E2 206: Information and Communication Complexity (2017)
Homework 1

Instructor: Himanshu Tyagi

Homework Questions

Q1 Consider discrete random variables X, Y taking values in $\mathcal{X} \times \mathcal{Y}$. For $\lambda > 0$, let $\mathcal{L}(y)$ denote the set

$$\mathcal{L}(y) = \{x \in \mathcal{X} : -\log \mathrm{P}_{X|Y}(x|y) \leq \lambda\}, \quad \forall\, y \in \mathcal{Y}.$$

Suppose that $\mathbb{P}(X \in \mathcal{L}(Y)) \geq 1 - \epsilon$. For $f(x, y) = x$, show that there exists a one-way randomized communication protocol which 2ϵ-computes f by communicating no more than $\lambda + \log 1/\epsilon + 2$ bits.

Q2 Show that

$$H_{\mathtt{min}}(P_{XY}|Y) = -\log \sum_y \mathrm{P}_Y(y) \max_x \mathrm{P}_{X|Y}(x|y).$$

Q3 Establish the following version of the leftover hash lemma:

Let (X, Y) be discrete random variables taking values in $\mathcal{X} \times \mathcal{Y}$, and $\mathcal{F}$ be a 2-universal hash family consisting of mappings from $\mathcal{X}$ to $\{0, 1\}^k$. Let F be distributed uniformly over $\mathcal{F}$. Then, for every $0 < \eta < 1$

$$\mathbb{E}\left[d_{\mathtt{TV}}\left(\mathrm{P}_{F(X)Y}, \mathrm{P}_{\mathtt{unif},k} \times \mathrm{P}_Y\right)\right] \leq 2\eta + \frac{1}{2}\sqrt{2^{k - H^{\eta}_{\mathtt{min}}(P_{XY}|Y)}},$$

where $\mathrm{P}_{\mathtt{unif},k}$ denotes a uniform distribution over $\{0, 1\}^k$.

Q4 Show that for an interactive private coin protocol π,

$$\mathtt{IC}(\pi|\mathrm{P}_{XY}) = \sum_{i:i \text{ odd}} I(\Pi_i \wedge X|Y) + \sum_{i:i \text{ even}} I(\Pi_i \wedge Y|X).$$

Q5 Compute $\mathtt{IC}(f)$ for the following functions:

(i) $f(x, y) = x$

(ii) $f(x, y) = (x, y)$

(iii) $f(x, y) = f_k(x, y)$ defined recursively as follows: $f_0(x, y) =$ constant,

$$f_{i+1}(x, y) = \begin{cases} f_{i+1}\left(f_i(x, y), x\right), & i \text{ even}, \\ f_{i+1}\left(f_i(x, y), y\right), & i \text{ odd}, \end{cases}$$

for $0 \leq i \leq k - 1$.