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

Q2 Show that
\[
H_{\text{min}}(P_{XY}|Y) = -\log \sum_y P_Y(y) \max_x P_{X|Y}(x|y).
\]

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 $0 < \eta < 1$
\[
\mathbb{E} \left[ d_{TV}(P_{F(X)Y}, \text{unif}_{k} \times P_Y) \right] \leq 2\eta + \frac{1}{2} \sqrt{2^{k-H_{\text{min}}(P_{XY}|Y)}}
\]
where $\text{unif}_{k}$ denotes a uniform distribution over $\{0,1\}^k$.

Q4 Show that for an interactive private coin protocol $\pi$,
\[
\text{IC}(\pi|P_{XY}) = \sum_{i: i \text{ odd}} I(\Pi_i \land X|Y) + \sum_{i: i \text{ even}} I(\Pi_i \land Y|X).
\]

Q5 Compute $\text{IC}(f)$ 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: $f_0(x, y) = \text{constant},$
\[
f_{i+1}(x, y) = \begin{cases} f_i(x, y), & i \text{ even}, \\ f_i(f_i(x, y), y), & i \text{ odd}, \end{cases}
\]
for $0 \leq i \leq k - 1$. 

1