Homework Problems

EE 480F

March 14, 2005

1. (a) Write the definition of $H(X)$.
   (b) Write the definition of $H(Y|X)$ and $H(Y,X)$.
   (c) Show that $H(Y,X) = H(Y|X) + H(X)$

   We can use the fact: $\Pr[X = x] = \sum_y \Pr[X = x, Y = y]$. So $H(X) = \sum_x \Pr[x] \log 1/\Pr[x] = \sum_x \sum_y \Pr[x,y] \log 1/\Pr[x]$. Now the sums of the two expressions $H(X)$ and $H(Y|X)$ match.

$$H(Y|X) + H(X) = \sum_{x,y} \Pr[x,y] \log 1/\Pr[y|x] + \sum_{x,y} \Pr[x,y] \log 1/\Pr[x]$$

$$= \sum_{x,y} \Pr[x,y] \log 1/(\Pr[y|x] \Pr[x])$$

   Since $\Pr[y|x] \Pr[x] = \Pr[x,y]$, we have $\sum_{x,y} \log 1/\Pr[x,y] = H(X,Y)$.

2. Prove $I(X;Y) = I(Y;X)$. $I(X;Y) = H(Y) - H(Y|X)$. Now, the

   chain rule above gives us $H(Y|X) + H(X) = H(X,Y) = H(X|Y) + H(Y)$. We simply expanded the rule in both directions. Rearranging gives us $H(Y) - H(Y|X) = H(X) - H(X|Y)$.

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?

For outcomes 1, 2, 5 and 6, the likelihood ratio is $(1/8)/(1/6) = 3/4$. For outcomes 3 and 4, the likelihood ratio is $(1/4)/(1/6) = 3/2$. For equal priors and uniform costs, our threshold is 1, so this means that for a single die roll, outcomes 3 and 4 trigger an alarm (biased!) These have a likelihood ratio above the threshold.

P_F is the probability of a false alarm. On a fair die, the probability of a 3 or 4 is $P_F = 1/3$. For a miss, we roll a biased die and imagine an alarm not occurring. This is the probability of a 1,2,5 or 6 on the biased die, with a probability of 1/2.

Finally, for a sequence of rolls, we just compute the product of the likelihood ratios: $3^7/2^1 1 = 2187/2048$, which is just over the threshold.

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

No. A redundant key can give you perfect secrecy with a skewed distribution.

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

This means X and $g(X)$ are independent, even though one is a function of the other. We can also see that by the definition, $I(X; g(X)) = 0$. How can $g(X)$ give us no information about X? The answer is that the function g is constant.

Note also that from problem 2, $I(g(X); X) = 0$ also, so $H(g(X)|X) = H(g(X))$. This means that knowing X does not help you compute $g(X)$!! Again, this can only happen when $g(x)$ is constant. Otherwise, knowing the input would help determine the output.

6. The one-time pad cipher has perfect secrecy. But there is a key ($k =$ `000000000000000`$\ldots$) that does nothing: $x =$ `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?

   A cipher with perfect secrecy must have the possiblity that the output equals the input. Otherwise, you leak information to the adversary: the adversary can rule out one possible message as the plaintext, namely the one that was just intercepted.

   You can't fix this. If you adopt the rule that any weak key is discarded just to be on the safe side, your ciphertext will leak some information about the plaintext.