Lecture 18

Thm. If $NP \subseteq P/poly$, then $PH = \Sigma_2^P$.

Proof: Show $\Pi_2^P \subseteq \Sigma_2^P$

$\rightarrow$ $\Pi_2 SAT \in \Sigma_2^P$

$\hookrightarrow$ Π_2^P-complete

$$\{ \varphi \mid \forall u \in \{0,1\}^n \ \exists v \in \{0,1\}^n \text{ s.t. } \varphi(u,v) = 1 \}$$

If $NP \subseteq P/poly$

$\Rightarrow$ $SAT \in P/poly$

$\Rightarrow$ $\forall$ boolean ϕ $\exists$ $\{C_n\}_{n \in N}$

s.t. $|\phi| = m$

$C_m(\phi) = 1 \Longleftrightarrow \phi$ is satisfiable.

$|C_n| = O(p(n)) \quad \forall n$, poly p.

- $\forall \psi$ on $2n$ variable

  $\forall u \in \{0,1\}^n$

  $\underbrace{\phi}_{n\text{-variables}} = \psi(u, \cdot)$

$\phi \in SAT \Longleftrightarrow \exists v$ s.t.

$\phi(v) = 1$

$\Longleftrightarrow \psi(u, v) = 1$

- Since $SAT \in P/poly$

$\phi \in SAT \leftrightarrow C_n(\phi) = 1$

$\leftrightarrow C_n(\varphi, u) = 1$

for any u.

- we have $\{C_n\}_{n \in \mathbb{N}}$ which decides if $\phi = \varphi(u, \cdot) \in SAT$

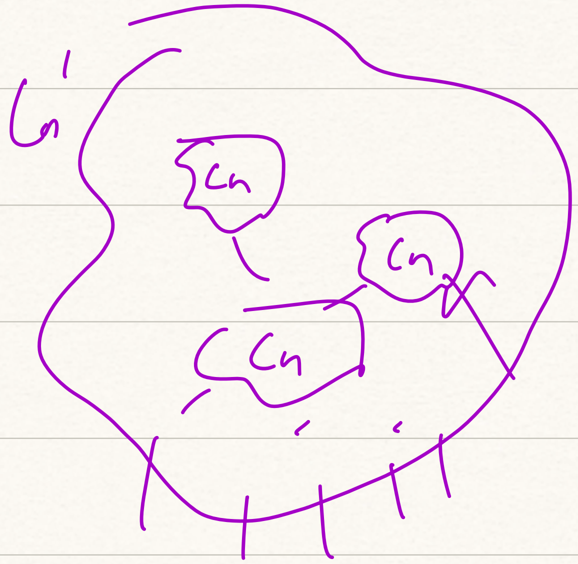
- We can use $\{C_n\}_{n \in \mathbb{N}}$ to make new circuit family $\{C_n'\}_{n \in \mathbb{N}}$ to find the SAT assignment

$C_n'(\varphi, u) = v \leftrightarrow$

P/poly , SAT

NP/P/poly

$\exists v$ s.t. $\varphi(u,v)=1$



$|C_n'| = O(q(n))$ for some polynomial $q \geq p$.

$\varphi \in \Pi_2\text{-SAT} \iff$

$$\forall u \in \{0,1\}^n \; \exists v \in \{0,1\}^n \; \varphi(u,v)=1$$

$$\iff \forall u \in \{0,1\}^n \; \exists v \in \{0,1\}^n \; C_n'(\varphi, u) = v$$

- P/poly only tells us

$\{C_n'\}$ exists, not how to construct it

- If $|C_n'| = q(n)$ then it has description size $O(q(n)^2)$
  - ↳ From adj. matrix view of C_n'

- $\exists w \in \{0,1\}^{q(n)^2} \; \forall u \in \{0,1\}^n$
  - $w = C_n'$ (it is the desc.); and
  - $\varphi(u, \underline{C_n'(\varphi, u)}) = 1$

$\Rightarrow \varphi \in \Sigma_2\text{-SAT}$

$\Rightarrow \Pi_2 SAT \in \Sigma_2^P$ $\#$

Theorem: $BPP \subseteq P/poly$.

Proof: $L \in BPP$. Then, $\exists$ DTM M in poly-time p s.t. $\forall n \in \mathbb{N}$ $\forall x \in \{0,1\}^n$

$$\Pr_{r \in \{0,1\}^m} [M(x,r) = L(x)] \geq 1 - \frac{1}{2^{n+1}}$$

$m = poly(n)$

$$\Pr_r [M(x,r) \neq L(x)] \leq \frac{1}{2^{n+1}}$$

For $x \in \{0,1\}^n$, we say $r \in \{0,1\}^m$ is <u>bad</u> for

x if $M_L(x,r) \neq L(x)$.

* otherwise r is good for x.

