02/11/21 :

We saw that $P \subsetneq P/poly$

HOLY GRAIL: Is $P \neq NP$?

Harder question: Is $NP \not\subseteq P/poly$?

if you separate NP from P/poly

$\Rightarrow P \neq NP$.

What happens if $NP \subseteq P/poly$?

Thm: [Karp-Lipton '80]

if $NP \subseteq P/poly$ then $PH = \Sigma_2^P$.

What happens if $PH \not\subseteq P/poly$?

This implies. $P \neq NP$.

if $P = NP$ then $PH = P = NP$

$P = NP = coNP = PH \subseteq P/poly$..

Proof of Karp-Lipton Thm :-

Assumption $\quad NP \subseteq P/Poly.$

To prove: $\quad PH = \Sigma_2^P$

It suffices to prove that $\Sigma_2^P = \Pi_2^P$.

Further it suffices to prove that $\Pi_2^P \subseteq \Sigma_2^P$.

$\Pi_2^P \subseteq \Sigma_2^P \Rightarrow \Sigma_2^P = \Pi_2^P$. (Easy)

Let's consider Π_2^P- complete language : Π_2- SAT

$$\forall x_1 \in \{0,1\}^{p(n)} \; \exists x_2 \in \{0,1\}^{p(n)} \text{ s.t.}$$

$$\varphi(x_1, x_2) = 1.$$

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

$$\Sigma_2\text{- SAT} := \{ \langle \psi(x_1, x_2) \rangle \mid \exists x_1 \in \{0,1\}^{p(n)} \; \forall x_2 \in \{0,1\}^{p(n)} \text{ s.t. } \psi(x_1, x_2) \text{ is true} \}$$

To show $\Pi_2^P \subseteq \Sigma_2^P$.

it suffices to show that Π_2- SAT can be recognized in Σ_2^P.

$\forall\, x_1 \in \{0,1\}^{p(n)}$ $\boxed{\exists\, x_2 \in \{0,1\}^{p(n)} \text{ s.t. } \varphi(x_1, x_2) = 1.}$

let's fix x_1.

$$\exists\, x_2 \in \{0,1\}^{p(n)} \text{ s.t. } \varphi(\underset{\substack{\uparrow\\ \text{fixed}}}{x_1}, x_2) = 1.$$

$\langle \varphi \rangle \in \Pi_2\text{-SAT} \iff \forall\, x_1,\ \varphi(x_1, x)$ is satisfiable

Assumption : $NP \subseteq P/poly$ ($\Rightarrow$ SAT has poly-size ckt)

$\Rightarrow \exists$ a circuit C of poly-size s.t. $C(\varphi(x_1, x))$

outputs whether $\varphi(x_1, x)$ is satisfiable or not.

$$\langle \varphi \rangle \in \Pi_2\text{-SAT} \iff \exists\, C \in \{0,1\}^{q(n)}\ \forall\, x_1 \in \{0,1\}^{p(n)}$$

?? Is this correct!

$\Rightarrow$ ✓ s.t. $C(\varphi(x_1, x)) = 1.$

$\Leftarrow$ X

C is of polynomial size in input-length.
when the input is $\langle \varphi(x_1, x) \rangle$ s.t.

$$|\langle \varphi(x_1, x) \rangle| = q'(n)$$

if $\langle \varphi \rangle \in \Pi_2\text{-SAT}$ then is Σ_2^P-algorithm correct?

$NP \subseteq P/poly \Rightarrow SAT := \{\langle \varphi \rangle \mid \varphi \text{ is satisfiable}\}$

has poly-size ckt family $\{C_n\}$

if $\langle \varphi(x_1, x_2) \rangle \in \Pi_2 - SAT$

$\Rightarrow \forall x_1 \in \{0,1\}^{p(n)}$ $\boxed{\exists x_2 \in \{0,1\}^{p(n)} \text{ s.t. } \varphi(x_1, x_2) = 1}$.

$\Rightarrow \forall x_1 \in \{0,1\}^{p(n)}$ $\boxed{\varphi(x_1, x) \text{ is Satisfiable}}$.

$\Rightarrow \forall x_1 \in \{0,1\}^{p(n)} \quad C(\varphi(x_1, x)) = 1.$

what happens if $\langle \varphi(x_1, x_2) \rangle \notin \Pi_2 - SAT$

$\Rightarrow \exists x_1 \in \{0,1\}^{p(n)} \; \forall x_2 \in \{0,1\}^{p(n)} \; \varphi(x_1, x_2) = 0$

Suppose our guessed ckt C is such that
on all input it outputs 1.

So we need to be able to verify that the
guessed ckt C is indeed a ckt for
SAT.

We need a certificate of Satisfiability from
the ckt C.

<u>Claim</u>:- Assuming $\exists$ a ckt of size s solving
SAT on instances with n variables.
Then, $\exists$ another ckt C' of size $O((s \cdot n)^2)$

s.t. C' on input φ outputs a satisfying assignment if φ is satisfiable.

or outputs an all zero string.

Proof:- Algo:- Input φ.

Step 1:- Checks if φ is satisfiable or not using C.

Step 2:- if φ is satisfiable then decide $\varphi(y_1 = 1, y_2, \ldots, y_n)$ is satisfiable. using C.

if yes then set $y_1 = 1$

otherwise set $y_1 = 0$

Step 3:- Go back to step 2.

