Homework Problem Sets
ENEE 722 Error Correcting Codes

Problem Set 1

1. Consider the following code:

Information Sequences	Code Words
0 0	0 0 0 0 0
0 1	0 1 1 0 1
1 0	1 0 1 1 1
1 1	1 1 0 1 0

   (a) Show that this is a systematic linear code and find the generator matrix and a parity check matrix.

   (b) Find the decoding table for maximum likelihood decoding with a BSC with $\epsilon < 1/2$.

   (c) Find the probability of a block decoding error when the maximum likelihood decoding table is used.

   (d) Compare this code with the Hamming and VGS bounds for (5,2) codes.

2. Code I is generated by the rule:
   $x_1 = u_1$, $x_2 = u_2$, $x_3 = u_3$, $x_4 = u_1+u_2$, $x_5 = u_1+u_3$, $x_6 = u_2+u_3$, and $x_7 = u_1+u_2+u_3$.
   Code II is the same except $x_6 = u_2$.

   (a) Find the generator and check matrices for both codes.

   (b) Find the decoding tables for both codes for a BSC with $\epsilon < 1/2$.

   (c) Calculate the probability of block decoding error for both codes.

   (d) Find $d_{\min}$ for both codes and give a counterexample to the conjecture that if one (N, K) code has a larger $d_{\min}$ than another (N, K) code, it has a smaller P_e on a BSC.

3. Find G and H for the repetition code of length N. Find $d_{\min}$ using arguments regarding H.

4. (a) Does a (10,7) linear code that corrects all single and double error patterns exist?

   (b) Find the Hamming bound of the guaranteed error correction capability, t, for (4,1) linear codes over GF(2) and GF(5).

   (c) Find the VGS bounds on $d_{\min}$ for (4,1) linear codes over GF(2) and GF(5).

5. A (4,2) code over GF(3) is generated by the following rules:

$$x_1 = u_1, \quad x_2 = u_2, \quad x_3 = u_1 + u_2, \quad x_4 = 2u_1 + u_2$$

(a) Find G and H.

(b) Assume the symbols are transmitted over a memoryless channel for which the probability of a correct transition is $1 - \epsilon$ and of an incorrect transition is $\epsilon/2$. Find the syndrome decoding table and P_e. Is the code perfect?

Problem Set 2

1. For the following binary convolutional code with $R = 1/2$, $N_0 = 2$, $m = 2$, and input/output equations

$$\begin{aligned} x_i^{(1)} &= u_i^{(1)} \\ x_i^{(2)} &= u_i^{(1)} + u_{i-1}^{(1)} + u_{i-2}^{(1)} \end{aligned}$$

   (a) Find $G_{(k)}^{(j)}(D)$ for $k = 1$ and $j = 1$ and 2.

   (b) Find the matrices $\mathbf{G}_0$, $\mathbf{G}_1$, and $\mathbf{G}_2$ and the $RN_A \times N_A$ matrix $\mathbf{G}$.

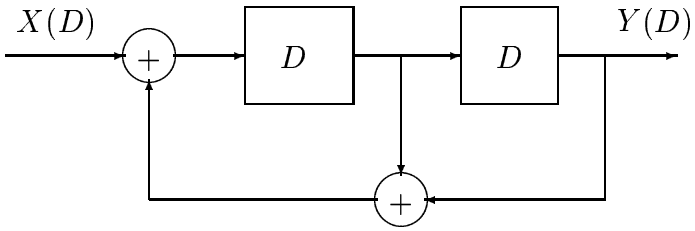
   (c) Sketch block diagrams of the type I and II encoders.

   (d) Find $d_{\min}$.

   (e) Find w_{avg} by using the formula derived in the notes and by direct calculation from a list of the code words.