- Let $S_x = \{ r \mid r \text{ is bad for } x \}$

- $|S_x| \leq \dfrac{2^m}{2^{n+1}} \quad \forall x$

union bound

- $\left| \bigcup_{x \in \{0,1\}^n} S_x \right| \leq \sum_{x \in \{0,1\}^n} |S_x|$

set of all r that are bad for all x.

$\leq 2^n \cdot \dfrac{2^m}{2^{n+1}} = 2^m/2$

- $\Rightarrow \exists\, r^* \in \{0,1\}^m$ s.t.

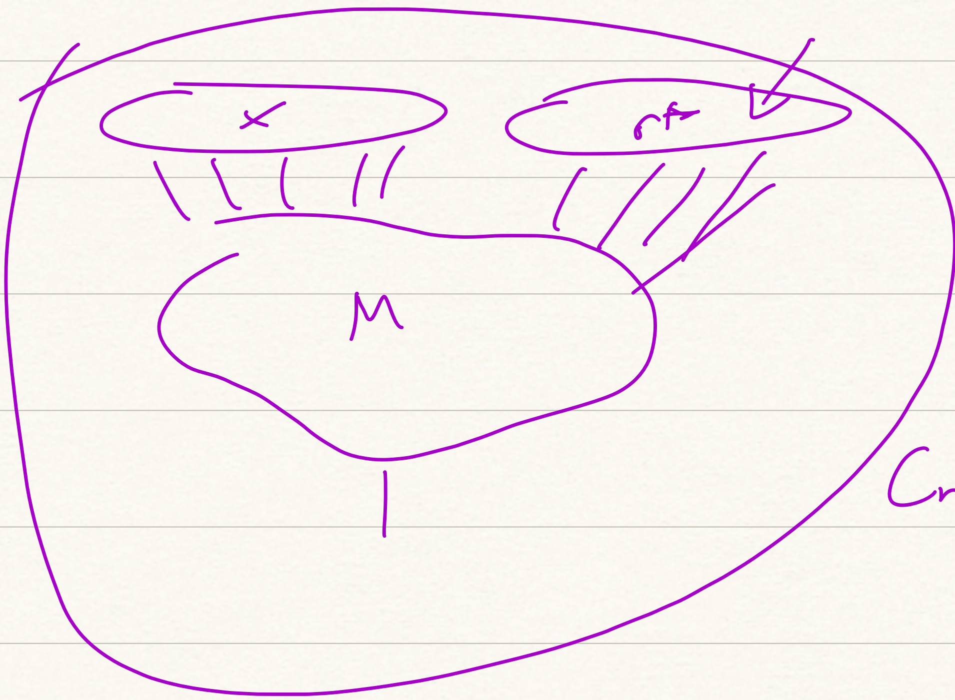
$\forall x \in \{0,1\}^n \quad M(x, r^*) = L(x)$.

M runs in time $p(n)$

$\Rightarrow$ can implement w/ circuit

C_n of size $|C_n| \le O(p(n)^2 + m)$

C_n has r^* hardcoded in it



C_n

$\Rightarrow C_n(x) = M(x, r) = L(x)$

$\forall x$

$\Rightarrow L \in P/poly$ $\square$

* Circuit lower Bounds

- If $NP \not\subseteq P/poly$, then $P \neq NP$ since $P \subseteq P/poly$
- Best lower bound for NP: any $L \in NP$ is decidable by a circuit family of size $\geq (5 - o(1))\, n$.

- Thm: (Shannon 49) $\forall n \in \mathbb{Z}^+$, $\exists\, f : \{0,1\}^n \to \{0,1\}$ that is not computable by any circuit of size $\leq 2^n/(10n)$.

Proof.

① # $f : \{0,1\}^n \to \{0,1\}$ is 2^{2^n}

② If C has size S, we can represent C with $\leq 9 \cdot S \log(S)$ bits.

$\Rightarrow$ # of circuits of size S $\leq 2^{9 S \log(S)} < 2^{S^2}$

- Set $S = 2^n/(10n)$

$$2^{(2^n/10n)^2} < 2^{2^n}$$ $\square$

- Can be improved to
  - $(1-\varepsilon)2^n/n \quad \forall \varepsilon > 0$
  - $2^n\left(1 + \frac{\log(n)}{n} - O\left(\frac{1}{n}\right)\right)$

Non-Uniform Time Hierarchy

Thm: $\forall\, T, T' : \mathbb{N} \to \mathbb{N}$ s.t.

