15-855: Introduction to Complexity Theory — Fall 2015

Take-Home Midterm

Due before class **October 29, 2015**.

Instructions

You must work *entirely by yourself*. You may refer to any material from your notes, the posted lecture notes and other material, the homework problems, and the homework solutions; *nothing else*. Use piazza to ask any clarifications about the questions or pertaining material.

Attempt any 6 out of 9 problems. If you attempt more then 6 problems, we will take the highest six scores.

---

1. For each of the following statements, answer

   True, False, or Open

   according to our current state of knowledge of complexity theory, as described in class. Give brief but convincing justifications for your answers (if your choice is Open, describe which major open problem would be resolved by a resolution of the stated question in either direction).

   (a) The language $\{0^n 1^n \mid n \geq 1\}$ is NP-complete (under many-one poly-time reductions).

   (b) TQBF $\in \mathsf{NL}$.

   (c) $\mathsf{coNP} \neq \mathsf{NEXPTIME}$.

   (d) $2SAT$ polytime mapping reduces to $CLIQUE$

   (e) $CLIQUE$ polytime mapping reduces $2SAT$

   (f) $3SAT$ is NL-complete.

   (g) $\#\mathsf{L} = \#\mathsf{P}$, where $\#\mathsf{L}$ is the class of functions f such that there is a nondeterministic logspace machine M with $f(x) = \#\{\text{accepting paths of } M \text{ on } x\}$.

   (h) $\mathsf{EXPSPACE}$ contains all decidable languages.

   (i) There is some fixed integer c for which every language in PSPACE has a circuit family of size $O(n^c)$. (Here n = size of input.)

   (j) $\mathsf{NP} \subseteq \mathsf{PP}$.

2. Let Shortest-Path $= \{\langle G, s, t, d\rangle \mid d$ is the length of the shortest path from s to t in directed graph $G\}$. In other words, $\langle G, s, t, d\rangle \in$ Shortest-Path if and only if there is **no** path from s to t in G of length $d-1$ but there **is** such a path of length d.

   Prove that Shortest-Path is NL-complete. (Do not forget to show that Shortest-Path $\in \mathsf{NL}$!)

3. Prove that a language $A \in \mathsf{P}/\text{poly}$ if and only if $A \in \mathsf{P}^S$ for some set $S \subseteq \Sigma^*$ with the property that there exists a finite c such that for all positive integers n, $|S \cap \Sigma^n| \leq cn^c$.

4. Define a language to be k-shallow if it is accepted by a family of depth two circuits that consist of an AND of OR's where the fan-in of each OR gates is bounded by a constant k, independent of the length n of the input. Prove that if both A and the its complement are k-shallow, then membership in A can be tested by examining a constant number (independent of n) of input positions.

   (Hint: One approach is to use induction on k.)

5. Prove that $\mathsf{BPP} \subseteq \mathsf{ZPP}^{\mathsf{NP}}$.

6. You showed in Problem Set 2 that for every $k \geq 1$, $\mathsf{PH} \not\subseteq \mathsf{SIZE}(n^k)$. In this problem, you will show the same conclusion for the class PP.

   (a) We know by Toda's theorem, and the equality $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}}$ that you showed in problem set 2, that $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}}$. Thus, PP is at least as powerful as PH. Give a brief reason why this doesn't immediately show $\mathsf{PP} \not\subseteq \mathsf{SIZE}(n^k)$ as a consequence of $\mathsf{PH} \not\subseteq \mathsf{SIZE}(n^k)$.

   (b) Show that if $\mathsf{P}^{\mathsf{PP}} \subseteq \mathsf{P}/\text{poly}$, then $\mathsf{P}^{\mathsf{PP}} \subseteq \mathsf{MA}$.

   (Hint: Use the fact that Permanent has a checker, as defined in Problem Set 3.)

   (c) Prove that for every $k \geq 1$, $\mathsf{PP} \not\subseteq \mathsf{SIZE}(n^k)$.

   (Hint: Assume otherwise, and derive a contradiction. Towards this, start by using part (b) above.)

7. In this problem you'll prove the hitting property for expander walks that we saw in class.

   (a) Let $G = (V, E)$ be an expander graph on N vertices with degree d and expansion parameter $\lambda(G) = \lambda$. Let $X_1, X_2, \ldots, X_n$ be a random walk on G starting from a uniformly random vertex $X_1 \in V$. For any $B \subseteq V$ with $|B|/N = \beta$, show that

   $$\mathbb{P}[\wedge_{i\in[n]}(X_i \in B)] \leq (\beta + \lambda)^n.$$

   The proof of (a) will proceed in several parts.