   (f) Repeat the problem for $x_i^{(2)} = u_i^{(1)} + u_{i-2}^{(1)}$

2. Find the transfer function $H(D) = Y(D)/X(D)$ for the binary circuit shown in the following figure.



3. Sketch block diagrams for the type I and II realizations of the transfer function

$$H(D) = \frac{1 + D^2}{1 + D + D^2 + D^3}$$

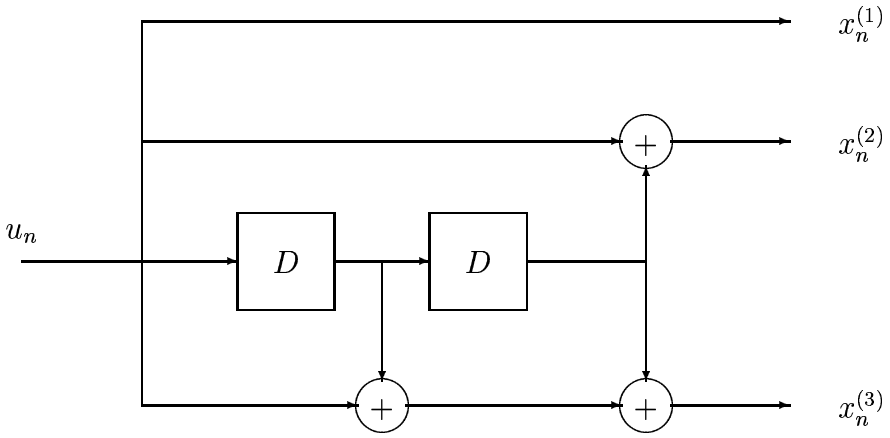
Problem Set 3

1. Show that $\{0, 3, 4, 9, 11\}$ is a perfect difference set with modulus 21. Sketch the encoder for the $N_0 = 2$, $R = 1/2$ self orthogonal convolutional code corresponding to this difference set. Sketch the definite and feedback decoders. What is the guaranteed error correction capability in both decoding modes? Does the feedback decoder have unlimited error propagation?

2. Verify that the sets of integers $\{0, 3, 15, 19\}$, $\{0, 8, 17, 18\}$, $\{0, 6, 11, 13\}$ can be used to construct $R = 1/4$ or $3/4$, $N_0 = 4$ self orthogonal convolutional codes. Find $d_{\min}$ for both codes. Sketch block diagrams for encoder, and definite and feedback decoders.

3. Find the APP decoder for the code of problem 1. Assume the symbols are transmitted over a BSC.

Problem Set 4
Viterbi Decoding Problem Set



1. (a) Draw the code tree, trellis, and state transition diagrams for the $K_0 = 1$, $N_0 = 3$, $m = 2$ convolutional encoder shown in the figure above.

   (b) Find the minimum free distance.

   (c) Find $T(D)$ and the number of paths of each weight.

   (d) The sequence 111 001 111 000 001 000 000 000 is received. Each triplet corresponds to $y_n^{(1)}, y_n^{(2)}, y_n^{(3)}$. Use the Viterbi algorithm to decode this sequence assuming a BSC. Show the survivors to each node on a trellis diagram. Label the survivor's Hamming distance cumulative metric at each node.

2. A (2,1) non-systematic binary convolutional code is described by

$$\begin{aligned} x_n^{(1)} &= u_n + u_{n-1} + u_{n-2} \\ x_n^{(2)} &= u_n + u_{n-2} \end{aligned}$$

   (a) Find the transfer function matrix $\hat{\mathbf{G}}(D)$ for the equivalent systematic code with feedback. Sketch the block diagram of a type II encoder.

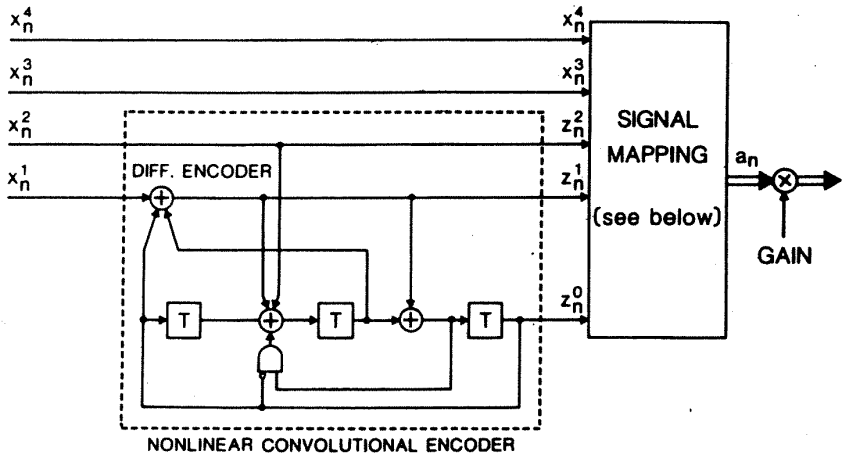
   (b) Draw the trellis and state transition diagrams for the systematic encoder.

   (c) Find $T(D)$, d_f, and the number of paths that start at and re-merge with the zero state and have weight n for $n = 0, 1, \ldots, 9$.

