Coding Theory **Jan, 2011**

Assignment 1

1. Write down the parity check matrix and the trellis for the $(3, 1, 3)$ repetition code. Suppose at the receiver, you receive the signal sequence y_1, y_2, y_3 where y_i is a real number (voltage received). Let us assume that the transmitted sequence to be estimated is x_1, x_2, x_3, where $x_i \in \{0, 1\}$. You are given that probability information $Pr(y_1|x_1 = 0) = 1/8$, $Pr(y_1|x_1 = 1) = 1/4$, $Pr(y_2|x_2 = 0) = 1/4$, $Pr(y_2|x_2 = 1) = 1/2$, $Pr(y_3|x_3 = 0) = 1/2$, $Pr(y_3|x_3 = 1) = 1/8$, What will be the codeword found out by the Viterbi algorithm on the trellis you have written? □

2. Consider the code over F_2^n consisting of all all words of even Hamming weight. Is the code linear? What is the rate and minimum distance of the code? Write down a generator matrix and parity check matrix for the code for $n = 2, 3, 4, 5$. Can you genralize the form of the generator and parity check matrices? □

3. Suppose we used the alphabet $F_3 = \{0, 1, 2\}$ instead of binary for messages and codewords, how will you modify the basic (non-asymptotic) versions of singleton bound and Plotkin bound? (Define the Hamming weight of a word in this case as the number of non-zero entries in the word and it is easy to show that this still defines a norm in F_3^n. Note that F_3 is a field with addition and multiplication $\mod 3$ and hence F_3^n is a vector space. Thus the basic theory of linear code goes through as with the binary case). □

4. Let $\mathcal{C}$ be an (n, k, d) linear code with $d > 1$. Suppose for some $1 \leq i \leq n$, we delete the ith cordinate from each codeword in $\mathcal{C}$. Let the resultant code $\mathcal{C}'$ be an $(n-1, k', d')$ code. ($\mathcal{C}'$ is said to be obtained by *punchuring* $\mathcal{C}$ at the i^{th} position). □

    1. Show that $k' = k$.
    2. Show that $d' \geq d - 1$.

5. Suppose $\mathcal{C}$ be an (n, k, d) linear and $\mathcal{C}'$ be an (n', k', d') linear codes. Consider the code $\mathcal{C}'' = \{(c_1, c_2) : c_1 \in \mathcal{C}, c_2 \in \mathcal{C}'\}$ (This is the code formed by concatinating codewords in all possible combinations with first codeword from $\mathcal{C}$ and second codeword from $\mathcal{C}'$. Show that $\mathcal{C}''$ is an $(n + n', k + k', d")$ code where $d'' = \min\{d, d'\}$. Suppose G, G' are generator matrices and H, H' parity check matrices for $\mathcal{C}, \mathcal{C}'$ repsectively, what will be (the general form of) the generator matrix and parity check matrix of $\mathcal{C}''$? □

6. Suppose $\mathcal{C}$ be an (n, k, d) linear and $\mathcal{C}'$ be an (n, k', d') linear codes. Consider the code $\mathcal{C}'' = \{(c_1, c_1 + c_2) : c_1 \in \mathcal{C}, c_2 \in \mathcal{C}'\}$ Show that $\mathcal{C}''$ is an $(2n, k + k', \min\{2d, d'\})$ code. Suppose G, G' are generator matrices and H, H' parity check matrices for $\mathcal{C}, \mathcal{C}'$ repsectively, what will be (the general form of) the generator matrix and parity check matrix of $\mathcal{C}''$? Let us call $\mathcal{C}''$ be the *semi-sum* of $\mathcal{C}$ and $\mathcal{C}'$. □

7. In this question we shall study the *Reed Muller Codes*. for any $m > 0$, define the code $\mathcal{R}(0, m)$ to be the $(2^m, 1)$ repetition code (i.e., each message symbol is repeated 2^m times) and the code $\mathcal{R}(m, m)$ is the whole space F_2^m. For $0 < r < m$, we define $\mathcal{R}(r, m)$ as the *semi-sum* (see previous question) of $\mathcal{R}(r, m - 1)$ and $\mathcal{R}(r - 1, m - 1)$. Show the following (use induction): □

    1. $\mathcal{R}(i, m - 1) \subseteq \mathcal{R}(j, m - 1)$ for $0 \leq i \leq j \leq m$.
    2. The dimension of $\mathcal{R}(r, m) = C(m, 0) + C(m, 1) + \cdots + C(m, r)$, Where $C(n, i) = \frac{n!}{i!(n-i)!}$ for $0 \leq i \leq n$.
    3. $\mathcal{R}(r, m)$ has minimum distance at least 2^{m-r}.

    $\mathcal{R}(r, m)$ is called the (r, m) Reed-Muller Code.