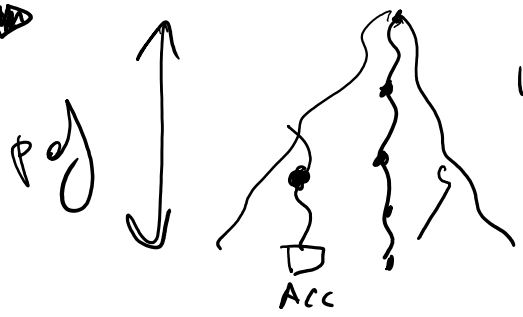
CC-Lecture-8-4-2020

8 April, 2020 10:25

- $\forall k \quad \exists L \in NP^{NP}$ s.t. $L \notin SIZE(n^k + k)$
- Bounded depth circuits – AC^0



nondet. computation poly-time with SAT as an oracle

NP^{SAT}

- $\forall k \quad \exists L \in EXP$ s.t. $L \notin SIZE(n^k + k)$

$\ldots \in PSPACE \ldots$

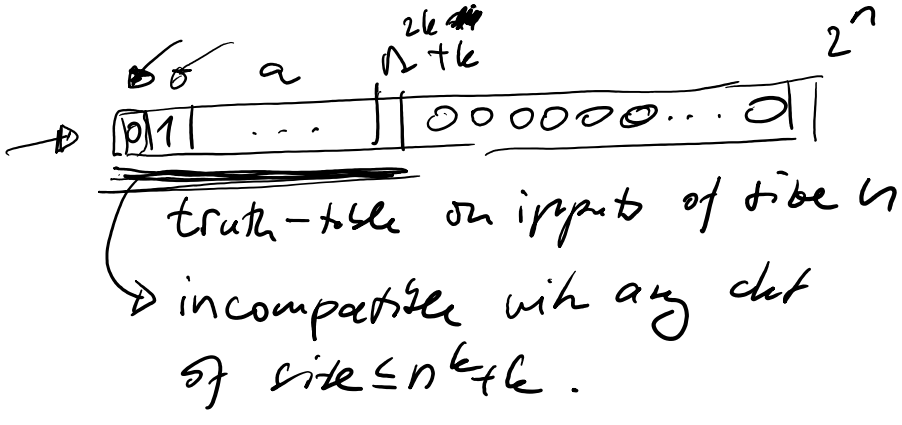
$NP^{NP} \subseteq PSPACE$

Want: $\forall k \quad \exists L \in NP$ s.t. $L \notin SIZE(n^k + k)$ ⇐

$\forall k \quad \exists L \in P$ s.t. $L \notin SIZE(n^k + k)$ ⇐

Thm: (Karp–Lipton): $\forall k \; \exists L \in NP^{NP}$ s.t. $L \notin SIZE(n^k + k)$

x input of size n



truth-table on inputs of size n

→ incompatible with any ckt of size $\leq n^k + k$.

of size $= n^k + k$.

$C_1, C_2, \ldots$ $\quad C_0 = \{$ all circuits of size $\leq n^k + k \}$

$$|C_0| \leq 2^{n^{2k}+k}$$

$$S = \{ a 0 1^n 0 1^m ; \; a \in \{0,1\}^* \text{ is a prefix of a truth-table of a fcn } f : \{0,1\}^n \to \{0,1\} \text{ s.t. } \sout{a \text{ is incompatible with all circuits of size } m} \; f \text{ is computable by some circuit of size } m \}$$

$S \in NP$: input $w = a 0 1^n 0 1^m$

guess a circuit of size $\leq m$ on n input bits & check if its truth table corresponds to a. — ACCEPT iff it is consistent w/ a

nondet. alg. in time $\simeq O(w^3)$.

$L \in NP^{NP}$ $\qquad$ oracle to be S $\qquad NP^S$

alg for L : on input x $\qquad n = |x|$

→ guess a of size $n^{2k}+k$

check $a 0 1^n 0 1^{n^k+k} \in S$ $\boxed{\to S'}$

if no then answer a_x

or $\circ$ if
$x > |a|$.

• nondet. pol. time with oracle S .

$x \xrightarrow{\text{guess } a} a_x = 1 \quad a 01^n 01^m \notin S \rightarrow$ ACCEPT x.

$x' \xrightarrow{\text{guess } a'} a'_{x'} = 1 \quad a' 01^n 01^m \notin S \rightarrow$ ACCEPT x'.

the first $n^{2k}+k$ x's would all be accepted & all the other REJECTED.

→ algorithm computes a fcn. that has small circuits!

$S' = \{ a 01^n 01^m :$ either $a 01^n 01^m \in S$ or
or $\exists a' \in \{0,1\}^{|a|}, a' <_{lex} a$
s.t. $a' 01^n 01^m \notin S \}$

	a		a'						
lex	000...0	00...01	00...010	.....					
S	1	1	0	1	1	0	0	1	0
S'	1	1	0	1	1	1	1	1	1

$S' \in NP$?

