8s Oracles

Thursday, April 14, 2022
11:55 AM

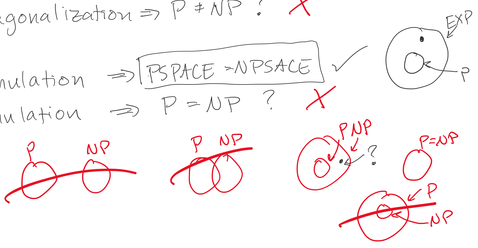
Big: Understand why P vs NP is so hard

Idea: Diagonalization ⇒ $P \neq EXP$ ✓ (also $P \subsetneq NP$)

Diagonalization ⇒ $P \neq NP$? ✗

Simulation ⇒ $PSPACE \neq NPSPACE$ ✓

Simulation ⇒ $P = NP$? ✗



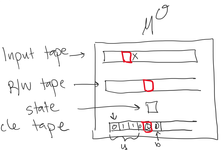
Goals

- Define and write proofs involving oracles
- Describe why oracles help us prove no proof exists

Questions

- Why is it important that PATH is NL-Complete? Hard to work with TMs.
- Why is f-function log-space
- Big-Picture Idea with Diagonalization
- EXP ≠P

def: A TM M with access to an oracle O is denoted M^O and looks like



O is a language. $O \subseteq \{0,1\}^*$

M^O can ask Oracle if $y \in O$? Questions = "queries"

$0110 \in O$

$b=1 \rightarrow 0110 \in O$

$b=0 \rightarrow 0110 \notin O$

$O = 3SAT$

$3SAT \in P^{3SAT}$

$NP \subseteq P^{3SAT}$ ⇐

def: Let $O \subseteq \{0,1\}^*$

- $L \in P^O$ if ∃ a polytime TM M^O that decides L.
- $L \in NP^O$ if ∃ a polytime TM M^O and a polynomial p s.t. $\forall x \in \{0,1\}^*$,

$x \in L$ iff $\exists u \in \{0,1\}^{p(|x|)} : M^O(x,u) = 1$

Group Problem Solving - One fun thing you want to do this summer

1. If $O \in P$ then $P^O \subseteq P$ ← $P \subseteq P^O$, $P^O \subseteq P$
2. $coNP \subseteq P^{3SAT}$

1. Let $O \in P$. Let $L \in P^O$. Then there exist a polynomial time TM M^O that decides L. There also also exist a polynomial time TM M_0 that decides O. Let M' be the TM that does the same as M^O except everytime M^O queres whether $y \in O$, M' runs $M_0(y)$ as a subroutine. The runtime of M' is ... polynomial. and M' decides L, so ⇒ $L \in P$

Facts $P \neq EXP$ using diagonalization. $\forall O$ $P^O \neq EXP^O$

1. $A \neq B \rightarrow \forall O, A^O \neq B^O$ F (Pset)
2. ✗ using diagonalization
3. $A = B \rightarrow \forall O, A^O = B^O$ F (using simulation)
4. $\exists O_1 : P^{O_1} \neq NP^{O_1}$ } Class
5. $\exists O_2 : P^{O_2} = NP^{O_2}$ }

T → T	= T
T → F	= F ✗
F → T	= T
F → F	= T

Using these facts, what can we say?

→ Diagonalization + simulation will not work to prove $P \neq NP$ or $P = NP$

Big Idea:

Interesting: Proving a proof approach fails

def: "relativizing" A proof relativizes if it holds in the presence on any oracle.
e.g. "Diagonalization is relativizing"

def: "non-relativizing" A proof is non-relativizing if it is inconsistent in the presence of oracles.
e.g. "P vs NP requires non-relativizing techniques."