Diagonalisation

- Uncountability of reals (Cantor)
- Undecidability of HALT (Turing)
- Incompleteness theorem (Gödel)

↳ only known method to prove limitations of TMs !

TMs \ inputs	$\langle M_1 \rangle$	$\langle M_2 \rangle$	$\langle M_3 \rangle$	$\langle M_4 \rangle$
M_1	$\cancel{1}$ 0	0	0	1 . . . .
M_2	0	$\cancel{1}$ 0	0	0
M_3	1	0	$\cancel{0}$ 1	1
M_4	0	1	0	$\cancel{1}$ 0
⋮				

$$D = \{ \langle M \rangle : M(\langle M \rangle) = 0 \}$$

Suppose for contradiction M_i decides D

$$M_i(\langle M_i \rangle) = 1 \iff \langle M_i \rangle \in D$$

$$\iff M_i(\langle M_i \rangle) = 0 \quad ↯$$

Time Hierarchy theorem

$$\underset{f(n)}{\mathrm{TIME}(n)} \subsetneq \underset{g(n)}{\mathrm{TIME}(n^3)}, \quad f(n)\log(f(n)) = o(g(n))$$

Universal TM:

There is TM U s.t.

$$U(\langle M, x\rangle) = M(x)$$

in $\underbrace{c_M}_{\text{constant}} \cdot \underbrace{t_M^2(n)}_{\text{runtime of } M}$ steps

Proof:

$$D = \{\langle M, 1^k\rangle : U(M, \langle M, 1^k\rangle) = 0 \text{ in } k^3 \text{ steps}\}$$

- $D \in TIME(n^3)$
- $D \notin TIME(n)$

Sup. M decides D in time $t(n) = \overset{\text{constant}}{c} \cdot n$

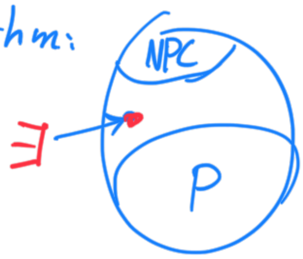
$$M(\langle M, 1^k\rangle) = 1 \iff \overbrace{\langle M, 1^k\rangle}^{n = |\cdot|} \in D$$

$$\iff U(M, \langle M, 1^k\rangle) = 0 \text{ in } \underbrace{k^3}_{> c_M \cdot c^2 \cdot (|M|+k)^2} \text{ steps}$$

$$\overset{\text{large } k}{\iff} M(\langle M, 1^k\rangle) = 0$$

More in textbook: Hierarchy for NTIME

Ladner's thm:



Oracle TMs

Let $A \subseteq \{0,1\}^*$ be arbitrary (even undecidable)

Oracle TM, denoted M^A, has a new instruction: in single step, can answer queries of the form

$$\text{“} x \overset{?}{\in} A \text{”}$$

(Think of black-box subroutine for A)

Complexity classes relative to oracles

$P^A = \{L : L$ decided by poly-time OTM $M^A\}$

$NP^A = \{$ ——— " ——— ND-OTM $\}$

Ex.

- $P^{\emptyset} = P$
- $P^A = P$ for $A \in P$
- $P^{SAT} \supseteq NP \cup coNP$

(P^{NP})

- $A \leq_p B \Rightarrow A \in P^B$ $\left[\Leftrightarrow A \leq_p^T B \right.$ "poly-time Turing red" "Cook red." $\left.\right]$

<u>Thm</u> [BGS'75]

The "P vs NP" question relativises both ways!

$\exists A, B: \quad P^A = NP^A \quad$ but $\quad P^B \neq NP^B$

<u>Upshot:</u> "<u>Relativising</u>" proof techniques cannot resolve P vs NP.

Ex. diagonalisation relativises

<u>Universal OTM</u> $\exists U^\bullet$:

$\forall A: \quad U^A(\langle M^\bullet, x\rangle) = M^A(x)$

in $c_M \cdot t_M^2(n)$ steps

<u>Relativised time hier:</u> $TIME^A(n) \subsetneq TIME^A(n^3)$

<u>Lemma:</u> Let A be <u>complete</u> for EXP.

$= \bigcup_k TIME(2^{n^k})$

Homework 1

Then:

$EXP \subseteq P^A \subseteq NP^A \subseteq EXP$

$B \qquad B$

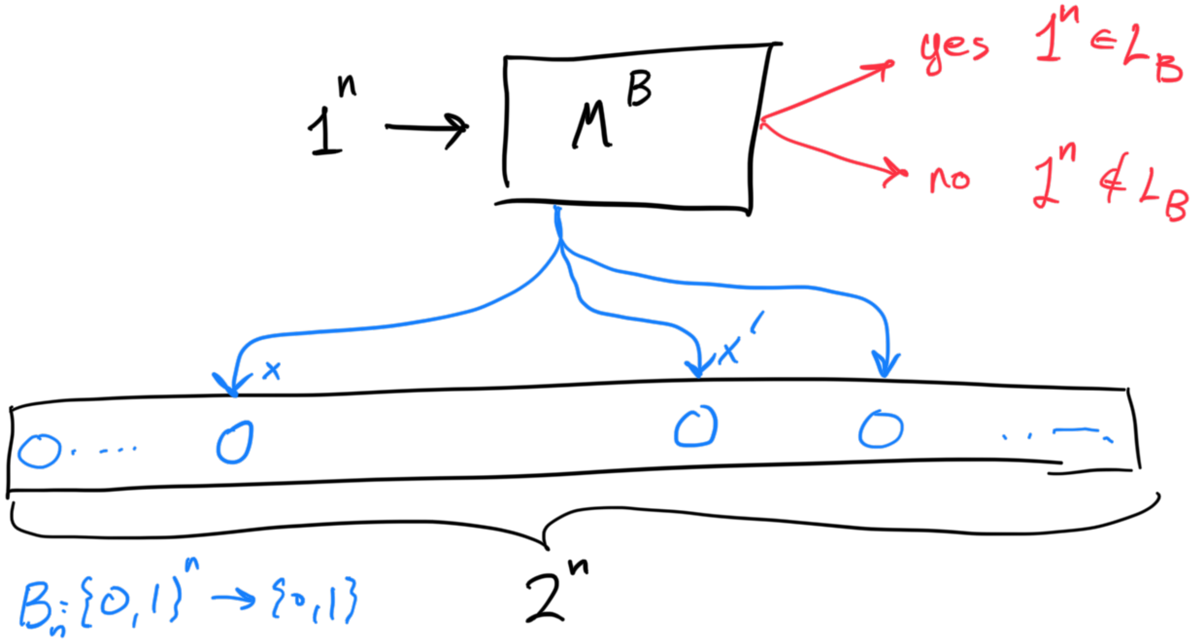
Lemma: $\exists B: \quad P^B \neq NP^B$

Proof $L_B = \{1^n : \exists x \in \{0,1\}^n : x \in B\}$

$\in NP^B$

Remains to show $L_B \notin P^B$

Fix polytime M^B, consider large n:



$B_n : \{0,1\}^n \to \{0,1\}$

Complete by iterating over all M^B:

$M_1^B, M_2^B, \dots, M_i^B$