$S' \in NP^{(NP)}$ $\quad NP^S$

→ check input $w \in S$ $\quad w = a 01^n$
if not guess $a' <_{lex} a$
if $a' 01^n 01^m \notin S$ then ACCEPT w
otherwise REJECT.

$\forall k \quad \exists L \in NP^{NP^{NP}}$ s.t. $L \notin SIZE(n^k + k)$

$\cap PSPACE$

want: $\forall k \quad \exists L \in NP^{NP}$ s.t. . . . .

Pf: two possibilities

1) $NP \not\subseteq PSIZE = \bigcup_k SIZE(n^k + k)$

$\Rightarrow \forall k \; \exists L \in NP$ s.t. $L \notin SIZE(n^k + k)$

$\subseteq NP^{NP}$ ✓

2) $NP \subseteq PSIZE$

for some k, $SAT \in SIZE(n^k + k)$

$\Rightarrow NP^{NP^{NP}} \subseteq NP^{NP}$

$\Rightarrow \forall k \exists L \in NP^{NP^{NP}} \subseteq NP^{NP}$ s.t. $L \in SIZE(n^k + k)$

$\exists L \in NP^{NP}$ s.t. $L \in SIZE(n^k + k)$

"collapse of polynomial hierarchy"

PH ... polynomial hierarchy

$$PH = \bigcup_\ell \underbrace{NP^{NP^{\cdots^{NP}}}}_{\ell} = \bigcup_\ell \Sigma_\ell^P$$

Σ_ℓ^P

$NP \subseteq PH$

$coNP \subseteq PH$

$P^{NP} \subseteq PH$ ...

$PH \subseteq PSPACE$

$\forall \ell \quad \Sigma_\ell^P \subseteq PSPACE$ (EXC)

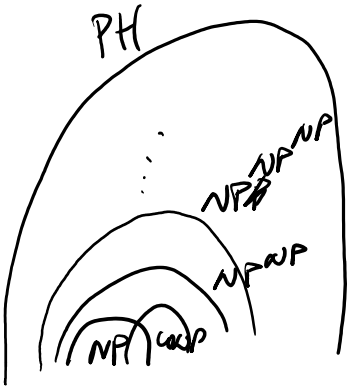
$\forall \ell \quad \Sigma_\ell^P \subseteq PSPACE$ (EXC)

- "If NP has poly-size circuits then polynomial hierarchy collapses to the second level"

$\Rightarrow \quad NP^{NP^{NP}} \subseteq NP^{NP^{NP}} \subseteq NP^{NP} \subseteq NP^{NP}$

