2.993: Principles of Internet Computing
Homework #9
Due: 5/6/99

1. *Hamming Bound* Let C be a given (n,k) binary codeword, i.e. n coded bits for every k data bits.
   a) Argue that M (defined below) is the total number of codewords (including C) that are at most t Hamming distance away from C. Hence conclude that a t-error correcting (n,k) binary code C must satisfy the following inequality:

$$2^{n-k} \geq M = \sum_{j=0}^{t} \binom{n}{j} \qquad \text{where } \binom{n}{j} = \frac{n!}{(n-j)!\,j!} \,.$$

   The term $\binom{n}{j}$, also known as "n choose j", is simply the number of ways of choosing k from n objects without order. For example, 4 letters A, B, C and D can be chosen $6 = \binom{4}{2} = \frac{4!}{2!2!}$ different ways: AB, AC, AD, BC, BD and CD.

   b) Compute the minimum required codelength n for k =1 to 12, t = 1.

   c) When equality holds for any (n,k) code using the Hamming bound, it is said to be *perfect*. Among the codes in b), which are perfect?

2. *Hamming Code* A binary, single-error correcting, perfect code is known as a Hamming code. A classic Hamming code is the (7,4) code. This code can correct any single bit error among 7 coded bits.

   a) Obtain the original data bits from the following stream of coded bits by decoding 7 bits at a time.
   1001011 0100011 0010011 1110101

   b) The (7,4) code can either detect 2 errors or correct a single error. Give an example of a block of 7 coded bits with 2 errors, that leads to a decoding error; i.e. by error correction, a 4-bit pattern is decoded incorrectly as another 4-bit pattern.