CS 337 **Test 1** **2/23/09**

Open book and notes.

Max points = 75 Time = 75 min Do all questions.

1. (Compression; 30 points)

   (a) (8 points) Given below is a Huffman tree over a set of symbols. Assign probabilities to the symbols. Note that the answer is not unique. Hint: it may be easier to use fractions, like 1/2 or 1/4, for probabilities.

   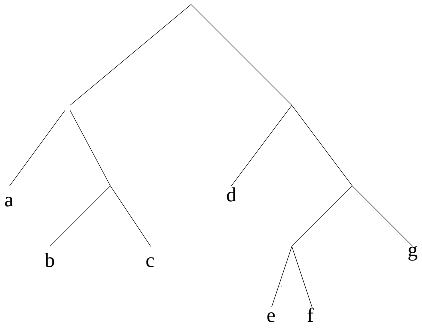

   Figure 1: Huffman Tree

   (b) (6 points) You have to transmit a string of one million symbols over the alphabet $\{a, c, g, t\}$; the transmitted string is in binary. The symbols and their probablities of occurrence are as follows: $a:\ 1/2$, $c:\ 1/4$, $g:\ 1/8$ and $t:\ 1/8$. What is the theoretical minimum length of the binary string you will have to transmit?

   (c) (10 points) A sender and receiver are using the Lempel-Ziv code. The sequence of transmissions are as follows: $(0, a)$, $(0, c)$, $(0, b)$, $(1, a)$, $(2, b)$, $(1, c)$, $(1, d)$, $(2, c)$, $(6, c)$, $(7, c)$, $(9, a)$.

      i. (6 points) Show the trie corresponding to these transmissions.

      ii. (4 points) What is the string that has been transmitted?

   (d) (6 points) Prove that all pairs in an LZ transmission are distinct. Argue rigorously, though you don't have to give a formal proof.

2. (Error Correction; 27 points)

   (a) (10 points) What is the exclusive-or of all the rows of a Hadamard Matrix, H_n, for arbitrary n, $n \geq 0$?

   (b) (6 points) Show a set of 6 codewords, each 7 bit long, so that you can detect 2 errors and correct 1 error.
   Hint: Do not try a brute-force approach, but think of a design strategy that has been discussed in class.

(c) (5 points) A consequence of the theorem on error detection/correction is that parity check code can detect at most one error, but correct none. In the RAID architecture, we are essentially using parity encoding (the extra disk keeps the check bit for each row). And, we are able to correct the failure of one disk. Is the theorem wrong? Answer in less than 4 sentences.

(d) (6 points) What string is transmitted if Hamming code is used on 101100? Show the steps.

3. (Cryptography; 18 points)

(a) (13 points) Alice sends a text message using Bob's public key (3,55). To send "abqr", for example, she first converts each letter to its position in the Roman alphabet to get four numbers: "01 02 17 18". Next, she sends the four numbers $(01)^3$ mod 55, $(02)^3$ mod 55, $(17)^3$ mod 55, $(18)^3$ mod 55, in sequence.

Suppose Alice sends "01 02" to Bob. What is her message?

Hint: You will have to do some calculations involving mod 55. Use modular simplification rule. Some long-hand multiplication and division is required.

(b) (5 points) A sender transmits a sequence of blocks using the following scheme. Encrypt the first block by doing exclusive-or of the block with a secret key, and subsequent blocks by doing exclusive-or with the previous encrypted block. Is this a good scheme?