \) and \( \exists \) an Algorithm \( B \) whose running time is polynomial in \( m+n \).
To determine the following question:
Given \((x, y) \in \{0,1\}^* \times \{0,1\}^* \)
   determine if \((x, y) \in B \)

This is a polynomial binary relationship:
\((x, y) \in B \) if \( x \) is a factor of \( y \)
that is \( \exists \) \( z \) such that \( y = x \cdot z \)
For every binary relation \( B \) we can define another language \( L_B \) as:
\[
L_B = \{ x \mid \exists y \in \{0,1\}^m, (x,y) \in B \}
\]

For example, \((x,y) \in \text{Factor}\) if \( y \) is a factor of \( x \):\(^1\)
\[
(\exists \ z \text{ such that } x = y \cdot z)
\]
\[
\text{composite} = L_{\text{factor}} \\
\text{not prime} = L_{\text{factor}} - \text{composite}
\]

If a binary relation \( B \) is a polynomial binary relation then \( L_B \in \text{NP} \).

Like teaching: Prof. Teng shows us proofs from others (Dijkstra, etc.), we verify

NP is a language that someone else can give you evidence;

you just have to verify it.

Zero knowledge proof: Prof. Teng teaches us, we understand.

are "happy" but we can't explain / do the proof by ourselves.

\( L \) is in \( \text{NP} \) if \( \exists \) a polynomial binary relation \( B \)
such that \( L = L_B \).

\[
(\text{Polynomial-time) Reduction})
\]
\[
L_1 \leq_p L_2 \\
\{0,1\}^n \to \{0,1\}^m
\]

\[
\exists \text{ polynomial-time function } f : \{0,1\}^n \to \{0,1\}^m \text{ such that } x \in L_1 \iff f(x) \in L_2
\]

In order to solve \( L_1 \) efficiently, you must be able to solve \( L_2 \)
efficiently — like such optimal substructure
If you can solve $L_2$ in polynomial time, you are already
given a polynomial-time algorithm to solve $L_1$.

**Undirected graph**

Input $G = (V, E)$

**Facebook networks**

- **clique**

4-clique b/c middle 4 nodes are all friends w/each other

**Does $G$ have a k-clique?** (this is an NP problem)

**Independent sets**: A collection of nodes that are completely isolated i.e., they have no edges between them.

**E.g., in the 4-color theorem**, countries of the same color are independent - not next to each other.

$(n, k)$-clique $\leq_p (n, k)$-independent set

$(G, k) \searrow$ like a friend graph to a non-friend graph

$(V, E)$ compliment of a graph $(\overline{G}, k)$

compliment is the $f$ for polynomial-time reduction

$(V, \overline{E})$

$$\overline{E} = \{ (u, v) \in \overline{E} \iff (u, v) \notin E \}$$

can compute compliment in $n^2$ polynomial time.
If $S$ is a clique in $G$ $\implies$ $S$ is an independent set in $G$

### Cook-Levin Theorem

**3-SAT**

**Input** $\phi \in C_1 \land C_2 \land \ldots \land C_m$

$C_i = x_{i_1} \lor x_{i_2} \lor x_{i_3}$

- May or may not have negation

**Options**

$C_i = \neg x_{i_1} \lor \neg x_{i_2} \lor \neg x_{i_3}$

Find an assignment of $x_i \in \{T, F\}$ such that $\phi$ is true

### Cook-Levin:

$NP \leq_P 3\text{-SAT}$