$\mathbb{P}$, $\mathbb{NP}$, & $\mathbb{P}/poly$

Could $\mathbb{NP} \subseteq \mathbb{P}/poly$?

Grand challenge: Circuit lower bounds for $\mathbb{NP}$

Thm [Karp-Lipton 80]:

If $\mathbb{NP} \subseteq \mathbb{P}/poly$, then $\mathbb{PH}$ collapses to Σ_2^P.

Proof: Suppose $\mathbb{NP} \subseteq \mathbb{P}/poly$.

There exists a circuit family of size $p(n)$ that decides SAT.

polynomial

We will prove $\Pi_2^P \subseteq \Sigma_2^P$ (implies collapse)

$$\Pi_2\text{-SAT} = \{ \langle \phi(x_1, x_2) \rangle \mid \forall\, x_1 \in \{0,1\}^n\ \exists\, x_2 \in \{0,1\}^n \text{ s.t. } \phi(x_1, x_2) \text{ is true} \}$$

We will prove that $\Pi_2\text{-SAT} \in \Sigma_2^P$

$$\langle \phi \rangle \quad \forall x_1 \underbrace{\boxed{\exists x_2 \ \phi(x_1, x_2) \text{ is true}}}_{\text{instance of SAT}}$$

$$\forall x_1 \, [\, \phi(\underbrace{x_1}_{\text{fixed}}, \overset{\text{free}}{\bullet}) \in SAT \,]$$

$$\forall x_1 \, [\, \underbrace{\langle \phi_{x_1}(x_2) \rangle}_{\text{of polynomial size } \lesssim n} \in SAT \,]$$

There is a circuit C_n of size $p(n)$ that decides SAT. $\phi(x_1, x_2) \in \Pi_2\text{-SAT}$ iff

$$\exists \underbrace{\langle C_n \rangle}_{\text{SAT solver}} \; \forall x_1 \, [\, C_n(\langle \phi_{x_1} \rangle) = 1 \,]$$

<u>Clm</u>: Given a circuit C and a formula Φ, there is a deterministic poly-time TM M that either:

(1) Finds a satisfying assignment for Φ ACCEPT

(2) OR (Determines that Φ is NOT satisfiable REJECT

OR Determines that C is not a SAT solver)

<u>Proof (sketch)</u>: Run C on Φ. If output is 1, fix first variable to both choices, and ~~call~~ run C on both.

Find a fix (setting) that makes Φ satisfiable, continue / recurse.

If both outputs are zero, reject.

We will prove: $\phi(x_1, x_2) \in \Pi_2\text{-SAT}$ iff

$$\exists \langle C_n \rangle \; \forall x_1 \; [\, M(\langle C_n \rangle, \langle \Phi_{x_1} \rangle) \text{ accepts}]$$

$(\Rightarrow)$ $\Phi(x_1, x_2) \in \Pi_2\text{-SAT}$

Let C_n be a $p(n)$ sized ~~sat~~ SAT solver.
(exists because $\mathbb{NP} \subseteq \mathbb{P}/poly$)

Because $\phi(x_1, x_2) \in \Pi_2\text{-SAT}$, $\forall x_1 \; \langle \Phi_{x_1} \rangle \in SAT$

Hence $M(\langle C_n \rangle, \langle \Phi_{x_1} \rangle)$ will find a ~~test~~ satisfying assignment.

$(\Leftarrow)$ ~~$\Phi(x_1, x_2)$~~ $\exists \langle C_n \rangle \; \forall x_1 \; [M(\langle C_n \rangle, \langle \Phi_{x_1} \rangle)$ accepts$]$

$\forall x_1$ M discovers a satisfying assignment for ~~$\langle \Phi_{x_1} \rangle$~~ Φ_{x_1}.

Hence $\forall x_1 \; \langle \Phi_{x_1} \rangle \in SAT$.

$$\forall x_1 \; \exists x_2 \; \Phi(x_1, x_2) \text{ is true}$$

$$\Rightarrow \Phi(x_1, x_2) \in \Pi_2\text{-SAT}$$

$\blacksquare$