Last time: • Ladner's thm: $P \neq NP \Rightarrow \begin{cases} SAT_H \notin P, \\ SAT_H \text{ not } NPC. \end{cases}$

NEW UNIT: ORACLES + POLY HIERARCHY

• $NP = \Sigma_1^P$, $coNP = \Pi_1^P$

Readings: Ca: 2.3–2.6
Pap. 17.2

Today: • Σ_k^P, Π_k^P, poly-time hierarchy (PH)
• Collapse thm
• Oracles, oracle reductions, $\Sigma_2^P = NP^{SAT}$
• circuit basics Pap. 4.3, 11.4; AB Chap. 6; Ca: 4.1, 4.2

Questions?

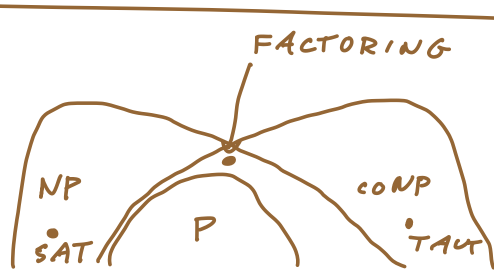
Recall $L \in NP = \Sigma_1^P$:

$w \in L \iff \exists^P y\, [\underbrace{D}_{\text{det poly time}}(w,y) = 1].$

$L \in coNP = \Pi_1^P$:

$w \in L \iff \forall^P y\, [\underbrace{D}_{\text{det poly time}}(w,y) = 1].$

Recall our belief:



If $NP \neq coNP$, then $P \neq NP$

Gen./ext. of NP $(= \Sigma_1^P)$, coNP $(= \Pi_1^P)$:
add on another layer of quant.

$\left(\begin{array}{ll} N: & \exists x \exists y \equiv \exists (x,y) \\ Y: & \exists x \forall y \ldots \end{array} \right)$

Def: Σ_2^P: $L \in \Sigma_2^P$ if there's a polytime det $O(\cdot,\cdot,\cdot)$ & a poly $p(n)$ s.t.

$$w \in L \iff \exists^p y\ \forall^p z\ [O(w,y,z)=1].$$

Π_2^P: $L \in \Pi_2^P$ if there's a polytime det $O(\cdot,\cdot,\cdot)$ & a poly $p(n)$ s.t.

$$w \in L \iff \forall^p y\ \exists^p z\ [O(w,y,z)=1].$$

Ex: MEF = Min Equiv. Formula

MEF $= \{\phi : \phi$ a Bool. formula s.t. no shorter Bool. form. ψ has $\phi \equiv \psi$ $(\forall x,\ \phi(x)=\psi(x))\}$.

$\overline{MEF} = \{\phi : \phi$ a Bool. formula s.t. there is a shorter Bool. form. ψ s.t. $\phi \equiv \psi$ $(\forall x,\ \phi(x)=\psi(x))\}$

$\phi \in \overline{MEF}$: means $\exists \psi\ \forall x\ \{\underbrace{\psi(x)=\phi(x)\ \&\ |\psi| \le |\phi|}_{\text{given } \phi, \psi, x, \text{ easy to check.}}\}$

So $\overline{MEF} \in \Sigma_2^P$.

Claim: $\underbrace{L \in \Sigma_2^P}$ $\iff$ $\overline{L} \in \Pi_2^P$.

Pf: $x \in L$: $\exists^p y\ \forall^p z\ [O(x,y,z)=1]$

$x \notin L$: $\neg \exists^p y\ \forall^p z\ [O(x,y,z)=1]$, i.e.

$$\forall^p y\ \exists^p z\ [O'(x,y,z)=1]$$

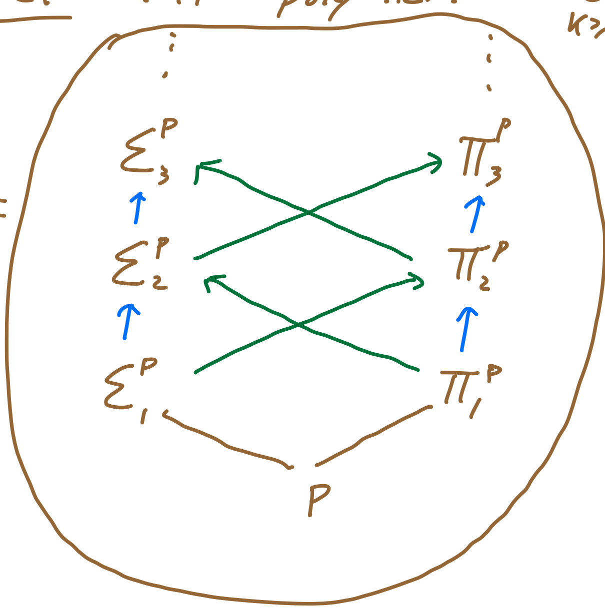
(D' just outputs neg. of D's output). ∎

Σ_k^P: sim., but now k alt. quant. starting w/ $\exists \ldots$.

