Math 5251 Error-correcting codes and finite fields
Spring 2007, Vic Reiner
Midterm exam 1- Due Wednesday February 21, in class

Instructions: This is an open book, open library, open notes, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult.

1. Let Ω be the probability space of all sequences of 3 flips of an *unfair* coin that has probabilities $P(\text{heads}) = \frac{2}{3}, \quad P(\text{tails}) = \frac{1}{3}$. Let X be the random variable on Ω whose value is the number of heads which appear among the 3 flips. Let Y be the random variable whose value is the number of tails appearing among the 3 flips.
(a) (10 points) Compute the entropy $H(X)$ of the random variable X.
(b) (10 points) Compute the conditional entropy $H(X|Y)$.

2. Let W be a memoryless source with 4 source words, having probabilities

$$(p_1, p_2, p_3, p_4) = (\frac{1}{3}, \frac{1}{3}, \frac{1}{6}, \frac{1}{6},)$$

(a) (5 points) Compute the (binary) entropy $H(W)$ for this source W.
(b) (10 points) Compute two different binary Huffman codes $\mathcal{H}_1, \mathcal{H}_2$ for the source W having *different* sets of code word lengths. For example, the maximum length of a code word should be *different* for the two codes.
(c) (5 points) Compute the average codeword lengths for $\mathcal{H}_1$ and for $\mathcal{H}_2$, and explain why there is no contradiction to the fact that any Huffman code should achieve the minimal average codeword length for W.

3. Let $\Sigma = \{0, 1, 2, 3\}$ be an alphabet of size $n = 4$. For each of the following list of codeword lengths $(\ell_1, \ldots, \ell_6)$ either prove that there is no prefix (instantaneous) code $\mathcal{C}$ using the alphabet Σ with those codeword lengths, or produce such a prefix code $\mathcal{C}$ explicitly if one exists.
(a) (10 points) $(\ell_1, \ldots, \ell_6) = (1, 1, 2, 2, 2, 2)$.
(b) (10 points) $(\ell_1, \ldots, \ell_6) = (1, 1, 1, 2, 2, 2)$.

4. (a) (10 points) Let W be a memoryless source emitting two words $\{0,1\}$ with probabilities $p, 1-p$ for some p in $[0,1]$. Use calculus to show that the entropy $H(W) = H(p)$ is maximized as a function of p when $p = \frac{1}{2}$. What is the maximum value of $H(p)$?
(b) (10 points) Let n be a real number greater than 1. Use calculus to find the value of p that maximizes the function

$$f(p) := -p\log_n(p) = p\log_n(\frac{1}{p})$$

for p in $[0,1]$. What is the maximum value of $f(p)$?

5. (20 points) Prove that any binary Huffman code $\mathcal{H}$ with codewords of lengths $(\ell_1, \ldots, \ell_t)$ will always attain *equality* in McMillan's inequality, that is, it will satisfy

$$\sum_{i=1}^{t} \frac{1}{2^{\ell_i}} = 1.$$

(Some hints: (a) In a sense, this has more to do with the shape of Huffman trees than with probabilities. (b) Proof by induction on t?)