- This contradiction refutes the existence of M.

$\Rightarrow$ Ntime$(f) \subsetneq$ Ntime(g). $\square$

- We continue with more diagonalization proofs.

- Are all the problems in $NP \setminus P$, NP-complete?

<u>Ladner's theorem</u>: If $P \neq NP$ then $\exists L \in NP \setminus P$ that is not NP-complete.

<u>Proof</u>:

- <u>Idea</u>: Pad SAT & use diagonalization.

- Say, $P \neq NP$. Then SAT $\notin P$. For some fn. $H(\cdot)$ consider the padding:

$SAT_H := \{ \varphi 0 1^{n^{H(n)}} \mid \varphi \in SAT \ \& \ |\varphi| = n \}$.

▷ $H(n) \to \infty \Rightarrow SAT_H$ is not NP-Complete.

Pf:-

If $SAT \leq_p SAT_H$ & $H(n) \to \infty$, then a CNF ψ of size n reduces to an instance $\varphi 0 1^{|\varphi|^{H(|\varphi|)}}$ of size n^c (constant c).

$\Rightarrow |\varphi| + |\varphi|^{H(|\varphi|)} = O(n^c)$.

$\Rightarrow |\varphi| = o(n)$.

Thus, ψ of size n reduces to a φ of size $o(n)$.

On repeating this again & again, we get a CNF τ of size $O(1)$.

$\Rightarrow SAT \in P$, which is a contradiction.

$\square$

- To deduce $SAT_H \notin P$ we define H in a way so that it grows <u>very</u> slowly:

  $H(n)$ is the smallest $i < \lg\lg n$ s.t. $\forall x \in \{0,1\}^{\leq \lg n}$, M_i accepts x in time $\leq i \cdot |x|^i$ iff $x \in SAT_H$, a recursive defn.

Or, if there is no such i then $H(n) := \lg\lg n$.

• How easy is it to compute $H(n)$?

By "brute-force" it requires

$$\underset{\uparrow}{\lg\lg n} \times \underset{\uparrow}{2^{\lg n}} \times (\lg \underset{\uparrow}{n})^{\lg\lg n} \times \underset{\uparrow}{2^{\lg n}} = o(n^3).$$

\# i's   \# x's   \# M_i steps   solving SAT on $\lg n$ size

▷ $SAT_H \notin P$.

Pf: Suppose a TM M solves SAT_H in time $\leq c \cdot n^c$. Pick a $j > c$ s.t. $M = M_j$.

⇒ M_j decides SAT_H in $< n^j$ time, implying $H(n) \leq j$, $\forall n > 2^{2^j}$.

⇒ SAT_H is just SAT padded with n^j 1's.

⇒ $SAT \in P$. A contradiction. □

▷ $H(n) \to \infty$.

Pf: Since $SAT_H \notin P$, $\forall i \exists x$ st. M_i cannot decide $x \in^? SAT_H$ in time $i \cdot |x|^i$.

⇒ $H(n) \neq i$, $\forall n > 2^{|x|}$.

⇒ $H(n)$ takes a value i only for

finitely many n. $\square$

- Thus, we have a poly-time fn. H s.t. $SAT_H \in NP \setminus P$ & SAT_H is not NP-C. $\square$

– We have seen such clever diagonalization tricks. Could they show $P \neq NP$?

<u>Oracles</u> (& Relativizing proofs)

<u>Defn</u>: We call a TM M an <u>oracle TM using a language O</u> if M has
- three special states q_{query}, q_{yes}, q_{no}
- a special oracle-tape,

such that when M enters q_{query} with a string y on the oracle-tape, in the next step it is in q_{yes} (resp. q_{no}) if $y \in O$ (resp. $y \notin O$).

Defn: • $P^O := \{L \mid L$ has a poly-time oracle TM using $O\}$.

• $NP^O := \{L \mid L$ has a poly-time oracle NDTM using $O\}$.

Proposition: (1) $\bar{O} \in P^O$.

(2) If $O \in P$ then $P^O = P$.

(3) Let $Expcom := \{(M, x, 1^n) \mid$ TM M accepts x in $\leq 2^n$ steps$\}$. Then,

$$P^{Expcom} = EXP = NP^{Expcom}.$$

Proof:

(1) Negate the answer of O.

(2) Ignore the oracle-tape; instead use the poly-time TM.

(3) Show the easy consequences,

$$EXP \subseteq P^{Expcom} \subseteq NP^{Expcom} \subseteq EXP^{Expcom} \subseteq EXP. \quad \square$$

Defn: A proof about complexity classes, $C_1 = C_2$ (resp. $C_1 \neq C_2$), is said to be *relativizing* if $\forall O$, $C_1^O = C_2^O$ (resp. $C_1^O \neq C_2^O$) also follows.

▷ Diagonalization proofs till now are relativizing.

Pf: Properties (1) & (2) before. □

$P \stackrel{?}{=} NP$ requires a non-relativizing proof

Theorem (Baker, Gill, Solovay, 1975): $\exists$ languages A & B s.t. $P^A = NP^A$ & $P^B \neq NP^B$.

Proof: • We have already seen $A := $ Expcom.

• Now we design B via diagonalization!

• For any B, the related unary language $U_B := \{1^n \mid \exists x \in B, |x| = n\} \in NP^B$.