$n < 10T(n) < T'(n) < 2^n/n$,

we have

$$SIZE(T) \subsetneq SIZE(T').$$

Proof: Let $f : \{0,1\}^\ell \to \{0,1\}$ be a function not computable by any C s.t. $|C| \le 2^\ell/10\ell$

$2n+n$

* Know: any $g: \{0,1\}^{n} \to \{0,1\}$
can be implemented by
circuit C of size $n \cdot 2^n$

- Set $\ell = \underline{(1.1)\log(n)}$
- $g: \{0,1\}^n \to \{0,1\}$

$g(x) = f(x_1, \ldots, x_\ell)$

$g \in \text{SIZE}(2^\ell \cdot 10\ell) \subseteq \text{SIZE}(n^2)$

$g \notin \text{SIZE}(2^\ell / 10\ell) \subseteq \text{SIZE}(n)$ □

Parallel Complexity

Def: $\forall i \in \mathbb{N}$, NC^i is all languages

L decidable by a circuit

family $\{C_n\}_{n \in \mathbb{N}}$ s.t.

1. $|C_n| \leq poly(n)$
2. $depth(C_n) \leq O(\log^i(n))$.

- $NC = \bigcup_{i \in \mathbb{N}} NC^i$

* NC^0 is special

↪ const. depth

⇒ output can only depend

on a const. # of inputs

⇒ uniform circuit class

- Uniform NC ::= NC w/ logspace uniform circuit families.

- <u>Def</u>: AC^i is identical to NC^i, except nodes have unbounded (polynomial) fan-in

$$AC = \bigcup_{i \in \mathbb{N}} AC^i$$

* $\forall i \quad NC^i \subsetneq AC^i \subseteq NC^{i+1}$

  * Unknown if this is <u>strict</u>

* DO know:

$$NC^0 \subsetneq AC^0$$

Thm: A language L has an efficient parallel algorithm iff $L \in NC$

Major open Question

$$P = NC ?$$

(we think $P \neq NC$)

* We can't even separate NC^1 from PH.

- Motivates P-completeness
  - L is P-complete if
    - $L \in P$
    - $L' \leq_L L \quad \forall L' \in P$

Thm: If L is P-complete:

1. $L \in NC \iff P = NC$
2. $L \in \mathbf{L} \iff P = \mathbf{L}$

   ← logspace

P complete lang:

$CIR\text{-}EVAL := \{(C, x) : C(x) = 1\}$

↓ circuit

PH via Exp-size Circuits

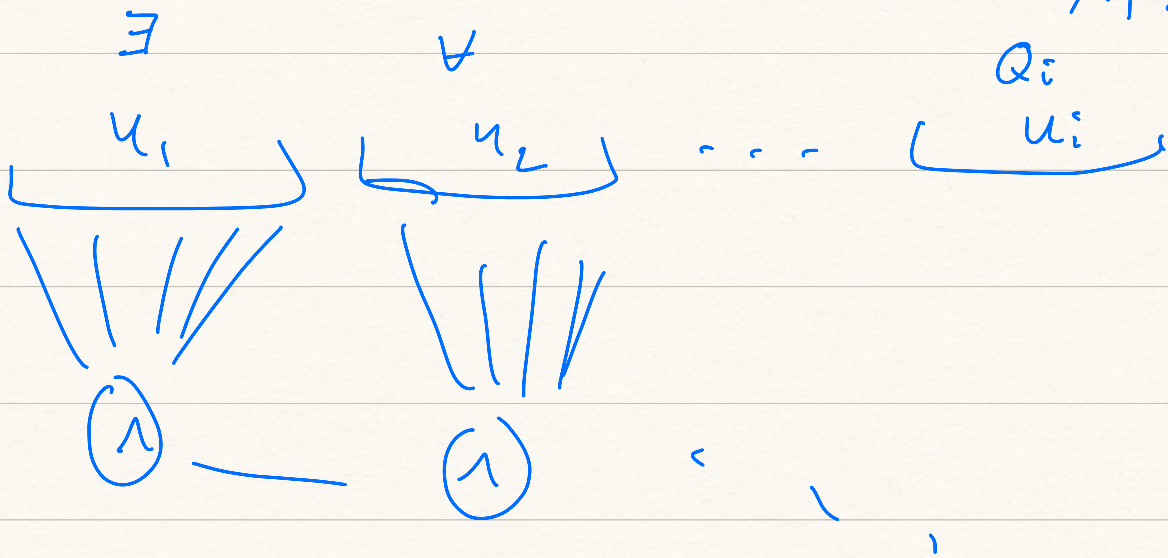
- **Def:** $\{C_n\}_n$ is DC-uniform if $\exists$ poly-time TM M s.t. $M(n,i)$ outputs i^{th} bit of $\langle C_n \rangle_2$.

- **Thm:** $L \in PH \iff L$ is decidable by DC-uniform $\{C_n\}$ w/ properties
  1. C_n has only AND, OR, NOT;
  2. $|C_n| \le 2^{n^{O(1)}}$, $\mathrm{depth}(C_n) = O(1)$
  3. C_n has unbounded (exp) fan-in

fan-in;

(4) every NOT is only @ input level —

if not const, then $L \in EXP$.



Lecture 19