ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
Communication Systems Department

Handout 15 Information Theory and Coding
Midterm December 4, 2000

Problem 1. (30 points.) Let M be a random variable representing a message taking values in $\mathcal{M}$. The message set $\mathcal{M}$ is finite and without loss of generality we assume $\mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$. Let Y be the random variable observed by a receiver which attempts to estimate M upon observing Y. More specifically, the receiver uses a function $g : \mathcal{Y} \to \mathcal{M}$ to declare an estimate $\hat{M} = g(Y)$.

An error occurs if $\hat{M}$ is different from M and this occurs with probability $P_e \stackrel{\triangle}{=} \Pr\{\hat{M} \neq M\}$.

(a) (4 pts.) Let E be an arbitrary random variable. Show that

$$H(M|Y) + H(E|M,Y) = H(E|Y) + H(M|E,Y).$$

(b) (4 pts.) Let E be the random variable defined by

$$E = \begin{cases} 0 & \text{if } g(Y) = M \\ 1 & \text{otherwise.} \end{cases}$$

Show that $H(E|M,Y) = 0$.

(c) (8 pts.) For E defined as in (b), justify (i) and (ii) below:

$$\begin{aligned} H(M|E,Y) &\stackrel{(i)}{=} \Pr(E=1) H(M|Y, E=1) \\ &\stackrel{(ii)}{\leq} \Pr(E=1) \log(|\mathcal{M}| - 1). \end{aligned}$$

where

$$H(M|Y, E=1) = -\sum_{m,y} \Pr(M=m, Y=y|E=1) \log \Pr(M=m|Y=y, E=1)$$

is the conditional entropy of M given Y conditioned on the event $E = 1$.

(d) (4 pts.) Argue that $H(E|Y) \leq H(E)$.

(e) (4 pts.) Show that $H(E) = h(P_e)$ and that $\Pr\{E=1\} = P_e$, where $h(p) = -p \log p - (1-p)\log(1-p)$ is the binary entropy function.

(f) (6 pts.) Starting with the equality in (a), use parts (b) through (e) to find an upper bound on $H(M|Y)$ that depends only on P_e and $|\mathcal{M}|$.

Problem 2. (35 points.) Consider a cryptographic system in which we wish to encrypt a source X with entropy $H(X)$ using a secret key K with entropy $H(K)$. There is a function $f(x,k)$ that maps the source X and the key K to the encrypted output Y. This function is decryptable in the sense that for each key k, $f(x_1,k) \neq f(x_2,k)$ for source letters $x_1 \neq x_2$. Assume that X and K are independent random variables. Assume also that the encryption scheme has the property that $I(X;Y) = 0$, which is to say that the observation of the output y provides no information about the source if one does not know the key.

(a) (12 pts.) Find the value of the following quantities in terms of $H(X)$ and $H(K)$.

(i) $H(X|Y)$

(ii) $H(X|K)$

(iii) $H(Y|X,K)$

(ii) $H(X|Y,K)$

(v) $I(X;Y|K)$

(vi) $H(Y|K)$

(b) (7 pts.) Suppose now and for the rest of the problem, that all the source letters x have a positive probability $\Pr(X = x)$. Fix an output y_0 with positive probability, and let $\mathcal{K}(x)$ be the set of keys k for which $f(x,k) = y_0$. Show that $\mathcal{K}(x_1)$ and $\mathcal{K}(x_2)$ are disjoint when $x_1 \neq x_2$. [Hint: the decryptability condition says that from an output y and key k it is possible to uniquely determine the source letter x which produced the output y.]

(c) (5 pts.) Suppose, in addition, and for the rest of the problem, that the number of keys is the same as the number of source letters. Using part (b) show that each set $\mathcal{K}(x)$ contains a single element.

(d) (4 pts.) Let the single element of $\mathcal{K}(x)$ of part (c) be denoted by $k(x)$. Show that

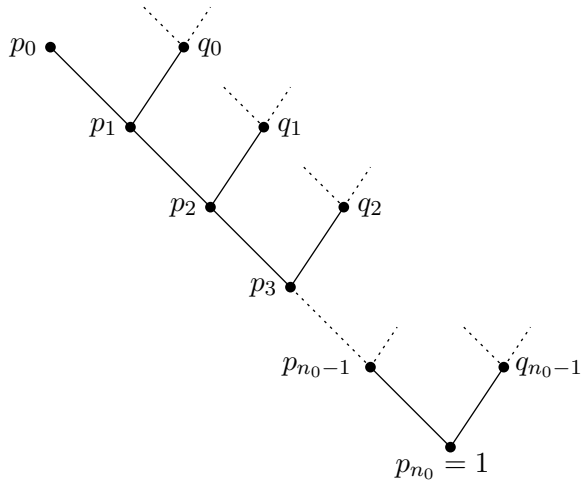
$$\Pr(Y = y_0|X = x) = \Pr[K = k(x)]$$

(e) (7 pts.) Using $I(X;Y) = 0$ conclude that for all x, $\Pr(Y = y_0|X = x) = \Pr(Y = y_0)$. Using part (d), conclude that $\Pr[K = k(x)]$ does not depend on x. Show that K is uniformly distributed.

Problem 3. (35 points.) The Fibonacci sequence F_n, $n \geq 0$ is given by $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

Let p_0 be the probability of some given letter of a source and let n_0 be the length of the codeword corresponding to that letter in a binary Huffman coding of the source.

(a) (10 pts.) Let the binary tree below represent part of the Huffman code tree, the dotted branches indicate that the tree possibly continues along those branches. The probabilities marked on each intermediate node are the sums of the probabilities of the children of the node (for example, $p_2 = p_1 + q_1$).



Show that for each $i \geq 1$, $q_i \geq p_{i-1}$. [Hint: If not, what can you do to get a better code?][Alternative Hint: Would the Huffman procedure merge q_{i-1} with p_{i-1} if q_i were less than p_{i-1}?]

(b) (7 pts.) Using part (a), show that $p_i \geq F_i p_0$ for all $i \geq 0$.

(c) (4 pts.) Conclude that the $p_0 \leq 1/F_{n_0}$.

(d) (6 pts.) Argue that the bound in part (a) can be met with equality, give an example with three source letters.

(e) (8 pts.) Show that the bound in part (b) cannot be met with equality for $i \geq 1$, but it can be approached arbitrarily closely. Conclude that the bound in part (c) cannot be met with equality, but can be approached arbitrarily closely.