CS 2429
Communication Complexity
ASSIGNMENT # 2
Due: November 28, 2012

1. (Private versus Public Randomness for Information Complexity). In the context of communication complexity, private and public coins are more or less equivalent. This problem explores this question with respect to information cost. Recall that a private coin protocol for a function $f : X \times Y \to Z$ can be viewed as a binary tree such that: (i) each nonleaf node is owned by A or B; (ii) Each nonleaf node owned by a player has a set of children that are owned by the other player; (ii) every node (owned by A) is associated with a function mapping X to distributions on children of the node, and similarly for B; (iii) the leaves of the protocol are labeled by output values. A public coin protocol is a distribution on private coin protocols, run by first using shared randomness to sample an index r and then running the corresponding private coin protocol, π_r. Given a protocol, π, a transcript of π on (x, y), $\pi(x, y)$ is the concatenation of the public randomness with all the messages that are sent during this execution of π. $\Pi(x, y)$ is a random variable over transcripts. The information cost of a protocol π over inputs from $X \times Y$ with respect to distribution μ is given by:

$$IC_\mu(\pi) = I(\Pi; X|Y) + I(\Pi; Y|X).$$

The ϵ-error information complexity of f with respect to μ is the infimum of the information cost over all (randomized) protocols π that achieve an error of at most ϵ with respect to μ.

   (a) Newman's theorem tells us that any protocol with public randomness can be converted into a protocol that is almost as efficient and with only private randomness. Does this hold in the information complexity context? Ie. Prove or disprove that if there is a protocol with information cost c and public randomness, that it can be simulated by a protocol with only private randomness and such that the resulting protocol has information cost close to c.

   (b) What about the reverse direction? It is trivial that if we have a protocol with only private randomness, that it can be simulated with public randomness with respect to communication complexity. Prove or disprove this statement in the context of information complexity. Hint: Consider a protocol where one party sends $x+r$, the bitwise parity of x with a random string r.

2. The informational divergence between two distributions is $D(A||B) = \sum_x A(x) \log(A(x)/B(x))$. Prove that $D(A||B) \geq |A - B|^2$.

3. Let μ be a distribution over inputs, and let $IC^i_\mu(\pi)$ be the internal information cost of protocol π and let $IC^o_\mu(\pi)$ be the external information cost of π.

   (a) Prove that if μ is a product distribution then $IC^i_\mu(\pi) = IC^o_\mu(\pi)$.

   (b) Prove that for every μ, $IC^o_\mu(\pi) \geq IC^i_\mu(\pi)$.

4. Let π be a permutation of $x_1, \ldots, x_n$, and let f be a boolean function on $x_1, \ldots, x_n$. Define $D(f, \pi)$ to be the deterministic 2-party communication complexity of f, where player 1 receives $\pi_1(x), \ldots, \pi_{n/2}(x)$, and player 2 receives $\pi_{n/2+1}(x), \ldots, \pi_n(x)$. Let $D^{worst}(f)$ to be the maximum over all π of $D(f, \pi)$. Consider the function $f_n(x_1, \ldots, x_n)$ which is 1 iff the n-bit string $x_1 \ldots x_n$ contains two consecutive 1's. Prove that $D^{worst}(f_n) = \Theta(n)$.

5. (Complexity of Relations) For any graph G with n vertices, consider the following communication problem. Alice receives a clique C in G and Bob receives an independent set, I. They want to communicate in order to determine $|C \cap I|$. (Note that this number is either 0 or 1.) Prove an $O(\log^2 n)$ upper bound on the (deterministic) communication complexity.