CPSC 421/501 Dec 2, 2024

- How **not** to solve Fermat's last theorem.

- How **not** to solve P vs. NP

Thm: there are oracles, A, B s.t.

$P^A = NP^A$, $P^B \neq NP^B$,

and for A we can take any PSPACE-complete problem.

- How to solve P vs. NP

Thm: If $P = NP$, there are poly sized circuits for 3COLOUR, etc.

Logistics:

- There is a final exam study guide being built.

- Dec 4: Presentation CPSC 501 + questions on final exam practice
- Dec 6: All questions on final exam practice
- Dec 9: Last office hours
- Dec 10: Final exam

Theorem (Fermat's Last Theorem):

Let $n \in \mathbb{N}$, $n \geq 3$. Then

there are no positive

$x, y, z \in \mathbb{N}$ s.t.

$$x^n + y^n = z^n.$$

Rem: This is not true if

we allow $x, y, z \in \mathbb{R}$!

for any $x, y \in \mathbb{R}$, we can take

$$z = (x^n + y^n)^{1/n} \in \mathbb{R} \ldots$$

Rem: A proof that works

for both

$\_\_\_ \quad x, y, z \in \mathbb{N} \quad \_\_\_$

AND

$\_\_\_ \quad x, y, z \in \mathbb{R} \quad \_\_\_$

must have an error ...

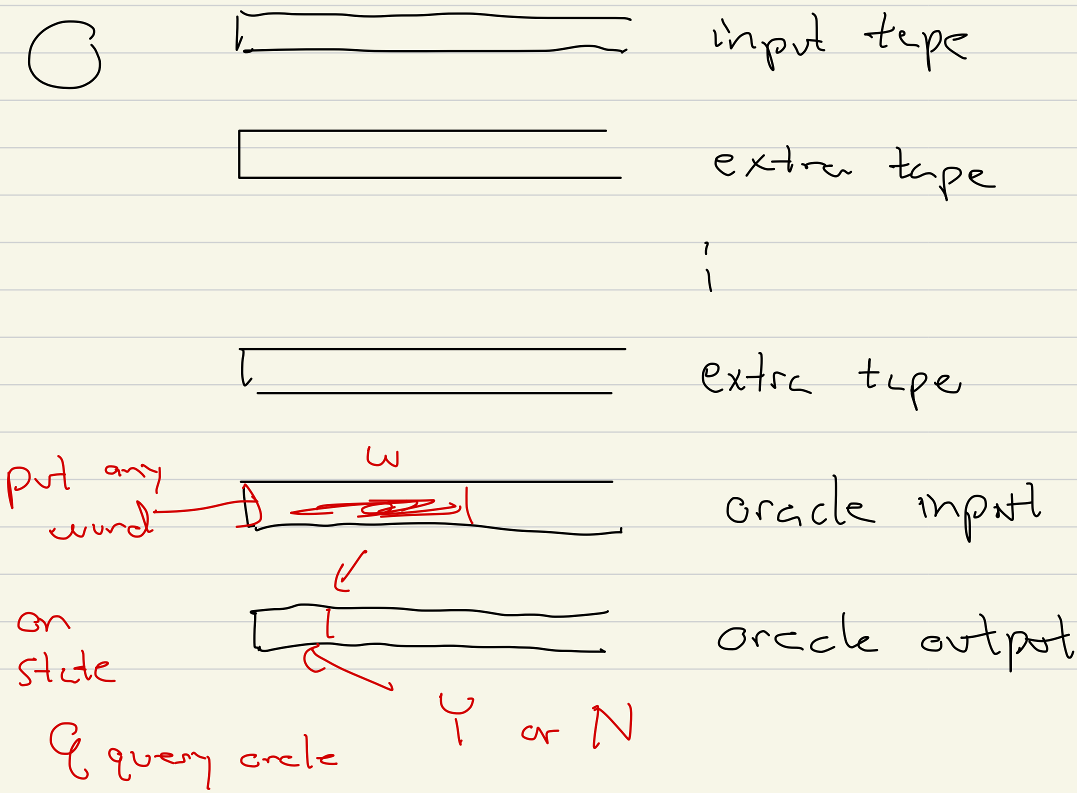
$x, y, z \in \mathbb{N} \Rightarrow$ statement is true

$\mathbb{R} \Rightarrow$ — — — false

Similarly for P vs. NP ...

