CS 337 **Quiz 1** **9/27/04**

Open book and notes.

Max points = 50 Time = 50 min Do all questions.

1. (Compression; 20 points)

   (a) (5 points) Symbols in an alphabet have the following frequencies: $\{10,\ 20,\ 21,\ 22,\ 27,\ 50,\ 60\}$. Create a Huffman tree.

   (b) (5 points) What is the structure of the Huffman tree over n symbols, $2 \leq n$, whose frequencies are powers of two: $\{2^0,\ 2^1,\ 2^2,\ \cdots\ 2^{n-1}\}$?

   (c) (10 points) Derive a formula, as a function of n, for the weighted pathlength of the tree in part(1b).

   Hint: The weighted pathlength of a tree is the sum of the weights of its non-leaf nodes. Use $(4 + 8 \cdots + 2^n) = 2^{n+1} - 4$.

2. (Error Correction; 15 points) Consider the Reed-Muller code in which the codewords are 8-bits long; see Table 2.12 on page 43 of your book.

   (a) (4 points) Is every word at Hamming distance 4 from a codeword itself a Reed-Muller codeword? Justify or give a counterexample.

   (b) (5 points) Suppose the sender sends 1 0 0 1 1 0 0 1 and the receiver receives 1 1 1 1 1 0 1 1. Can the receiver detect that the transmission is erroneous? Justify your answer. If he tries to correct the errors, which codeword will he pick?

   (c) (6 points) The receiver is told that transmission of a 8-bit codeword is either completely error-free or exactly two errors are introduced in each half, left and right (so, 4 errors are introduced). With this additional knowledge, can he detect erroneous transmissions?

3. (Cryptography; 15 points)

   (a) (5 points) Bob has to develop the public and private keys under the following constraints. Let $p = 3$, $q = 5$. What are n and $\phi(n)$? Choose an appropriate d. What is e? Use simple inspection, not Euclid's algorithm.

   (b) (4 points) Bob plans to send text to Alice whose public key is $(3, 55)$. Take each letter to be a block; suppose the letters are represented in plaintext by their numeric order: $a:\ 01$, $b:\ 02$, etc. What does Bob send for the plaintext *eda*?

   (c) (6 points) Can Bob figure out Alice's private key given that her public key is $(3, 55)$?