Last time:
- more on NP
- co-classes, e.g. coNP
- Reductions, completeness, favorite NPC problems
- PS1 out

Readings: Sipser 7.4, 7.5
AB 2.2–2.4, Pap. 8, 9

NPC, Cook-Levin,

Today:
- **Ladner's Thm:** $P \neq NP \Rightarrow \exists$ "NP-intermediate" languages

Reading: AB Chap. 3.3

- Start Unit 2: Oracles + the Polynomial Hierarchy

Reading: Ca: 2.3–2.6, Pap. 17.2

Questions?

Some NPC decision problems:
- CIRCUIT-SAT
- 3CNF-SAT
- CLIQUE
- INDEPENDENT-SET
- SUBSET SUM
- HAMILTONIAN PATH
- COLORABILITY
- ⋮

Nat. to wonder:

is **every** $L \in NP$ NPC?

NO (assuming $P \neq NP$) (Ladner)

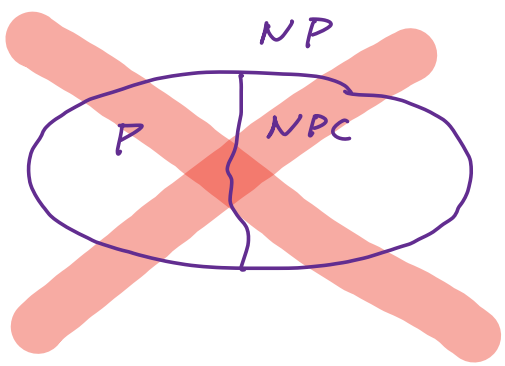
If P=NP: every lang $L \in NP$ (except $L = \{\}$, $L \in \Sigma^*$) is NPC.

→ b/c any $L' \in NP$ is in P, ← P

so can red. L' to L just by solving $x \in L'$?
∀ always mapping to same fixed y inst.
dep. on whether $x \in L$.

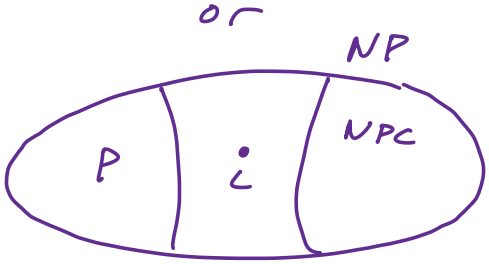
If $P \neq NP$:

Ladner's Thm: If $P \neq NP$, then $\exists\ L \in NP$ st
- $L \notin P$ ∀
- L is not NPC.



Either

or



Idea of orig. pf: double diag.
over
- poly-time TM's, ∀ over
- poly-time reductions.

Resulting L obt. from doing this correctly: not in P, not NPC

Tricky...

2nd pf (we'll do, Impagliazzo):

assuming $L \in NP \setminus P$, pf constructs "easier" "watered-down" version L' of L. (padding)

- L' is strictly easier than L, hence not a "hardest" lang in NP, hence not NPC;
- but L' still hard enough to be outside P.

Diag.-inspired careful choice of padding fn.

Setup:

- Get to assume throut that $P \neq NP$, hence $SAT \notin P$.

- Recall TM's can be enum: let M_i be i^{th} TM in enumeration

1st impt def: Given any $H: \mathbb{N} \to \mathbb{N}$, define SAT_H to be lang. of all length-n sat. Bool formulas padded w/ $n^{H(n)}$ many dummy chars:

$$SAT_H := \bigcup_{n \geq 1} \{ \psi 01^{n^{H(n)}} : \psi \in SAT, |\psi| = n \}$$

length is $n + 1 + n^{H(n)} \approx n^{H(n)}$

→ this is a watered-down ver. of SAT.

Consider $\langle \psi 01^{2^{|\psi|} - \psi - 1} \rangle$: if $|\psi| = \ell$,

$\to = 2^k = n$, so poly(n) time is $2^{O(k)}$ time.

2nd impt def: the specific H of the pf:

$H: \mathbb{N} \to \mathbb{N}$,

$H(n)$ = the smallest $i < \log\log n$ s.t. for every $x \in \{0,1\}^*$ with $|x| \le \log n$, M_i outputs $SAT_H(x)$ within $i|x|^i$ steps.