Π_k^P: sim., but now k alt. quant. starting w/ $\forall \ldots$.

Def: PH = poly hier. = $\bigcup_{k \geq 1} (\Sigma_k^P \cup \Pi_k^P)$.

PH =



Easy obs:

$\Pi_k^P \subseteq \Pi_{k+1}^P$

EO1: $\Sigma_k^P \subseteq \Sigma_{k+1}^P$

(ignore last quant.)

Also

$\Sigma_k^P \subseteq \Pi_{k+1}^P$ (ignore 1st quant)

$\Pi_k^P \subseteq \Sigma_{k+1}^P$

EO2: $\Sigma_k^P = \Pi_k^P \iff \Sigma_k^P \subseteq \Pi_k^P$

$\Longrightarrow$: obvious.

$\Longleftarrow$: sps $\Sigma_k^P \subseteq \Pi_k^P$.

Let $L \in \Pi_k^P$. $\quad \overline{L} \in \Sigma_k^P \subseteq \Pi_k$, so

$L = \bar{\bar{L}} \in \Sigma_k^P$. So $\Pi_k^P \subseteq \Sigma_k^P$ & they're $=$.

We believe $\Pi_k^P \neq \Sigma_k^P$ $\forall k$. Some evidence:

"Collapse thm": If $\Pi_k^P = \Sigma_k^P$, then "PH collapses to level k":

$$PH = \Sigma_k^P = \Pi_k^P.$$

Pf: Special case (easy gen.):
Sps $\Sigma_1^P = \Pi_1^P$, we'll argue that
By E02, get $\Sigma_2^P = \Pi_2^P$, so

$$\Sigma_2^P \subseteq \Sigma_1^P \subseteq \Sigma_2^P$$

E02 $\subseteq \Pi_2^P$

$$\Sigma_1^P \overset{E01}{\subseteq} \Sigma_2^P = \Pi_2^P \subseteq \Sigma_1^P \subseteq \Sigma_2^P \quad \text{so } \Sigma_2^P = \Sigma_1^P.$$

To show: $\Sigma_1^P = \Pi_1^P \Longrightarrow \Sigma_2^P \subseteq \Sigma_1^P$.

Let $L \in \Sigma_2^P$: $\quad x \in L \iff \exists^P y \, \forall^P z \, [O(x,y,z)=1]$

Let $A := \{(x,y) : |y| = p(|x|), \ \forall^P z \, [O(x,y,z)=1]\}$.

$A \in \Pi_1^P$, so by , $A \in \Sigma_1^P$:

$$(x,y) \in A \iff \exists^q w \, [O'(x,y,w)=1].$$

So

$$x \in L \iff \exists^P y \ (x,y) \in A$$

$$\iff \exists^P y \, \exists^P w \, [O'(x,y,w)=1],$$

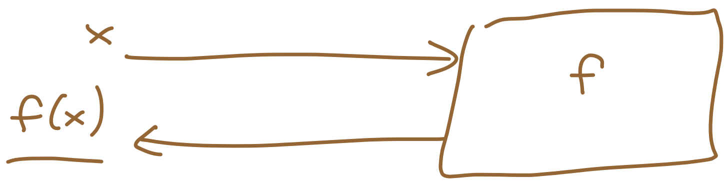
$$\underbrace{\qquad\qquad\qquad}\equiv \exists^{2p}(y,w)\left[D'(x,(y,w))=1\right]$$

so $L \in \Sigma_1^P$.

ORACLES (+ oracle TMs)

↳ (we'll see conn. of ↓ + PH soon...)

An <u>oracle</u> for $\boxed{\text{fn } f:}$ "magic black box" returning $f(x)$, on input x, in one time step.



TM: "query tape" for oracle; write x on it; enter query; machine goes to state $\to q_y$ if $f(x)=1$, $\searrow q_N$ if $f(x)=0$

$f: \to \{0,1\}$

oracles for f corr. to dec. problems

The TM does need to take time to write x, read f(x).

