# Crypto HW #7 -- Error Detecting and Error Correcting Codes

1) Please show that the ISBN code is not a linear code.

2) Please find a binary (n, M, d)=(n, 2, n)-code which is not equivalent to the repetition code of length n.

3) What is the minimal Hamming distance of the ternary code C = {(1, 0, 2, 1, 1), (0, 0, 2, 0, 1), (2, 1, 0, 0, 2), (1, 2, 0, 1, 2)}? How many errors can it detect and how many errors can it correct? What is its code rate?

4) Please compute the (n, M, d) and [n, k, d] invariants for the linear 3-ary code generated by the vectors:
   v1 = (1, 1, 2, 2, 0, 0, 1)
   v2 = (2, 2, 1, 1, 0, 0, 2)
   v3 = (1, 2, 0, 1, 2, 0, 1)
   v4 = (1, 0, 1, 0, 1, 0, 1)

5) What is the systematic generating matrix and associated parity check matrix for this code? What is the syndrome of the received messages r1 = (0, 2, 2, 1, 1, 0, 0) and r2 = (2, 1, 0, 2, 1, 0, 2), and what does this tell us about the original codeword that was sent?

6) What is the systematic generating matrix for the (linear) 2-dimensional binary parity code with n=2 and m=3?

7) Can we find an binary (n, M, d)-code for each of the following values? If not, please explain why not. If so, please exhibit the code.
   (n, M, d) = (2, 2, 2)
   (n, M, d) = (3, 3, 3)
   (n, M, d) = (10, 64, 6)
   (n, M, d) = (7, 7, 2)