

Computational Complexity II

Take Home Exam

November 24, 2006

Due Date: Nov 25 '06, 12 noon.

Total points: 100

Note: Write precise answers. There are nine questions in all. Please *do not* discuss with each other. Please slip your answers under my office door on Saturday, Nov 25. I'll collect your answers soon after the deadline.

The first two problems require suitable relativizations of the Impagliazzo-Wigderson theorem.

(1) The problem is to “derandomize” the Valiant-Vazirani Lemma. Formulate the problem and identify the right kind of pseudorandom generator required to do the derandomization. Make a suitable hardness assumption and prove the existence of such a generator under the assumption. **10 points**

(2) Show under a suitable hardness assumption that $\text{PH} \subseteq \oplus\text{P}$. **10 points**

(3) Suppose \mathcal{A} is a BPP algorithm with error probability $1/3$ that on inputs of length n uses r random bits. Let $N = 2^r$ and G be a λ -spectral expander on N nodes for some constant $\lambda < 1$. Prove that the following strategy will allow us to reduce the error probability to $2^{-\Omega(t)}$: pick a random element $w_1 \in V(G)$ and do a t -step random walk w_1, \dots, w_t . Output the majority vote on $\mathcal{A}(x, w_i), 1 \leq i \leq t$. **15 points**

(4) Suppose $f : X \times Y \rightarrow \{0, 1\}$ for finite sets X and Y and we are interested in lower bounding the deterministic communication complexity $D(f)$ of f . Let $|X| = M$ and $|Y| = N$. Define the $M \times N$ matrix \mathcal{M} whose rows are indexed by X and columns by Y , and whose x, y -th entry is $f(x, y)$. Show that $\log_2 \text{rank}(\mathcal{M})$ is a lower bound on $D(f)$. Use this to lower bound $D(f)$ for the disjointness problem. Can you upper bound $D(f)$ as a function of $\log_2 \text{rank}(\mathcal{M})$? **15 points**

(5) Let G be a connected undirected d -regular multigraph. For each $s \in V(G)$, let C_s denote the expected time to visit all vertices of G in a random walk on G starting at vertex s . Let $C(G) = \max_s \{C_s\}$. If G is a λ -spectral expander derive a bound (as tight as possible) for $C(G)$ in terms of λ and n . What does this bound imply for an arbitrary undirected d -regular multigraph? **10 points**

(6) Show that either $\text{NEXP} \not\subseteq \text{P/poly}$ or E does not have circuits of size $2^{\epsilon n}$ for some constant $\epsilon > 0$. **5 points**

(7) Consider the two statements $\text{coNP} \subseteq \text{NP}/\text{poly}$ and $\text{coNE} \subseteq \text{NEXP}/\text{poly}$. Is either of them unconditionally true? Does one imply the other? Does one (or both) imply some unlikely consequence like, for example, $\text{P}=\text{NP}$ or the collapse of PH? **15 points**

(8) In $\text{PCP}(r(n), q(n))$, recall that $r(n)$ bounds the number of random bits and $q(n)$ the number of query bits used for inputs of length n . The protocol accepts “yes” instances with probability 1 and rejects the “no” instances with constant probability, say $1/2$. Show that $\text{NP} \subseteq \text{PCP}(o(\log n), O(1))$ implies $\text{P}=\text{NP}$. What is the class $\text{PCP}(O(\log n), 2)$? **10 points**

(9) Given oracle access to a function $f : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$, p a prime independent of n , and a parameter ϵ , give a randomized algorithm that runs in time polynomial in n/ϵ and outputs a list of all linear functions $L : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$ that agrees with f on at least $\frac{1}{p} + \epsilon$ of inputs from \mathbb{Z}_p^n . **10 points**