Homework Problems

EE 480F

March 3, 2005

1. (a) Write the definition of $H(X)$.

   (b) Write the definition of $H(Y|X)$ and $H(Y,X)$.

   (c) Show that $H(Y,X) = H(Y|X) + H(X)$

2. Prove $I(X;Y) = I(Y;X)$.

3. On a loaded die, Pr[1] = Pr[2] = Pr[5] = Pr[6] = 1/8, while Pr[3] = Pr[4] = 1/4. A die is equally likely to be fair or loaded, so assume equal priors ($\pi_1 = \pi_0 = 0.5$), and uniform costs.

   For a single die roll:

   (a) Show the likelihood ratio test for all six outcomes.

   (b) Show whether each outcome is considered evidence that the die is fair or loaded.

   (c) What is P_F and P_M for a single die roll?

   Suppose you roll the following sequence: 1, 3, 2, 2, 4, 5, 3. Do you conclude the die is fair or loaded?

4. Suppose a cipher has perfect secrecy. Must every key be chosen with equal probability?

5. If $H(X) = H(X|g(X))$, what does that tell us about $g(x)$?

6. The one-time pad cipher has perfect secrecy. But there is a key ($k =$ `000000000000000`...) that does nothing: $x = \texttt{Encrypt}(x, k)$. This means the data is transmitted unencrypted!

   (a) Explain why a cipher can have such a flaw and yet be considered "perfect".

   (b) Can you fix the cipher so that it does not possess this "weak" key, yet retains perfect secrecy?