COL 351 Lecture 37 2023/04/17

Topic : Cook – Levin Theorem

NP – hardness and NP – completeness

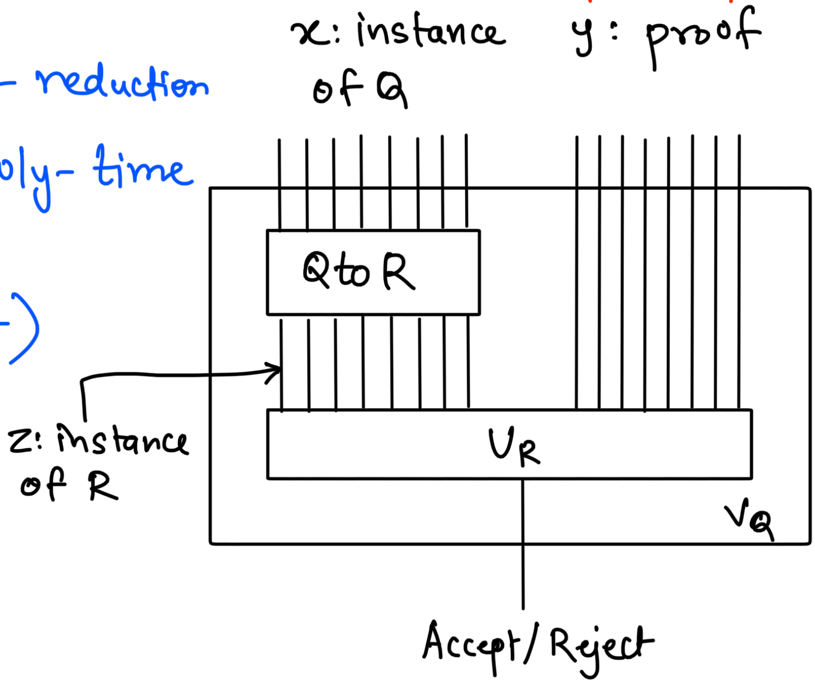
Claim: If $Q \le_{\text{karp}} R$ and $R \in NP$, then $Q \in NP$

Proof: Let QtoR be a Karp – reduction from Q to R. Let V_R be a poly-time verifier for R.

V_Q (x : instance of Q, y : proof)

  $z \leftarrow$ QtoR (x)

  Return V_R (z, y)



x is a yes instance of Q $\iff$ z = QtoR(x) is a yes instance of R $\iff$ $\exists y$ $V_R(z, y)$ accepts $\iff$ $\exists y$ $V_Q(x, y)$ accepts.

Claim: If $Q \le_{\text{karp}} R$ and $Q \notin NP$ then $R \notin NP$.

Claim: If $Q \leq_{Karp} R$ and $R \in \mathbb{P}$ then $Q \in \mathbb{P}$.

Claim: If $Q \leq_{Karp} R$ and $Q \notin \mathbb{P}$ then $R \notin \mathbb{P}$.

Cook-Levin Theorem: Every problem in $\mathbb{NP}$ is Karp-reducible to CIRCUITSAT.

High-Level proof sketch: Suppose $Q \in \mathbb{NP}$. Let V_Q be a poly-time verifier for Q. Given an instance x of Q, construct a circuit C_x whose inputs are the bits of the proof which V_Q would expect. C_x simulates the behavior of V_Q on (x,y), and $C_x(y)$ evaluates to true iff $V_Q(x,y)$ accepts.

(For a more rigorous proof, take COL352 next year.)

Corollary: If CIRCUITSAT $\in \mathbb{P}$ then $\mathbb{P} = \mathbb{NP}$.

Definition: A decision problem H is said to be $\mathbb{NP}$-hard if every problem in $\mathbb{NP}$ is Karp-reducible to H. H is said to be $\mathbb{NP}$-complete if H is $\mathbb{NP}$ and H is $\mathbb{NP}$-hard.

Cook-Levin Theorem (restated): CIRCUITSAT is $\mathbb{NP}$-hard.
($\therefore$ CIRCUITSAT is $\mathbb{NP}$-complete).

Claim: If $Q \leq_{Karp} R$ and Q is $\mathbb{NP}$-hard, then R is $\mathbb{NP}$-hard.

Proof: Every problem in $\mathbb{NP}$ is Karp-reducible to Q. We are also given $Q \leq_{Karp} R$. $\therefore$ By transitivity, every problem in $\mathbb{NP}$ is Karp-reducible to R.

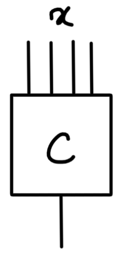
An $\mathbb{NP}$-hard problem that is unlikely to be in $\mathbb{NP}$:

Input: Boolean circuit C with an m-bit input x and an n-bit input y.

Output: Does there exist x such that for all y $C(x,y)$ evaluates to TRUE?

Check: If this problem is in $\mathbb{NP}$, then $\mathbb{NP} = \mathrm{co}\mathbb{NP}$.

Karp reduction from CIRCUITSAT to this problem:

On input 

output