Last time:

- Σ_k^p, Π_k^p, poly-time hierarchy (PH)
- Collapse thm: if $\Pi_2^p = \Sigma_2^p$, then $PH = \Sigma_2^p$
- Oracles, oracle reductions, start $\Sigma_2^p = NP^{SAT}$ ($\subseteq$)

Readings: Ca: 2.3–2.6, Pap. 17.2

Today:

- $NP^{SAT} \subseteq \Sigma_2^p$
- Circuits, P/poly, nonuniformity

  Reading: Pap. 4.3, 11.4, AB 6.4, Ca: 4.1, 4.2
- Karp-Lipton thm: $NP \subseteq P/poly \Rightarrow$ PH collapses to Σ_2^p.

  Reading: AB 6.4, Ca: 4.2, Papad. 17.13

Questions?

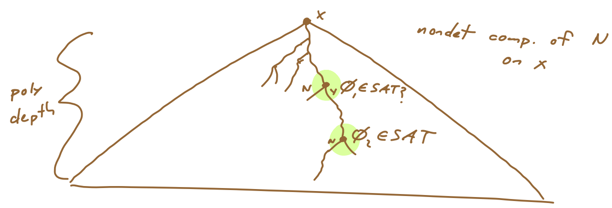
To show: $L \in \Sigma_2^p$.

Reminder: PS1 due Wed

Proving $NP^{SAT} \subseteq \Sigma_2^p$:

Fix $L \in NP^{SAT}$, so L decided by N = NTM w/ SAT oracle.

Each comput. path of N may ask poly(n) many queries to SAT oracle.



Proof idea:

① We construct equiv. NTM N' that asks ≤ 1 SAT query on each path (at end of path). (decides same lang. L as N^{SAT})

For each path P, N' constructs formula ϕ_P, asks "$\phi_P \in SAT$?"; accepts if $\phi_P \notin SAT$, rejects if $\phi_P \in SAT$.

② With this N', easy to argue $L \in \Sigma_2^p$.

(1) Here's how N' works:

Sim. N until N's 1st query to SAT: "$\phi_1 \in SAT$?"

N' doesn't ask oracle; instead, guesses Y/N.

- On Y: further guesses sat. asst. to ϕ_1; checks it;

— if asst. indeed sat. ϕ_1, continues N's comput. along q_{yes} path

— if asst doesn't sat. ϕ_1, halt & reject.

- On N: continue N's comput. in q_{no} (& "remembers" that guessed "$\phi_1 \notin SAT$"; adds ϕ_1 to set C of form. to be checked later.)

Subseq. comput. of N handled same way.

When N halts: if it rej., so does N'.

if it acc: N' must confirm that every form. $\phi_i \in C$ is indeed not in SAT.

Does this by querying SAT once, on

$$\phi_p = \bigvee_{\phi \in C} \phi$$ ← diff vars for each $\phi \in C$

N' acc iff $\phi_p \notin SAT$. Did (1).

(2): Given N', argue $L \in \Sigma_2^P$.

$x \in L$ iff some path P (of N on x w/ SAT oracle) acc.

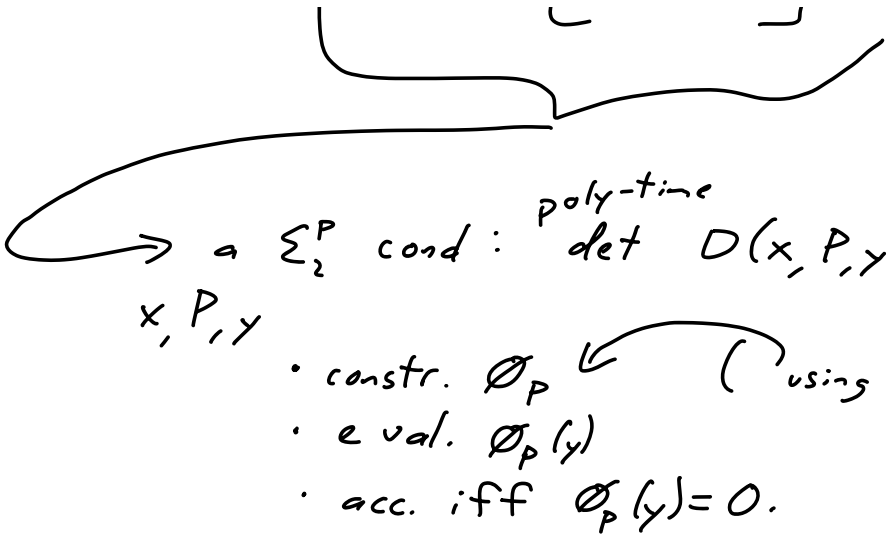
iff some P (of N' on x w/ SAT oracle) accepts.