   (d) Generate a code word several blocks long. Introduce a single error and use the Viterbi algorithm to correct the error.

Problem Set 5

From: G. Ungerboeck, *Communications Magazine*, Vol. 25, No. 2, February 1987.



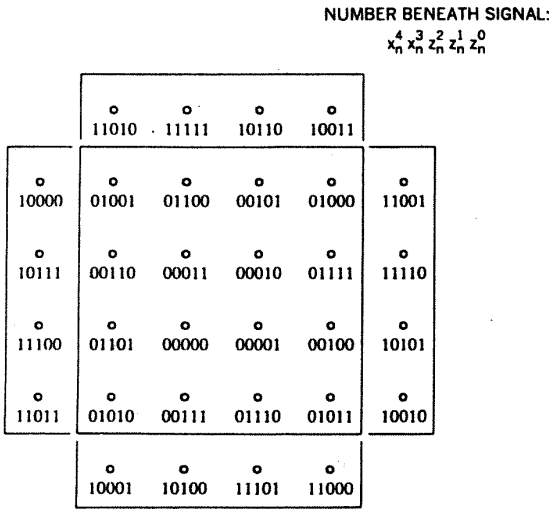


Fig. 7. Alternative nonlinear 8-state encoder/modulator with integrated differential encoding and general signal mapping for 16-QASK, 32-CROSS, etc., signal sets.

1. Make an encoder state transition and output table showing $s_{n+1}^{(2)}, s_{n+1}^{(1)}, s_{n+1}^{(0)}, z_n^{(1)}, z_n^{(0)}$ in terms of $x_n^{(2)}, x_n^{(1)}, s_n^{(2)}, s_n^{(1)}, s_n^{(0)}$.

2. Prove that the encoder outputs satisfy the parity check equation

$$z_n^{(0)} + z_{n-3}^{(0)} + z_{n-1}^{(1)} + z_{n-2}^{(1)} + z_{n-2}^{(2)} = \overline{z_{n-2}^{(0)}} \cdot z_{n-1}^{(0)}$$

where $\cdot$ designates the logical "and" function.

3. Notice that any constellation point with label

$$(x_n^{(4)}, x_n^{(3)}, z_n^{(2)}, z_n^{(1)}, z_n^{(0)})$$

when rotated 90 degrees counterclockwise becomes

$$(x_n^{(4)}, x_n^{(3)}, z_n^{(2)}, z_n^{(1)} + z_n^{(0)}, \overline{z_n^{(0)}})$$

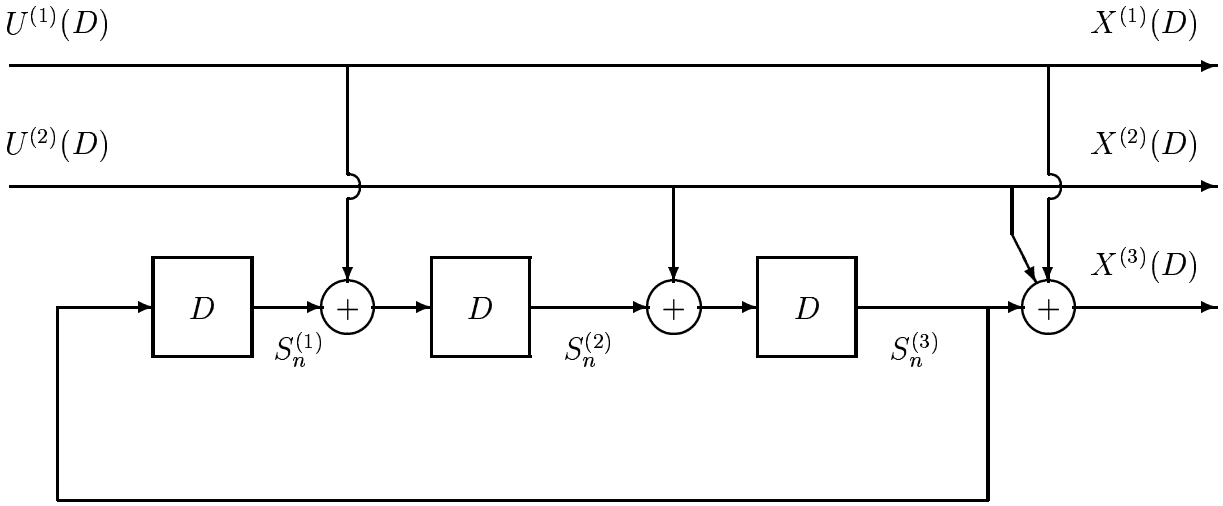
Also, when considered as two bit integers, $(z_n^{(1)}, z_n^{(0)}) + (0,1) = (z_n^{(1)} + z_n^{(0)}, \overline{z_n^{(0)}})$ mod 4. Prove that any sequence of code constellation points when rotated 90 degrees still satisfies the parity check equation of 2.

