QUIZ 5 : MATH 4161 - MARCH 18, 2010

OPEN BOOK, OPEN NOTES, CLOSED FRIENDS AND ENEMIES

No computers. Do not access the internet when you do this quiz.

(1) A candy maker manufactures 7 chocolate Easter bunnies of increasing sizes. His plan was to use 10 grams of chocolate for the first and 10 additional grams for each of the successive ones. So, at the end the bunnies should have weighed 10, 20, 30, 40, 50, 60, 70 grams respectively. However, he takes a lunch break after making the first k where $0 \leq k \leq 7$ and during that time a mischievous helper messes up his scale so at the end the remaining $7-k$ end up weighing 10 grams more than they should have. Suppose that you are to determine after which bunny he went to lunch by means of a scale with outputs $<, =$, or $>$. Say that all 8 possibilities are equally likely. We know that the maximum number of bits of information that we can get from a single weighing is $log_2(3)$ bits of information. Precisely how many bits of information is learned on average when we put the bunnies that are supposed to weigh 50 and 70 in one pan and in the other pan the ones that are supposed to weigh 40 and 60?

(2) Say that the letters A, B, C and D are generated randomly and occur with probabilities 1/16, 3/16, 5/16, 7/16 respectively.
   (a) Draw the Huffman tree which has the minimum expected code length.
   (b) For each branch of this tree, assume that if the branch is towards the letter A it is labelled with 1 and other branches labelled with 0. What word does the message 10111011111011110 correspond to?
   (c) What is the expected number of bits needed to encode a letter on average using this code?
   (d) Now encode letters two at a time. Draw the tree with the minimum expected code length using the encoding of letters two at at time.
   (e) What is the expected number of bits *per letter* needed to encode on average using this code?

(3) Say that there are 3 plaintext messages m_1, m_2 and m_3 that occur with probability 1/8, 3/4 and 1/8 respectively. Say also that there are 4 different keys k_1, k_2, k_3 and k_4 that occur with probability 1/8, 3/8, 3/8, 1/8 that encode the message with the following table, the cyphertexts c_1, c_2, c_3, and c_4 are selected by the row indexed by the key and the column indexed by the message.

	m_1	m_2	m_3
k_1	c_1	c_4	c_3
k_2	c_4	c_1	c_2
k_3	c_3	c_2	c_1
k_4	c_2	c_3	c_4

   (a) Explain why this system does or does not achieve perfect secrecy. (Note: it is not sufficient to answer 'yes' or 'no.' Show your work.)
   (b) Calculate $H(K|C)$.

(4) The following cyphertext was encrypted with the Vernam system with two keys of length 3 and 5 respectively.

MWPOG VPWDC NTMXU ROBTK ABJFG NNZLG LW

The cyphertext DCN starting at position 9 is known to be 'eat' and the letters OBTK at position 17 correspond to the word 'less.' Recover the message.