Umans

Karp-Lipton Theorem:

SAT = P/poly implies

Collapse of Polynomial-Time Hierarchy

Karp-Lipton Theorem

- We know that **P** = **NP** implies SAT has polynomial-size circuits.

  (showing SAT does *not* have poly-size circuits is one route to proving **P** $\neq$ **NP**)
- **P/poly** = Family of languages recognized by polynomial size boolean circuits
- Suppose SAT has poly-size circuits, so:

  $$\text{SAT} \in \textbf{P/poly}$$

  – Any consequences?

  – Will show: SAT $\in$ **P/poly** $\Rightarrow$ **PH** collapses

Recall Polynomial-Time Hierarchy PH

$$\Sigma_0 = \Pi_0 = \mathbf{P}$$

$\Delta_1 = \mathrm{P}^{\mathrm{P}}$	$\Sigma_1 = \mathrm{NP}$	$\Pi_1 = \mathrm{coNP}$
$\Delta_2 = \mathrm{P}^{\mathrm{NP}}$	$\Sigma_2 = \mathrm{NP}^{\mathrm{NP}}$	$\Pi_2 = \mathrm{coNP}^{\mathrm{NP}}$
$\Delta_{i+1} = \mathrm{P}^{\Sigma_i}$	$\Sigma_{i+i} = \mathrm{NP}^{\Sigma_i}$	$\Pi_{i+1} = \mathrm{coNP}^{\Sigma_i}$

Polynomial Hierarchy $\mathbf{PH} = \cup_i \Sigma_i$

Recursive Definition of Polynomial-Time Hierarchy PH

$$\Sigma_0 = \Pi_0 = P$$

$$\Delta_{i+1} = P^{\Sigma_i} \quad \Sigma_{i+i} = NP^{\Sigma_i} \quad \Pi_{i+1} = coNP^{\Sigma_i}$$

Polynomial Hierarchy **PH = $\cup_i \Sigma_i$**

- Example:
  - MIN CIRCUIT: given Boolean circuit C, integer k; is there a circuit C' of size at most k that computes the same function C does?
  - MIN CIRCUIT $\in \Sigma_2 = P^{NP}$

SAT is Self-Reducible

Lemma: SAT is Self-Reducible

Proof:

Let $\boldsymbol{\varphi(x_1,x_2,\ldots,x_n)}$ be a Boolean Formula of n variables $\mathbf{x_1,x_2,\ldots,x_n}$.

Recall $\boldsymbol{\varphi(x_1,x_2,\ldots,x_n)} \in$ SAT iff $\boldsymbol{\varphi(x_1,x_2,\ldots,x_n)}$ has a satisfying Boolean variable assignment.

Fixing $\mathbf{x_1=0}$ gives $\boldsymbol{\varphi(0,x_2,\ldots,x_n)}$.
Fixing $\mathbf{x_1=1}$ gives $\boldsymbol{\varphi(1,x_2,\ldots,x_n)}$.

Hence: $\boldsymbol{\varphi(x_1,x_2,\ldots,x_n)} \in$ SAT iff

$\boldsymbol{\varphi(0,x_2,\ldots,x_n)} \in$ SAT OR $\boldsymbol{\varphi(1,x_2,\ldots,x_n)} \in$ SAT

QED

Karp-Lipton Theorem

Theorem (KL):

If SAT $\in$ **P/poly** (SAT has poly-size circuits) then **PH** collapses to the second level.

Proof:

Suffices to show $\Pi_2 \subset \Sigma_2$

L $\in$ Π_2 implies L expressible as:

$L = \{ x : \forall y \, \exists z \, (x, y, z) \in V \}$ with $V \in P$.

poly time verifier

Proof of Karp-Lipton Theorem

$L \in \mathbf{\Pi_2}$ implies L expressible as: $L = \{ x: \forall y \exists z\ (x, y, z) \in V \}$

Given (x, y), "$\exists z\ (x, y, z) \in V$?" is in **NP**

poly time verifier

Recall: P/poly = Languages accepted by polynomial time oracle TMs with polynomial advise.

Also P/poly = Languages accepted by Boolean circuit families of polynomial size.

So if SAT $\in$ P/poly, then SAT is solved by a Boolean circuit family C of polynomial size.

Proof Trick: We will existentially guess poly size circuit family C that solves SAT, then use self-reducibility of SAT

Proof of Karp-Lipton Theorem

Given $L = \{x : \forall y\, \exists z\, (x, y, z) \in V\}$ with $V \in P$:

Claim: if SAT $\in$ P/poly, then let C be poly size circuit family solving SAT.

$L = \{x : \exists C\, \forall y$ [use poly size circuit in C to repeatedly to **find** some z for which $(x, y, z) \in V$; accept iff $(x, y, z) \in V$] $\}$

Proof sketch:

If $x \in L$:

- some poly size circuit family C decides SAT

  $\Rightarrow \exists C\, \forall y$ [...] accepts

If $x \notin L$:

- $\exists y \forall z\, (x, y, z) \notin V \Rightarrow \exists C\, \forall y$ [...] rejects