Time Limit: 3 hours

Instructions:

• No written material is allowed.

• Please write clearly, and prove your answers. In case you are using an unproven “fact”, please state the fact clearly, and explain why you are not proving it: “lack of time”, “easy to see”, etc.

• You should answer all four questions.

Good Luck!
Unless said otherwise, in the following $X, Y, Z$ are (jointly distributed) random variables, and $p, q$ are distributions over $[m]$.

1. (25 point, entropy)

   (a) (10 points) Define the following notions: $H(X), H(X, Y), H(X|Y)$.

   (b) (15 points) Let $X, Y$ be integer-valued random variables and let $Z = X + Y$.
      i. Prove that $H(Z|X) = H(Y|X)$.
      ii. Prove that if $X$ and $Y$ are independent, then $H(Z) \geq \max\{H(X), H(Y)\}$.
      iii. Given an example of $X, Y$ such that $H(Z) < \min\{H(X), H(Y)\}$

2. (25 points, relative entropy)

   (a) (5 points) define $D(p\|q)$.

   (b) (10 points) Prove that $I(X, Y) = \mathbb{E}_{x\leftarrow X}[D(Y|X=x\|Y)]$.

   (c) (10 points) Assume that $D(p\|q) < 5$ and that $\Pr_{x\leftarrow p}[P(x) = 1] = 1$, for some deterministic algorithm $P$. Prove that $\Pr_{x\leftarrow q}[P(x) = 1] \geq 1/32$.

3. (25 points, compression)

   Let $X$ be a random variable over $\{0, 1\}^*$ and let $C$ be a binary prefix code for $X$.

   Prove that $H(X) \leq L_X(C)$ (recall that $L_X(C) = \mathbb{E}_{x\leftarrow X}[C(x)]$).

4. (25 points, pseudoentropy)

   Let $f: \{0, 1\}^n \mapsto \{0, 1\}^n$ be a permutation, and let $g: \{0, 1\}^{n+1} \mapsto \{0, 1\}^{n+1}$ be defined by
   
   $$g(x) = \begin{cases} x_1, f(x_2, \ldots, x_{n+1}), & x_1 = 0; \\ x, & \text{otherwise}. \end{cases}$$

   Let $b$ be an $(s, \varepsilon)$-hardcore predicate of $f$ and let $h: \{0, 1\}^{n+1} \mapsto \{0, 1\}^{n+2}$ be defined by
   $h(x) = g(x), b(x_2, \ldots, x_{n+1})$. Prove that $h(U_{n+1})$ has $(s - O(n), \varepsilon)$ min-pseudo-entropy $n + \frac{3}{2}$.

   (i.e., $\exists c > 0$ and rv $Y$ with $H_\infty(Y) \geq n + \frac{3}{2}$, such that and no algorithm of size $s - cn$ distinguishes $Y$ from $h(U_{n+1})$ with advantage $> \varepsilon$).

   Bonus (10 points): Assuming that $b$ is computable by algorithm of size $s(n)$, prove that $h$ does not have $(s(n) + O(n), \frac{1}{4})$ pseudo-entropy $n + 2$.

   (i.e., $\exists c > 0$ such that for any rv $Y$ with $H(Y) \geq n + 2$, exists algorithm of size $s(n) + cn$ that distinguishes $Y$ from $h(U_{n+1})$ with advantage $\geq \frac{1}{4}$).