1: Problem 1 (Randomized and Distributional Communication Complexity) 25 pts

Let $f : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}$ be a 2-party Boolean function.

(1) Show that f admits a 2-bit randomized (public-coin) communication protocol that succeeds with probability $\geq 1/2 + 2^{-2n}$.

(2) Show that for any prior distribution μ, there is a 2-bit protocol for f with success probability $\geq 1/2 + Disc_\mu(f)$, where $Disc_\mu(f)$ is the discrepancy of f w.r.t μ.

(3) Show that $R^{priv}_{1/3}(f) \geq \lg D(f)$, where $D(f)$ is the deterministic communication complexity of f and $R^{priv}_{1/3}(f)$ is the private-coin randomized communication complexity of f with error $1/3$. (For simplicity, you may assume that the probabilities of transmitting $0/1$ in any execution of a randomized protocol for f are rational numbers). Make sure you understand why your argument fails for *public*-coin protocols.

Conclude that $R^{priv}_\epsilon(EQUALITY_n) \geq \Omega(\lg n)$ (which is the maximal separation possible due to Neumann's theorem).

2: Problem 2 (Internal vs. External Information Complexity) 20 pts

Recall that the *external information complexity* of a communication protocol π with respect to $(X,Y) \sim \mu$, is defined as $IC^{ext}_\mu(\pi) := I(\Pi; XY)$ (as usual, Π denotes the (r.v) transcript of π).

(1) Prove that for any (randomized) protocol π and any distribution μ, $IC^{ext}_\mu(\pi) \geq IC_\mu(\pi)$.

(2) Prove that if μ is a *product* distribution ($\mu(x,y) = \mu(x)\mu(y)$), then $IC^{ext}_\mu(\pi) = IC_\mu(\pi)$.

3: Problem 3 (Indexing Lower Bound via Information Complexity), 25 pts

Let $IND_n : \{0,1\}^n \times [n] \mapsto \{0,1\}$ denote the Indexing function, in which Alice holds an n-bit array A, Bob holds an index $i \in [n]$, and the players' goal is to compute $IND_n(A,i) := A_i$.

There is a trivial $\lceil \lg n \rceil$-bit protocol by having Bob send his index to Alice. But what if *only Alice can speak*? Let us denote by $R^{A \to B}_{1/3}(IND_n)$ the *one-way* randomized communication complexity of IND_n, i.e., the minimum length of a (possibly randomized) message $|M|$ that Alice can send Bob, which allows Bob to recover A_i w.p $\geq 1/3$. Prove that $R^{A \to B}_{1/3}(IND_n) \geq \Omega(n)$.

(Hint: Recall that if the entries A_j are independent random variables, then $\sum_j I(A_j; M) \leq I(A_1, \ldots, A_n; M)$. This should guide you how to find the hard distribution $(A,i) \sim \mu$. Then use Fano's inequality).

4: Problem 4, An $\Omega(\sqrt{n})$ LB for DISJ under product distributions, 30 pts

In this exercise, we will use a simplified version of the $\Omega(n)$ randomized Set-Disjointness lower bound we saw in class, to prove that the distributional communication complexity of $DISJ_n$ with respect to *product distributions* is $\Omega(\sqrt{n})$. To this end, let μ denote the distribution on (X_i, Y_i), in which X_i and Y_i are i.i.d $Ber(1/\sqrt{n})$, and let us consider the product distribution $(X, Y) \sim \mu^n$ on inputs $X := X_1, \ldots, X_n, Y := Y_1, \ldots, Y_n \subseteq [n]$. A simple calculation shows that $\Pr_{\mu^n}[X \cap Y = \emptyset] \approx 1/e$, so for large enough n, the distribution is roughly "unbiassed". We shall show that $D^{1/3}_{\mu^n}(DISJ_n) \geq \Omega(\sqrt{n})$:

(1) Let Π be an optimal (deterministic) protocol for $DISJ_n$ under μ^n (recall that we may indeed assume Π is deterministic by an averaging principle). Use Π in order to design a (randomized) protocol π for the 2-bit $AND(a, b)$ function s.t: (i) $\forall (a, b) \in (\{0, 1\})^2 \quad \Pr_\pi[\pi(a, b) = AND(a, b)] \geq \Omega(1)$, and (ii) When $(A, B) \sim \mu$, then $I_\mu(\pi; A, B) \leq \|\Pi\|/n$. (note that, since μ is *product*, the "embedding" is simpler as the players can *privately* complete the remaining coordinates to Π).

(2) Let π_{ab} denote the distribution of (the transcript of) π when $A = a, B = b$. Use part (1.i) to prove that : (i) $\Delta(\pi_{00}, \pi_{11}) \geq \Omega(1)$ (where $\Delta(\cdot, \cdot)$ is the total variation distance). (ii) Use part (1.ii) + Pinsker's inequality to prove that: $\mathbb{E}_{(a,b)\sim\mu}[\Delta^2(\pi_{a,b}, \pi)] \leq O(\|\Pi\|/n)$, where π here denotes the prior distribution of the transcript $\pi(A, B)$, where $(A, B) \sim \mu$.

(3) Use the definition of μ to argue that part (2.ii) implies $\Delta^2(\pi_{10}, \pi) \leq O(\|\Pi\|/\sqrt{n})$, and similarly $\Delta^2(\pi_{01}, \pi) \leq O(\|\Pi\|/\sqrt{n})$. Now conclude that

$$\Delta^2(\pi_{10}, \pi_{01}) \leq O(\|\Pi\|/\sqrt{n}).$$

(4) On the other hand, use part (2.i) and the "Cut-and-Paste" Lemma from class, to prove that $\Delta^2(\pi_{10}, \pi_{01}) \geq \Omega(1)$.

(5) Conclude by (3) and (4) that $\|\Pi\| \geq \Omega(\sqrt{n})$.

5: Problem 5, (Parity Game), 25 pts

Alice and Bob play the following communication game $G_\oplus(x, y)$: The players receive n-bit strings x, y respectively, s.t $Parity(x) = \oplus_{i=1}^n x_i = 0$, and $Parity(y) = \oplus_{i=1}^n y_i = 1$. Note that this implies that $x \neq y$. The goal of Alice and Bob is to *deterministically* find a coordinate $i \in [n]$ s.t $x_i \neq y_i$ (both players must know such i by the end of the protocol). Show that any deterministic protocol that solves $G_\oplus$ must spend $2\lg(n)$ bits of communication.

(Hint: Design a hard distribution μ and then show that the information learnt by each player from any Π that solves the game under μ must be large).