$NP^{\cdots^{NP}} \subseteq NP^{NP}$

$\forall \ell \quad \Sigma_\ell \subseteq NP^{NP}$



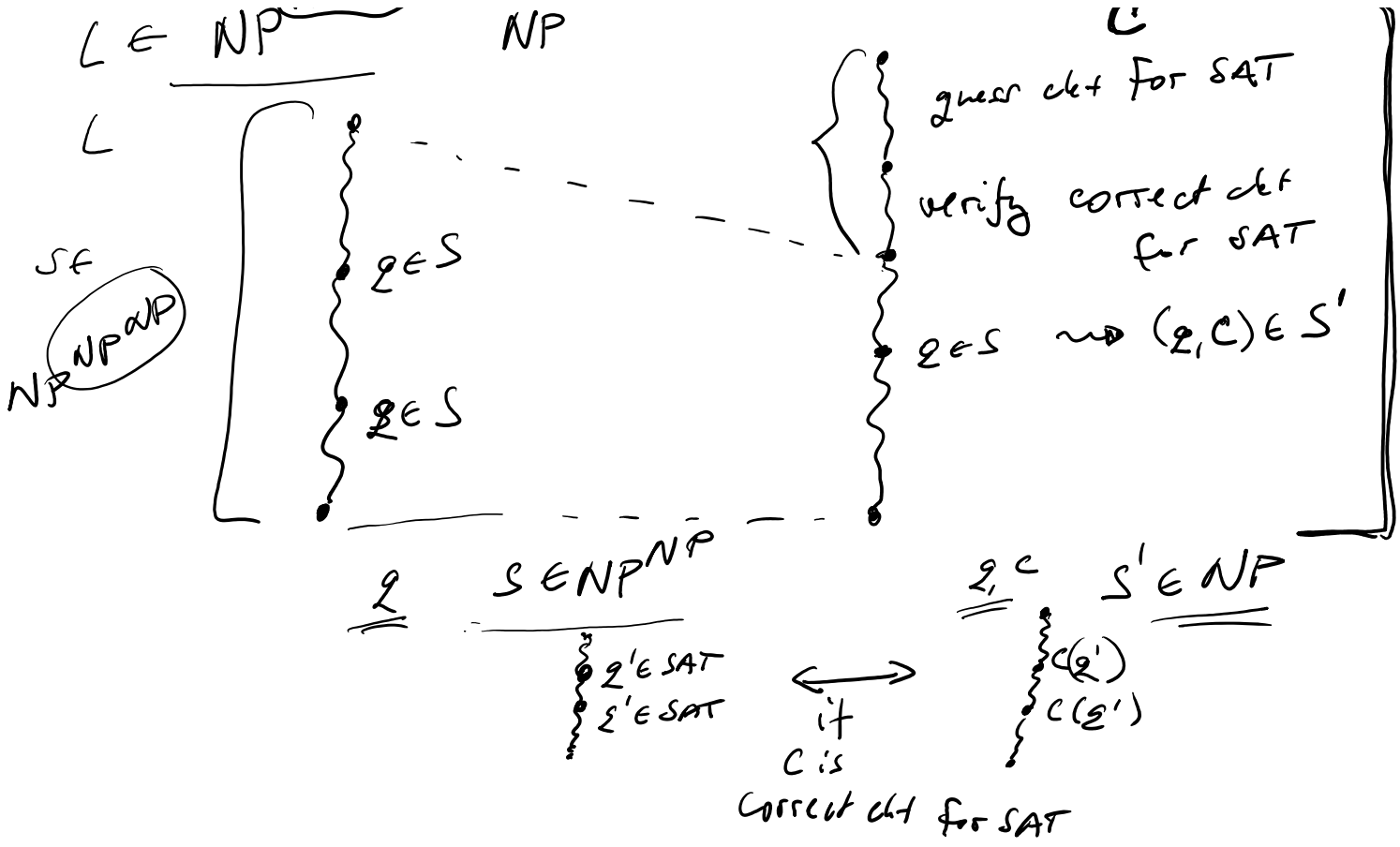
- $NP \subseteq PSIZE \Rightarrow PH \subseteq NP^{NP}$
- $NP \subseteq PSIZE \Rightarrow NP^{NP^{NP}} \subseteq NP^{NP}$

Open problem? Belief: $NP \not\subseteq PSIZE$

- If NP has poly-size ckt's $SAT \in P^k + k$ we can guess them & using NP oracle we can verify that they are correct.

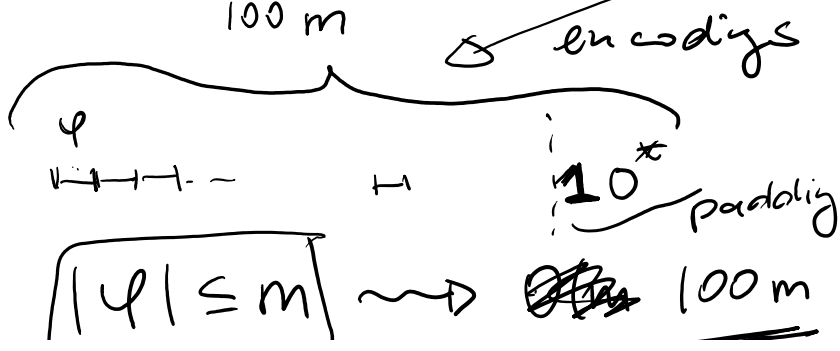
$L \in NP^{NP^{NP}}$ $\quad NP^{S' \in \overline{NP}}$ $\quad NP^{S', SAT}$

C ("guess ckt for SAT")



- to verify that a ckt C is a correct ckt for SAT can be done using oracle queries for SAT.

C of size $n^k + k$ need to check that it correctly answers φ $\quad C(\varphi) = 1 \iff \varphi \in SAT$.



$|\varphi| \le m$ $\rightsquigarrow$ 100m bits

$m = n^{O(1)}$ $\quad n'$

C of $n'^k + k$

$\varphi(x_1, \dots x_n) \in SAT \iff \varphi(x_1, \dots, x_{n-1}, 0) \in SAT$ or $\varphi(x_1, \dots, x_{n-1}, 1) \in SAT$

For ckt C: $\forall \varphi$ of size at most m

check

(*) $C(\varphi(x_1 \dots x_n)) = 1$ iff $C(\varphi(x_1 \dots x_{n-1}, 0)) = 1$ or $C(\varphi(x_1 \dots x_{n-1}, 1)) = 1$

C check ∃ coNP type condition

(**) $C(\varphi(0, \dots 1)) = 1$ iff $\varphi(0, \dots 1)$ is true

a single NP-query can check both conditions at once.

$L_{\neg SAT} = \{ C \mid C$ is ckt doesn't compute SAT $\} \in NP$

∎