I.e.

$x \in L \Leftrightarrow \exists^P P$ s.t. path P of N' acc. x.

$\Leftrightarrow \exists^P P \ \phi_p \notin SAT$ (1)

$\Leftrightarrow \exists^P P \ \forall^P_y [\phi_p(y) = 0.]$



→ a Σ_2^P cond: poly-time det $D(x, P, y)$ given x, P, y

- constr. $\varnothing_P$ (using x)
- eval. $\varnothing_P(y)$
- acc. iff $\varnothing_P(y) = 0$.

So, $NP^{SAT} = \Sigma_2^P$.

Generalizes...

→ NP equipped w/ some NP-oracle

$$\Sigma_2^P = NP^{SAT} = NP^{NP}$$

More precisely: given $\mathcal{C}$ a cxity class, define

$$NP^{\mathcal{C}} = \bigcup_{A \in \mathcal{C}} NP^{A}$$

$NP^{(NP^{NP})} = NP^{\Sigma_2^P} = \Sigma_3^P$. Etc...

Going (a little) beyond P...?

Nonuniform poly-time; poly-size ckts.

TM: "uniform" model: same alg (TM) for all input sizes.
? Too restrictive ?"

Nonuniform comput: allow diff. algs for diff. input lengths.

First nonunif. model:

Can augment std TM model to make it nonunif. by giving our TM's "advice".

For each n (input length), have unique "advice string" α_n for the TM.

On input x, TM gets $(x, \alpha_{|x|})$. ($\alpha_{|x|}$: program for TM to run on x.)

Model / alg:

$(M; \alpha_1, \alpha_2, \ldots, \alpha_n, \ldots)$

Note:
If TM M runs in poly(n) time, then w/log $|\alpha_n| \leq$ poly(n).

More precisely:

Def $P/poly$:

$L \in P/poly$ if $\exists\ L' \in P$ and seq. $\alpha_1, \ldots, \alpha_n, \ldots$ $|\alpha_n| \leq poly(n)$, s.t.

$\forall\ x \in \Sigma^n$, have $x \in L$

$\Updownarrow$

$(x, \alpha_{|x|}) \in L'$.

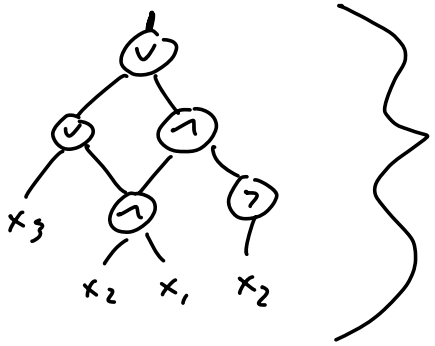
Can sharpen to $P/\ell(n)$ for arb. fn $\ell(n)$

$|\alpha_n| \leq \ell(n)$.

$$P/poly = \bigcup_{c>0} P/n^c.$$

Second nonunif. model: Bool. circuits (ckt)

See Ca: p. 52, other books:

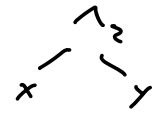


any fixed ckt has partic. # inputs;

diff ckts for diff. values of n: nonuniform!

Basis for circuit: finite set of allowed gates.

$\{\wedge_2, \vee_2, \neg\}$: one basis



$\{NAND\}$: $x \; NAND \; y = \neg(x \wedge y)$

another basis

→ universal

etc.

A basis is universal if ckts over the basis can compute any Bool. fn.

Fact: Every $f: \{0,1\}^n \to \{0,1\}$ is comp. by a Bool ckt over $\{\wedge_2, \vee_2, \neg\}$.

(use a $\vee$ of $\wedge$ ONF or $\wedge$ of $\vee$ CNF rep.)