If there's no such i then $H(n) = \log\log n$.

$SAT_H(x) = 1$ if $x \in SAT_H$, $= 0$ if $x \notin SAT_H$.

---

2 prelim. claims for pf:

Claim 1: H is well defined & $H(n)$ can be computed in poly(n) time given n. HW.

Claim 2: $SAT_H \in P$ iff $H(n) = O(1)$.

$\exists C$ st $\forall n$ $H(n) \le C$.

In fact, if $SAT_H \notin P$ then $\lim_{n\to\infty} H(n) = \infty$.

Pf: $\Rightarrow$: Sps $SAT_H \in P$. Then $\exists$ TM M solving SAT_H in cn^c time for some fixed c. This M shows up as M_i in our enum. of TMs for some $i > c$. But then for $n > 2^{2^i}$, have $H(n) \le i$. So $H(n) = O(1)$. ∎

$\Leftarrow$ Sps $\lim_{n\to\infty} H(n) \neq \infty$. Means $\exists C$ st

$H(n) \le C$ for poly many n's. (Follows from $H(n) = O(1)$).
So $\exists\, i^*$ s.t. $H(n) = i^*$ for poly many n's. (!)

Sps M_{i^*} fails to output right answer for $SAT_H(x')$ for some x' in time $i^*|x'|^{i^*}$.
Then $\forall n > 2^{|x'|}$, $H(n)$ must $\neq i^*$. But this contrad.

So M_{i^*} does output right answer on every x in $i^*|x|^{i^*}$ time = poly time. So $SAT_H \in P$.

Now proof of thm: $SAT_H \notin P$, SAT_H not NPC.

$SAT_H \notin P$: we argue that if $SAT_H \in P$ then $P = NP$.

So, sps $SAT_H \in P$. By 2nd claim, $H(n) \le C$, so SAT_H is SAT padded w/ n^C many 1's: hence a poly-time alg for $SAT_H \Rightarrow$ poly-time alg for SAT, so $P = NP$.

SAT_H not NPC: we argue that if SAT_H is NPC, then $P = NP$.
If SAT_H were NPC, then $\exists$ red. f from SAT to SAT_H running in $O(n^K)$ time for some fixed K.
By (2), since $SAT_H \notin P$, $H(n) \to \infty$ (length-n inputs).
f runs in $O(n^K)$ time: maps input ϕ to SAT to input $\psi 01^{n^{H(n)}}$ to SAT_H, where length $\le O(n^K)$. But $O(n^K) << n^{H(n)}$ for large n, since

$$T(n) = (\text{time for reduc.}) + T(n^{1/3})$$

In partic., $T(n) = n^5 + T(n-1)$

$$O(n^k) << (n^{1/3})^{H(n^{1/3})}.$$

But this means ϕ (length-n) $\in$ SAT iff

(length $\leq n^{1/3}$) $\psi \in$ SAT.

This gives a poly-time recursive alg for SAT.
So P=NP. ∎

This lang is ... highly unnatural!

There are nat. problems believed to be neither NPC nor in P:

- FACTORING — quasipolytime: $n^{\text{poly}(\log n)}$
- GRAPH ISOMORPHISM

END of basics...

Oracles + poly-time Hierarchy

Recall $L \in NP$ iff $\exists$ poly $p(n)$, det TM D, (poly-time)

s.t.

$$w \in L \iff \exists y \in \{0,1\}^{p(n)} \left[D(w,y) = 1 \right].$$

Notation: "$\exists^{p(n)} y$" "$\exists\, y \in \{0,1\}^{p(n)}$"

→ NP also called Σ_1^P.

coNP also called Π_1^P.

Recall $L \in$ coNP if there's a poly $p(\cdot)$, a poly-time det D s.t.

$$w \in L \iff \nexists^{p(n)} y \left[D(w,y) = 1 \right]$$

i.e. $w \in L \iff \forall^{p(n)} y \left[D'(w,y) = 1 \right]$.

↓ D' outputs opp. of D.

More coming...