

Problem 1

Recall that a search algorithm for a search problem R outputs, on input x , a string y such that $(x, y) \in R$ if such a y exists.

Consider the search problem R defined as follows:

$(\langle M \rangle, x, z, 1^t, y) \in R$ if $|y| \leq t$, z is a prefix of y , and M is a deterministic Turing Machine that accepts input (x, y) in at most t steps.

- (a) Show that if $L_R \in P$, then there is a polynomial-time search algorithm for R .
- (b) Show that if $P = NP$, then every NP-search problem has a polynomial-time search algorithm.¹

Problem 2

Let $s(n)$ be a function such that $s(n) = o(2^n/n)$.

- (a) Show that there exists a decision problem L and a string x such that $L \in \text{SIZE}(s(n))$, but $L \cup \{x\} \notin \text{SIZE}(s(n))$.
- (b) Using part (a), show that $\text{SIZE}(s(n)) \neq \text{SIZE}(s(n) + O(n))$.
- (c) Define $\text{DTIME}(t(n))$ as the class of problems decided by Turing Machines running in time $t(n)$. Why can't we use the same argument to "prove" that $\text{DTIME}(n^3) \neq \text{DTIME}(n^3 + O(n))$?

Problem 3

In this problem we prove circuit lower bounds for the polynomial hierarchy.

- (a) Show that $\Sigma_4 \not\subseteq \text{SIZE}(n^{10})$.
- (b) Show that $\Sigma_2 \not\subseteq \text{SIZE}(n^{10})$. (Use part (a).)

¹The same argument also shows that if $NP \subseteq P/\text{poly}$, then every NP-search problem can be solved by a circuit family of polynomial size.

Problem 4

In class we saw that EXP contains decision problems that are not in P.

- (a) Show the following stronger statement: There is a decision problem L in EXP such that for every $A \in P$ and every sufficiently large n

$$\Pr_{x \sim \{0,1\}^n} [A(x) \neq L(x)] > 1/2n.$$

Namely, L and A differ on at least $1/2n$ fraction of inputs on sufficiently large input lengths.

Hint: Let M_1, M_2, \dots be an enumeration of all Turing Machines. On input x , try to simulate $M_i(x)$ for $1 \leq i \leq |x|$.

- (b) **(Extra credit)** Can you show

$$\Pr_{x \sim \{0,1\}^n} [A(x) \neq L(x)] > 1/3?$$

How about

$$\Pr_{x \sim \{0,1\}^n} [A(x) \neq L(x)] > 1/2 - 2^{-\Omega(n)}?$$

- (c) Show that for every L there exists a decision problem $A \in P$ such that for infinitely many n ,

$$\Pr_{x \sim \{0,1\}^n} [A(x) = L(x)] \geq 1/2.$$