COMP 531: Advanced Theory of Computation (Winter 2014)

Assignment 3

Due March 17th

Instructions

Follow these instructions closely.

You will benefit most if you seriously try solving each problem yourself. You may work with each other but you must write up your own solutions. For each question, you should clearly acknowledge the people you have worked with. You are not allowed to use any resources that contain the solution to an assignment question. However, we value honesty above all. You will get full marks if you happen to find the solution to a question and you write your own solution, **as long as you properly acknowledge your source**. Failure to acknowledge your source can result in 0 points.

Clarity and conciseness of your solutions are as important as correctness. It is important to learn how to write your ideas and solutions clearly and rigorously. You will lose marks for correct solutions that are poorly explained/presented. When writing your solutions, assume that your audience is your class mates rather than the instructor of the course. The high level ideas and an overview of your argument should be presented before any technical details, and all non-trivial claims have to be proven.

If you do not know how to solve a problem, do not answer it. This will earn you 20% of the points. Do not make yourself believe in a wrong proof, this is bad for you. **And definitely do not try to sell it!** If you don't know how to solve a problem but you have some non-trivial ideas, write them down. If you have a solution with gaps, write your argument and clearly indicate the gaps.

Submit your assignments in class or send a copy to `aada@cs.mcgill.ca` before midnight of the due date.

Questions

1. Let P be a randomized protocol that computes a function $F : X \times Y \to \{0,1\}$ with ϵ probability of error. Design a new protocol P' for F that has error probability less than ϵ, but has cost more than P (i.e., reduce the error probability of P at the expense of increasing the cost). What kind of trade-off can you get between the cost and the error probability? Explain whether your argument depends on the underlying computational model.

2. Let $F : X \times Y \to \{0,1\}$. Let $\mathbf{U}(F)$ denote the cost of the most efficient randomized protocol P such that for all $(x,y) \in X \times Y$, $\Pr[F(x,y) \neq P(x,y)] < 1/2$. Note that the success criterion is very liberal. Achieving error $1/2$ is trivial: just output a random bit. In this model it is important that the randomness used is *private*: show that if we allow *public* randomness then computing every function becomes trivial.

3. Let $\pi(n)$ be defined as the number of primes less than or equal to n. In CS, most applications require only the fact that $\pi(n) = \Omega(n/\log n)$.

   (a) Show that a prime p divides $n!$ $\sum_{i=1}^{i=\infty} \lfloor \frac{n}{p^i} \rfloor$times. Define $r(p)$ as the natural number such that $p^{r(p)} \leq 2n < p^{r(p)+1}$. Show that p does not divide $\binom{2n}{n}$ more than $r(p)$ times. Conclude that $2^n \leq \binom{2n}{n} \leq \prod_{prime\ p \leq 2n} p^{r(p)} \leq (2n)^{\pi(2n)}$.

   (b) Show that $\pi(n) \geq \frac{n}{2 \log n}$.

   (c) Let x and y be two distinct n-bit integers. Let p be a uniformly chosen random prime in the range $[2..4n^2]$. What kind of upper bound can you get for $\Pr[x = y \pmod p]$?

   (d) Let $\mathrm{EQ} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ denote the equality function seen in class. Show that $\mathbf{R}^{\epsilon}(\mathrm{EQ}) = O(\log n)$ using a protocol that is different than the one presented in class. What is the error probability of your protocol?

4. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a communication problem and let $\mathbf{D}(F)$ denote the deterministic communication complexity of F. Consider the following model for computing F. Alice sends a message to Bob and then Bob decides the output. The cost is the length of Alice's message. Let $\mathbf{D}^{A \to B}(F)$ denote the cost of the most efficient protocol that computes F in this model. Give an example of a function F with small $\mathbf{D}(F)$ but large $\mathbf{D}^{A \to B}(F)$. Try to make the gap as large as possible.

5. (a) Let $F : X \times Y \to \{1,-1\}$ and μ be a distribution over $X \times Y$. In class we saw the discrepancy method to prove lower bounds on the randomized communication complexity:

$$\mathbf{R}^{\epsilon}(F) \geq \mathbf{D}^{\epsilon}_{\mu}(F) \geq \log\left(\frac{1-2\epsilon}{\mathrm{disc}_{\mu}(F)}\right).$$

Recall that the *Disjointness* function is defined as $\mathrm{DISJ}(x) = 1$ iff there is some $i \in [n]$ with $x_i = y_i = 1$. Show that under any distribution μ over $\{0,1\}^n \times \{0,1\}^n$, $\mathrm{disc}_\mu(\mathrm{DISJ}) \geq \Omega(1/n)$. This means that one cannot prove strong randomized communication complexity lower bounds for DISJ using the discrepancy method.

(b) Let $G : X \times Y \to \{1, -1\}$. Recall that the correlation between F and G under the distribution μ is defined as

$$\mathrm{Cor}_\mu(F, G) = \left| \Pr_{(x,y)\sim\mu}[F(x,y) = G(x,y)] - \Pr_{(x,y)\sim\mu}[F(x,y) \neq G(x,y)] \right|.$$

Prove

$$\mathbf{R}^\epsilon(F) \geq \mathbf{D}^\epsilon_\mu(F) \geq \log\left(\frac{\mathrm{Cor}_\mu(F,G) - 2\epsilon}{\mathrm{disc}_\mu(G)}\right).$$

This allows us to prove a lower bound for the communication complexity of F in situations where F itself does not have small discrepancy, but it correlates well with a function G (e.g., the correlation is some constant more than 2ϵ) that has small discrepancy. Indeed, one can prove strong lower bounds on the randomized communication complexity of DISJ using this technique.

6. In this question you are asked to read and write about an application of communication complexity. Find a result that interests you and present the main ideas behind it. Focus on how communication complexity is used in the result. Limit your answer to 1 to 2 pages. Communication complexity has connections/applications to circuit complexity, time/space tradeoffs for Turing Machines, VLSI chips, machine learning, game theory, data structures, proof complexity, pseudorandom generators, pseudorandomness, branching programs, lower bounds for polytopes representing NP-complete problems, data streaming algorithms, quantum computation, etc. You can use any resource you want.