$\{\wedge_2, \oplus_2\}$ universal. $\quad x \oplus_2 y$: x XOR y

- $\{\oplus_2\}$ not univ.
- $\{\wedge_2, \vee_2\}$ not univ. (are univ. for monotone $f: \{0,1\}^n \to \{0,1\}$)

f is mon. if $x \leq y \Rightarrow f(x) \leq f(y)$ (coordinatewise)

$x = 1101001$ $\quad x \leq y$

$y = 1111001$

Fix a univ. basis (say, $\wedge/\vee/\neg$).

Def: Let $f: \{0,1\}^n \to \{0,1\}$.
The ckt cxity of f is the # of gates in smallest Bool ckt computing f.

- depends on choice of basis, but only by const. factor.
- can count input vars $x_1, \ldots, x_n$ as gates

Def: A fn $f: \{0,1\}^* \to \{0,1\}$ has ckt cxity $s(n)$ if $\forall n$, f on $\{0,1\}^n$ is computed by a ckt of size $\leq s(n)$.

Def: Lang $L \subseteq \{0,1\}^*$ has $s(n)$-size ckts $C_1, C_2, \ldots$ if there is a family $(C_n)_{n \geq 1}$ of ckts s.t.

- $|C_n| \leq s(n)$
- $\forall n$, $\forall x$ $|x| = n$, $x \in L \Leftrightarrow C_n(x) = 1$.

Ex: $L = \{x \in \{0,1\}^* : \#\text{ of } 1\text{s in } x \text{ is odd}\}$.

$\leq$ PAR

$11010\underline{1}\underline{0}\underline{1}\underline{0} \notin L$ $\qquad$ $1101010101010 \in L$

$$PAR(x) = \sum_i x_i \bmod 2$$

Exercise: PAR has $O(n)$-size ckts. (induction).

Thm: $L \in P/poly$ iff L has poly(n)-size ckts.

- **Poly time TMs w/ advice can sim. poly-size ckts:**

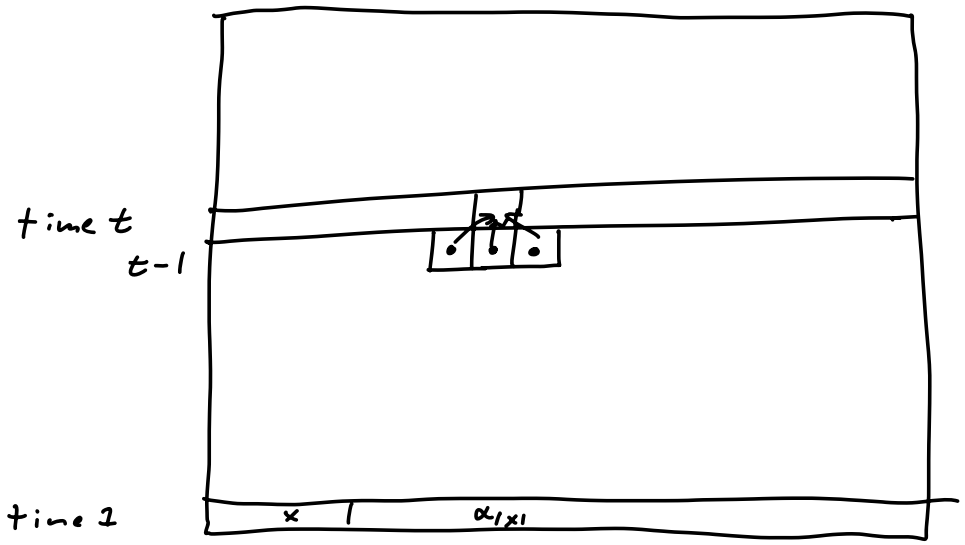
$C_1, C_2, \ldots, C_n, \ldots$

Have the advice string α_n encode C_n;
on input $|x|=n$, TM eval.'s C_n on x. Poly time.

- **Poly-size ckts can sim. poly-time TM w/ advice:**

Just like Cook-Levin: unroll $t(n)$-time comput. into a $t(n) \times t(n)$ tableau, & have ckt verify (everywhere in tableau) "local consistency according to M".

$M, x, \alpha_{|x|}$:



Next time: Karp-Lipton

∀ Baker-Gill-Solovay