This algorithm takes. $O((n+1) \cdot s)$ time.

From $P \subseteq P/poly$ we get $\exists$ a ckt C' of size. $O((n \cdot s)^2)$.

Getting back to Σ_2^P-algo: it guesses C' instead of C.

$\langle \varphi(x_1, x_2) \rangle \in \Pi_2\text{-SAT} \iff \exists\ c' \in \{0,1\}^{q^2(n)}$

Σ_2^P-characterisation $\begin{cases} \forall\ x_1 \in \{0,1\}^{p(n)} \\ \text{s.t. } \varphi(x_1, \underbrace{c'(\varphi(x_1, x))}_{x_2}) = 1 \end{cases}$

Suppose $\langle \varphi(x_1, x_2) \rangle \notin \Pi_2\text{-SAT}$

$\Rightarrow \exists\ x_1\ \ \forall\ x_2\ \ \varphi(x_1, x_2) = 0.$

This shows. $\Pi_2\text{-SAT} \in \Sigma_2^P$

$\Rightarrow \Pi_2^P \subseteq \Sigma_2^P$

∎

Thm :- (Meyer's Thm) If $\Sigma XP \subseteq P/Poly$

then $\Sigma XP = \Sigma_2^P$

Cor :- if $P = NP$ then $EXP \notin P/Poly$.

(converting upper bounds into lower bounds).

Proof: if $P = NP \Rightarrow PH = P = NP$

$\Rightarrow P = \Sigma_2^P$ —

Suppose $EXP \subseteq P/Poly$ then Meyer's thm implies $\Sigma XP = \Sigma_2^P$ —

$\Rightarrow P = \Sigma XP$ But this is a contradiction to deterministic time Hierarchy.

(Non)-Deterministic time Hierarchy.

$$\mathrm{DTIME}(T(n)) \subsetneq \mathrm{DTIME}(T(n)\log T(n))$$

— × — × —

Q: Are there Boolean functions $f: \{0,1\}^n \to \{0,1\}$ that require large circuits?

if we prove that $\exists f_n : \{0,1\}^n \to \{0,1\} \in NP$

s.t. f_n requires more than poly-size ckt.

then $NP \not\subseteq P/poly$.

[Current Best lower bound. $\exists$ a function $\in NP$ s.t. it needs ckts of size $5n$.]

Thm:- Almost all Boolean functions on n-variables require ckts of size $\frac{2^n}{10n}$.

$f: \{0,1\}^n \to \{0,1\}$ — Boolean function on n variable.

Boolean function on n-vars $= 2^{2^n}$

How many ckts are there over n-variables of size at most s ?

$g_1, \ldots, g_s$

$g_1, \ldots, g_n = \{x_1, \ldots, x_n\}$

For other gates $n+1 \leq i \leq s$,

you need to assign g_i a label in $\{\vee, \wedge, \neg\}$

and you have to assign two inputs to g_i

$$\Big(\underbrace{(n+3)\cdot\binom{s}{2}}_{\text{\# choices for each gate}}\Big)^s \quad \text{or,} \quad \left(3\cdot\binom{s}{2}\right)^s$$

total # ckts of size at most s over n-variables $\leq \left(3\binom{s}{2}\right)^s$

$$\leq \left(3\cdot s^2\right)^s$$

$$s = \frac{2^n}{10n}$$

$$(3 \cdot S^2)^S = \left(3 \cdot \frac{2^n}{10 \cdot n}\right)^{2 \cdot \frac{2^n}{10 \cdot n}}$$

$$\leq \frac{2^{n \cdot \frac{2^n}{5n}}}{2^{O(\log n) \cdot \frac{2^n}{5n}}}$$

$$= 2^{\frac{1}{5} \cdot 2^n - \frac{2^n}{n} \cdot O(\log n)}$$

$$\leq 2^{2^n\left(\frac{1}{5} - \frac{O(\log n)}{n}\right)}$$

$$\leq 2^{2^n \cdot \frac{1}{5}}$$

total Boolean function $= 2^{2^n}$

$\Rightarrow$ $\exists$ a function $f : \{0,1\}^n \to \{0,1\}$ on n-variables that requires ckt of size $> \frac{2^n}{10n}$.

[Shannon's Thm. '49] (Counting Argument)

But the whole game is to come up with explicit functions that require large ckt $\boxtimes$

the lower bound that we saw $\frac{2^n}{10n}$

Obvious upper bound $\bigvee_{x \in f^{-1}(1)}$ [Indicator function for x]

$(x_1, x_2, x_3, x_4) = (1,1,0,1)$

$x_1 \wedge x_2 \wedge (\neg x_3) \wedge x_4$

$0010 = \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4$

Total size

$|f^{-1}(1)| \cdot n$

$\leq n \cdot 2^n$

But Lupanov (1950s) showed that every Boolean function on n variables has a ckt of size $\frac{2^n}{n}(1+o(1)) \leq 5 \cdot \frac{2^n}{n}$

And Lupanov also showed $\exists$ a $f: \{0,1\}^n \to \{0,1\}$ s.t. it requires ckt of size at least $\frac{2^n}{n}(1-o(1))$