   (i) Show that the normalized adjacency matrix A of G can be written as

   $$A = J + \lambda E,$$

   where J is the matrix with all entries equal to $1/N$, and $\|E\| \leq 1$. (Here, $\|\cdot\|$ denotes spectral norm).

   (ii) Let D be the diagonal matrix where $D_{j,j}$ is 1 if $j \in B$ and 0 otherwise. Show that

   $$\mathbb{P}[\wedge_{i\in[n]}(X_i \in B)] = \|(DA)^{n-1} \cdot D \cdot \mathbf{1}/N\|_1.$$

   (iii) Use part (i) to bound

   $$\|(DA)^{n-1} \cdot D \cdot \mathbf{1}/N\|_1 \leq (\beta + \lambda)^n.$$

   (Note: Any bound that decays exponentially in n will receive partial credit)

(b) Extend your argument in part (a) to show that, for any $S \subseteq [n]$,

$$\mathbb{P}[\wedge_{i \in S}(X_i \in B)] \leq (\beta + \lambda)^{|S|}.$$

8. In this problem you'll use the conclusion of the previous problem (which you may assume for this problem) to prove the Chernoff bound for expander walks that we saw in class. (As well as giving an alternative proof for the standard Chernoff bound.)

   (a) Let $X_1, \ldots, X_n$ be $\{0,1\}$-valued random variables. Suppose there is some $\delta \in (0,1)$ so that for all $S \subseteq [n]$,

   $$\mathbb{P}[\wedge_{i \in S}(X_i = 1)] \leq \delta^{|S|}.$$

   Show that for any $\gamma \in [\delta, 1]$,

   $$\mathbb{P}\left[\sum_{i=1}^{n} X_i \geq \gamma n\right] \leq e^{-nD(\gamma || \delta)},$$

   where

   $$D(p||q) := p \log(p/q) + (1-p)\log((1-p)/(1-q)).$$

   (Hint: Imagine choosing $S \subseteq [n]$ so that each index is included independently with probability $q = (\gamma - \delta)/(\gamma(1-\delta))$. Let $\mathcal{E}$ be the event that $\sum_{i=1}^{n} X_i \geq \gamma n$, and notice that $\mathbb{P}[\mathcal{E}] \leq \frac{\mathbb{E}[\wedge_{i \in S} X_i = 1]}{\mathbb{E}[\wedge_{i \in S} X_i = 1 | \mathcal{E}]}$, where the expectation is over both S and the X_i.)

   (b) Show that $D(x + \epsilon || x) \geq 2\epsilon^2$, and arrive at the same conclusion with

   $$\mathbb{P}\left[\sum_{i=1}^{n} X_i \geq \gamma n\right] \leq e^{-2n(\gamma - \delta)^2}.$$

   Given the conclusion of the previous problem, conclude a Chernoff-like bound for expander walks.

9. Consider a random variable $X = (X_1, \ldots, X_n) \in \{0,1\}^n$ with the following property. For some $\delta > 0$, and for all i, and for all $x_1, \ldots, x_{i-1} \in \{0,1\}^{i-1}$,

   $$\mathbb{P}\left[X_i = 1 \mid X_j = x_j \forall j < i\right] \in [\delta, 1 - \delta].$$

   Call such a source "δ-unpredictable."

   (a) Show that such a random variable X has $H_\infty(X) \geq \log\left(\frac{1}{1-\delta}\right) \cdot n$.

   (b) Show that for all $f : \{0,1\}^n \to \{0,1\}$, there exists a δ-unpredictable source X on $\{0,1\}^n$ with

   $$\left|\mathbb{P}[f(X) = 1] - \frac{1}{2}\right| \geq \frac{1}{2} - \delta.$$

   Conclude that we cannot have deterministic extractors for such sources.

   (Hint: Prove by induction on n the stronger statement that for any function $f : \{0,1\}^n \to \{0,1,\perp\}$, there is a δ-unpredictable source X so that $|\mathbb{P}[f(X) = 1 \mid f(X) \neq \perp] - 1/2| \geq 1/2 - \delta$.)