CS 535: Complexity Theory, Fall 2023

Homework 4

Due: 11:59PM, Tuesday, October 3, 2023.

Reminder. Homework must be typeset with LaTeX preferred. Make sure you understand the course collaboration and honesty policy before beginning this assignment. Collaboration is permitted, but you must write the solutions *by yourself without assistance*. You must also identify your collaborators. Assignments missing a collaboration statement will not be accepted. Getting solutions from outside sources such as the Web or students not enrolled in the class is strictly forbidden.

Problem 1 (Padding and Time Hierarchies)**.** Hint: Use part (a) to solve part (b).

(a) Show that if f, g, t are time-constructible, and $\mathbf{DTIME}(f(n)) = \mathbf{DTIME}(g(n))$, then $\mathbf{DTIME}(f(t(n))) = \mathbf{DTIME}(g(t(n)))$. (4 points)

(b) Show that $\mathbf{DTIME}(n) \neq \mathbf{DTIME}(n \log n)$. (4 points)

Problem 2 (**NP** vs. **PSPACE** relative to an oracle)**.** The Baker-Gill-Solovay Theorem (Theorem 3.7 in Arora-Barak) shows that there is an oracle A relative to which $\mathbf{P}^A \neq \mathbf{NP}^A$. This problem will walk you through a proof that there is also an oracle A relative to which $\mathbf{NP}^A \neq \mathbf{PSPACE}^A$. This proof will hopefully illuminate a general recipe for proving oracle separations.

(a) A DNF formula D is an OR of "terms," where each term is an AND of literals. The *width* of a DNF is the maximum number of literals appearing in any term and the *size* is the number of terms. For example, $(x_1 \wedge \overline{x_2}) \vee (x_2 \wedge x_3 \wedge x_4)$ is a DNF of width 3 and size 2.

Believe it or not, the whole proof rests on the following simple combinatorial fact[1]: The function $\mathrm{XOR}_N(x_1, \ldots, x_N) = x_1 \oplus \cdots \oplus x_N$ cannot be computed by a DNF $D(x_1, \ldots, x_N)$ of width $< N$. Prove this fact. (4 points)

(b) Another way to think of an oracle A is as an infinitely long vector, indexed by binary strings. That is, for $z \in \{0,1\}^*$, let $A_z = 1$ if $z \in A$ and $A_z = 0$ if $z \notin A$. Recall that to query A, a TM can write a string z to its oracle tape and receive the bit A_z.

For an oracle A, define the unary language

$$\begin{aligned} L_{\mathrm{XOR}}(A) &= \{1^n \mid \mathrm{XOR}_{2^n}((A_z)_{z \in \{0,1\}^n})\} \\ &= \{1^n \mid z \in A \text{ for an odd number of strings } z \in \{0,1\}^n\}. \end{aligned}$$

Show that $L_{\mathrm{XOR}}(A) \in \mathbf{PSPACE}^A$ for every oracle A. (4 points)

[1] Well, in the same way that Baker-Gill-Solovay rests on the fact that OR_N cannot be computed by a "decision tree" of depth $< N$.

(c) Now our job is construct an oracle A for which $L_{\text{XOR}}(A) \notin \mathbf{NP}^A$. We'll do this by first arguing that the output of an $\mathbf{NP}^A$ machine is just a DNF applied to the oracle A.

Let M be a nondeterministic oracle Turing machine running in time $T(n)$. Show that for every $n \in \mathbb{N}$ there exists a DNF formula D_n of width at most $T(n)$ and size at most $2^{O(T(n))}$ such that for every oracle A,

$$M^A(1^n) = 1 \iff D_n(A) = 1,$$

again regarding A as an infinite vector $(A_z)_{z \in \{0,1\}^*}$. (4 points)

Hint 1: When run on an input of length n, the machine M can query the oracle at most $T(n)$ times.

Hint 2: A binary tree of depth T has at most 2^T leaves.

Your job is done now, but stick around for the exciting conclusion! Next we diagonalize against all nondeterministic machines running in time $T(n) = 2^n/10$ to instantiate the oracle A. Let $M_1, M_2, \ldots$ be an enumeration of such machines, with each machine appearing infinitely often in the list. We construct an oracle A^* such that for every machine M_i in the enumeration, there exists an input 1^{n_i} such that $M_i^{A^*}(1^{n_i}) = 1 \iff 1^{n_i} \notin L_{\text{XOR}}(A^*)$.

We construct A^* iteratively as follows. We initialize A^* to be the empty language, and in each round i, commit to including or excluding strings of a certain length n_i in A^*. We choose n_i large enough so that no string of length n_i has had its fate decided in any previous round.

Let D_{n_i} be the DNF formula guaranteed by part (c) capturing the behavior of machine M_i on input 1^{n_i}. By part (a), there exists an oracle $A^{(i)}$ such that

$$D_{n_i}(A^{(i)}) \neq \text{XOR}_{2^{n_i}}((A_z^{(i)})_{z \in \{0,1\}^{n_i}}).$$

Actually, something stronger is true. Since $\text{XOR}_{2^{n_i}}(A)$ only depends on the values of A_z for $z \in \{0,1\}^{n_i}$, we may assume that $A_z^{(i)} = A_z^*$ for every $|z| < n_i$.

Now for all of the (finitely many) z for which the variable A_z appears in the DNF D_{n_i}, set $A_z^* = A_z^{(i)}$. That is, for each such z, commit to including z in A^* if $z \in A^{(i)}$ and commit to excluding z from A^* if $z \notin A^{(i)}$. Then by part (b),

$$M_i^{A^*}(1^{n_i}) = 1 \iff D_{n_i}(A^*) = 1 \iff \text{XOR}_{2^{n_i}}((A_z^*)_{z \in \{0,1\}^{n_i}}) = 0 \iff 1^{n_i} \notin L_{\text{XOR}}(A^*).$$

Let M be any nondeterministic TM running in time $T_M(n) = \text{poly}(n)$. Let n_* be sufficiently large so that $T_M(n^*) \leq 2^{n^*}/10$. Since M appears infinitely often in our enumeration, there exists some $n \geq n_*$ such that $M^{A^*}(1^n) = 1 \iff 1^n \notin L_{\text{XOR}}(A^*)$. Hence, $L_{\text{XOR}}(A^*)$ is not decided by any poly-time NTM, so $L_{\text{XOR}}(A^*) \notin \mathbf{NP}^{A^*}$.

On the other hand, we showed in part (b) that $L_{\text{XOR}}(A) \in \mathbf{PSPACE}^A$ for every oracle A, and in particular for A^*. Hence $\mathbf{NP}^{A^*} \neq \mathbf{PSPACE}^{A*}$.

Problem 3 (*Bonus Problem*, **NP** vs. **PSPACE** relative to a random oracle)**.** Are oracles that separate **NP** from **PSPACE** rare, or are they common? In this problem, you'll show that $\mathbf{NP}^A \neq \mathbf{PSPACE}^A$ not only for some contrived oracle A, but for *almost all* oracles.

(a) Show that for sufficiently large N, for every DNF D of width at most $\sqrt{N}$,

$$\Pr_{x \sim \{0,1\}^N}[D(x) \neq \mathrm{XOR}_N(x)] \geq 0.1.$$

(b) Let $A \subseteq \{0,1\}^*$ be a random oracle. That is, for every string $z \in \{0,1\}^*$, include z in A independently with probability $1/2$. Show that $\mathbf{NP}^A \neq \mathbf{PSPACE}^A$ with probability at least 0.99 over the choice of the random oracle A.[2]

[2]Complexity class separations satisfy a *zero-one law*, which implies that the probability of a separation is actually 1.