EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 2
30 January 2020

Professor Dunham
Due: 6 February 2020

Suggested Reading in Menezes, Oorschot and Vanstone: Chapter 10, Sections 1-3 and 5.
Suggested Reading in Medard: Lectures 1 and 2 (through Data Processing Theorem).
Suggested Reading in MacKay: Sections 2.1-2.7 (2.3 optional), 4.1, 5.1-5.5.

1. Establish the following relationships:
   (a) $H(X|Y) \geq 0$.
   (b) $H(Y,Z|X) = H(Y|X) + H(Z|YX)$.
   (c) Show that $H(Y|X) = H(Y)$ if X and Y are independent.

2. Given a discrete random variable X, define a new random variable $Y = g(X)$ where g is a deterministic function. Show that $H(Y) \leq H(X)$. Under what conditions will the equality hold.

3. Let X and Y be real-valued random variables and let $Z = X + Y$.
   (a) Show that $H(Z|X) = H(Y|X)$.
   (b) If X and Y are independent, show that $H(Y) \leq H(Z)$ and that $H(X) \leq H(Z)$.
   (c) Give an example where $H(X) > H(Z)$ and $H(Y) > H(Z)$. *Hint:* It suffices to consider a random variable that only takes on the values of 0 and 1.

4. Let X be a random variable that has a geometric probability mass function with parameter α (as discussed in Handout #04). Determine $H(X)$ as a function of the parameter α.