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

1. (Compression)

   (a) Huffman tree over $\{10,\ 20,\ 21,\ 22,\ 27,\ 50,\ 60\}$.

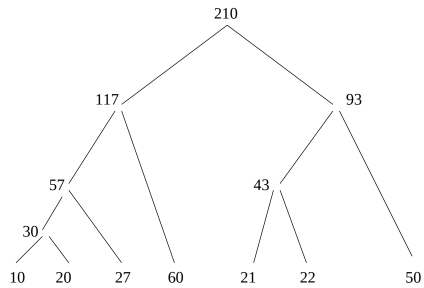

Figure 1: Huffman tree over the given frequencies

   (b) Structure of the Huffman tree over n symbols, $2 \le n$, whose frequencies are powers of two: $\{2^0,\ 2^1,\ 2^2,\ \cdots\ 2^{n-1}\}$:

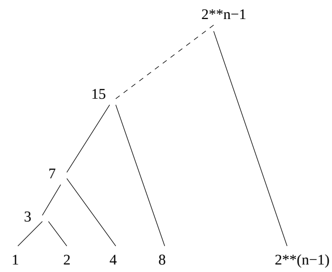

Figure 2: Huffman tree over $\{2^0,\ 2^1,\ 2^2,\ \cdots\ 2^{n-1}\}$

   (c) From the hint and the figure in part (b), we have to compute

$$
\begin{array}{ll}
 & 3 + 7 + \cdots + (2^n - 1) \\
= & \{\text{add 1 to each term and subtract } n-1\text{, the number of 1's added.}\} \\
 & [4 + 8 \cdots + 2^n] - (n-1) \\
= & \{\text{add the terms within brackets; use hint}\} \\
 & 2^{n+1} - 4 - (n-1) \\
= & \{\text{simplify}\} \\
 & 2^{n+1} - (n+3)
\end{array}
$$

2. (Error Correction)

   (a) Every word at distance 4 from a codeword is not itself a codeword. 1 1 1 1 1 1 1 1 is a codeword (top row of Table 2.12). But 0 0 0 0 1 1 1 1 is not.

(b) (5 points) If the sender sends 1 0 0 1 1 0 0 1 and the receiver receives 1 1 1 1 1 0 1 1, the Hamming distance between the two words is 3. Since the distance among codewords is exactly 4, the received message is not a codeword; so the receiver can detect the error.

He will pick the closest codeword to 1 1 1 1 1 0 1 1 which is 1 1 1 1 1 1 1 1.

(c) No. Suppose 1 1 1 1 1 1 1 1 is sent and it is corrupted to 1 0 1 0 1 0 1 0; there is exactly two errors in each half, left and right. The received word is also a codeword. So the receiver cant tell if 1 0 1 0 1 0 1 0 was sent and received perfectly, or 1 1 1 1 1 1 1 1 was sent and received erroneously.

3. (Cryptography)

(a) Given $p = 3$ and $q = 5$, $n = 15$ and $\phi(n) = 8$? Choose d to be a prime exceeding p and q; say, 7. Then, $7 \times e \overset{\text{mod } 8}{\equiv} 1$. By simple inspection, $e = 7$.

(b) We have to encrypt *eda* which is 05 04 01. We compute

$$5^3 \bmod 55 = 15,\ 4^3 \bmod 55 = 9,\ 1^3 \bmod 55 = 1$$

So, the ciphertext is 15 09 01.

(c) Bob can easily factor 55 to get $p = 5$ and $q = 11$. So, he computes $\phi(n)$ to be $4 \times 10 = 40$. He knows

$$d \times e \overset{\text{mod } \phi(n)}{\equiv} 1, \text{ i.e.,}$$
$$d \times 3 = 40 \times k + 1, \text{ for some } k$$

He looks for the smallest number of the form $40 \times k + 1$ which is divisible by 3. This is 81. So, $d \times 3 = 81$, or $d = 27$.