Write "M^f" to indicate TM M has oracle access to f.

<u>Def</u>: We say lang B "oracle reduces"

Cook reduces

Turing reduces

to lang A if there's a det poly time oracle TM M s.t. M^A decides B.

written "$B \leq_T^P A$" ; "$B \in P^A$".

<u>Def</u> P^{SAT} = all lang. dec. by some poly-time oracle TM that gets a SAT oracle.

Observe

- $P \subseteq P^{SAT}$
- $NP \subseteq P^{SAT}$ (SAT is NPC; one oracle call at end.)
- $coNP \subseteq P^{SAT}$ ($L \in coNP$ means $\overline{L} \in NP$: use prev + flip output.)

Here's a lang seemingly is not in NP,
" " coNP,
but is in P^{SAT}:

LC
LARGEST-CLIQUE = { (G, K): K = size of largest clique in G }.

$///^{SAT}$

Use 2 oracle calls to CLIQUE oracle:
(G, k) then (G, k+1)
Y N $\Longrightarrow$ (G, k) ∈ LC.

<u>DEF</u> NP^{SAT} : $L \in NP^{SAT}$ if some poly-time oracle NTM decides L, given a SAT oracle.

<u>Thm:</u> $NP^{SAT} = \Sigma_2^P$. (sim. pf: $\Pi_2^P = coNP^{SAT}$.)

<u>Pf</u>: • $\Sigma_2^P \subseteq NP^{SAT}$:

Fix some $L \in \Sigma_2^P$. $x \in L \Leftrightarrow \exists^P y \, \forall^P z \, [O(x,y,z)=1]$

Let $A = \{(x,y) : \forall^P z \, [O(x,y,z)=1]\}$.

$A \in coNP$, so $\overline{A} \le_p SAT$.
So poly-time alg can, given (x,y), compute $\phi_{x,y}$

s.t. $(x,y) \notin A \Leftrightarrow \phi_{x,y} \in SAT$.

So $\boxed{x \in L} \Leftrightarrow \exists^P y \, [(x,y) \in A]$

$\Leftrightarrow \boxed{\exists^P y \, [\phi_{x,y} \notin SAT]}$

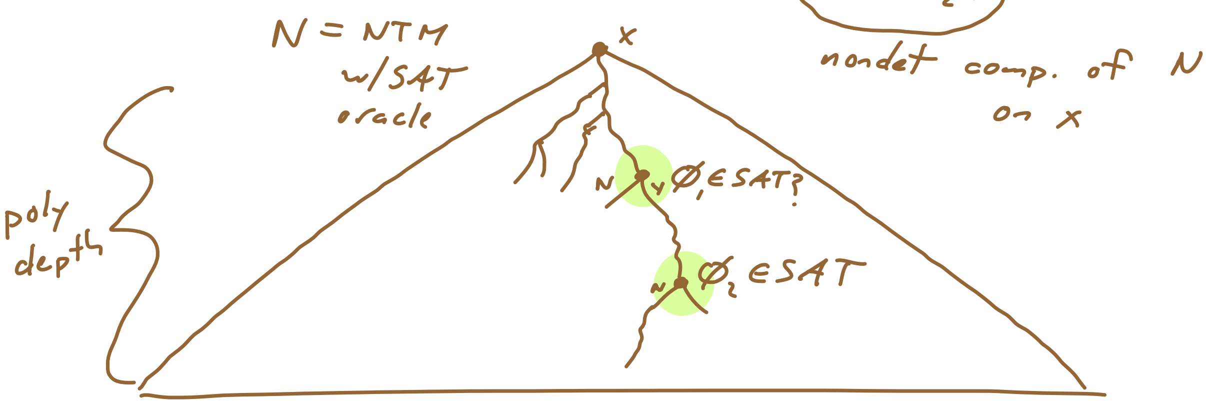
So a NTM $\overset{N}{\text{with}}$ a SAT oracle can det. $x \overset{?}{\in} L$ by: on input x, N nondet. guesses y, computes $\phi_{x,y}$, calls SAT on $\phi_{x,y}$, acc. iff SAT oracle says "no, $\phi_{x,y}$ not in SAT". $\blacksquare$

($\Sigma_2^P \subseteq NP^{SAT}$).

- $NP^{SAT} \subseteq \Sigma_2^P$:

$\underline{\exists\forall}$

Fix $L \in NP^{SAT}$. To show: $L \in \Sigma_2^P$.



Next time: · such an L is in Σ_2^P.
· ckts, nonunif. cxity.