Oracle Turing machines (Ch 3)

with oracle $A \subset \Sigma^*$:



TM^A = Turing machine with oracle A:

an additional q query oracle state

whatever on oracle input tape

$$\underbrace{|\,a\,|\,b\,|\,b\,|\,a\,|\,a\,|}_{w}\,\sqcup\,|\,\sqcup\,|$$

yes	no
$w \in A$	$w \notin A$

=

e.g. oracle A = Acceptance_{TM}

very very powerful

Theorem: Baker - Gill - Solovay

Ch 9: If A is any PSPACE-complete language (TQBF)

then

$$P^A = NP^A$$

(basically using Savitch's thm)

And there exists an oracle B

s.t.

$$P^B \neq NP^B \quad \longleftarrow ?$$

Rem: Diagonalization, simulation of certain types, all work with any oracle

You'd think, maybe ...

$$P^{3SAT} \stackrel{?}{=} NP^{3SAT}$$

certainly unclear

$$\underset{coNP \subset}{NP} \subset \underbrace{P^{3SAT}}_{\text{is very powerful}}$$

$$P^{2COLOUR} \stackrel{?}{=} NP^{2COLOUR}$$

$$P \stackrel{?}{=} NP$$

Rem: If $3SAT \in P$

$\Rightarrow P^{3SAT} = P$

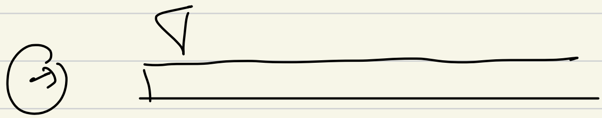
$P^{ACCEPTANCE_{TM}} \supsetneq P$

$\not\parallel$

$P^{Acceptance(TM^{Acc_{TM}})}$

$\vdots$

How to solve P vs NP ---

time 1 

$X_{1j\sigma}$ tape contents time 1

Y_{1j} tape head location time 1

Z_{1q} the state at time 1

Boolean 3CNF phrase

time 2: $X_{2j\sigma}$, Y_{2j} , Z_{2q}

Cook-Levin for 3SAT: NP-complete

Then

$$\{x_{1j\sigma}\}\ \{y_{1j}\}\ \{z_{1q}\}$$

$$\Big\Downarrow \text{ determine}$$

$$\{x_{2j\sigma}\},\ \{y_{2j}\},\ \{z_{2q}\}$$

$$\Downarrow$$

$$\vdots$$

$$3SAT \in TIME(n^k)$$

$\Rightarrow$ $3SAT_n$ has circuits size $O(n^{2k})$

$$w = \underbrace{\sigma_1 \sigma_2 \cdots \sigma_n}_{\text{input}}$$

X's

y's

Z's time 1

X's

y's

Z's time 2

⋮

time

Cn^k

Formula is a certain type of circuit ...

Today, Dec 2, 2024

no one knows how to identify a function (3SAT, 3COLOUR, something in NP) that requires formulas of size $\geq n^{3.00001}$ for an instance of input size n.

Subbotovskaya 1961 :

$XOR_n = x_1 \oplus \dots \oplus x_n$

requires $\geq C \cdot n^{1.5}$ size

formula with $\wedge, \vee, \neg$

⋮

1990's Håstad ...

=

P, NP, PSPACE, NL, L, ...

randomness : RP, BPP, ...

Class ends

$P^A \stackrel{def}{=} \{ L \mid$ L can be decided in poly time by a Turing m. with oracle A $\}$

PSPACE-complete: means L s.t.

(1) $L \in$ PSPACE,

(2) $L' \in$ PSPACE, $L' \leq_{\substack{poly\\time}} L$