4. Show that

$$x_n^{(1)} = z_n^{(0)} + z_n^{(1)} + s_n^{(1)} = z_n^{(0)} + z_n^{(1)} + z_{n-2}^{(0)} + z_{n-1}^{(1)} + z_{n-1}^{(2)} + \left(\overline{z_{n-1}^{(0)}} \cdot z_n^{(0)}\right)$$

Prove that $x_n^{(1)}$ does not change when the trellis constellation sequence is rotated 90 degrees.

Problem Set 6
Convolutional Encoder and Viterbi Decoder Project



1. Construct a state transition table for this encoder with nine columns consisting of:

$$u_n^{(1)} \quad u_n^{(2)} \qquad s_n^{(1)} \quad s_n^{(2)} \quad s_n^{(3)} \qquad s_{n+1}^{(1)} \quad s_{n+1}^{(2)} \quad s_{n+1}^{(3)} \quad x_n^{(3)}$$

   This table can be used to implement the encoder.

2. Find d_f and the transfer function matrix $\mathbf{G}(D)$ for this code.

3. Let $S_n = 4s_n^{(1)} + 2s_n^{(2)} + s_n^{(3)}$ and $X_n = 4x_n^{(1)} + 2x_n^{(2)} + x_n^{(3)}$. Construct a table that can be used in a Viterbi decoder showing for each state $S_{n+1} \in \{0, 1, \ldots, 7\}$, the four previous states S_n with branches converging on S_{n+1} and the corresponding branch code bits represented as X_n. The table should have three columns with headings S_{n+1}, S_n, and X_n.

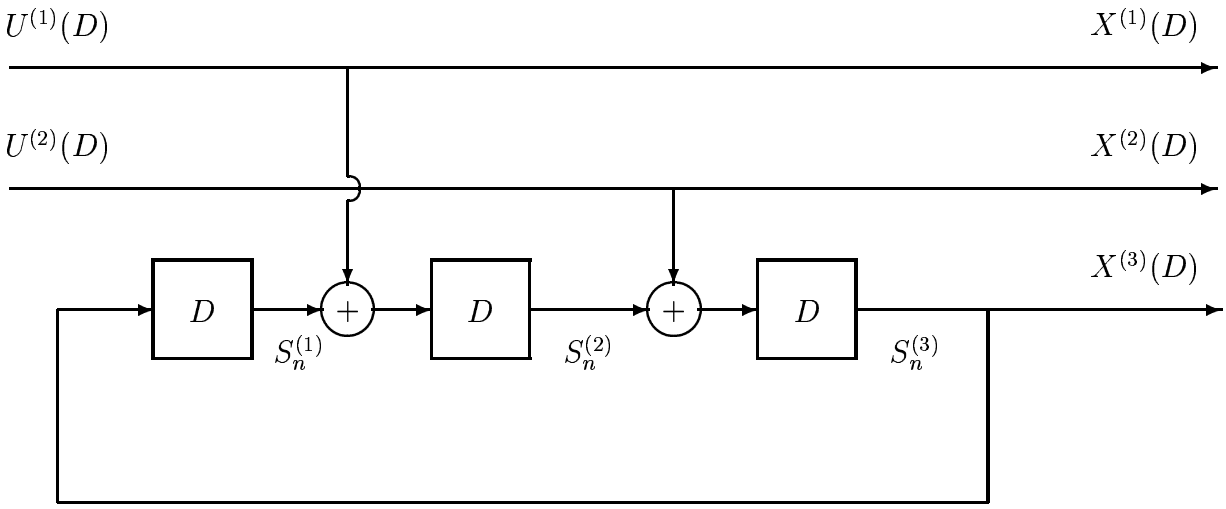
4. The encoder was started in the 0 state, 1050 code branches were generated with a pseudo-random input sequence, and files for several error rates were generated. The files have names of the form `receive`xx`.dat` where xx is a two digit integer. Higher values of xx correspond to fewer errors. The resulting files can be found in my web site at `http://www.ee.umd.edu/~tretter` under the heading "ENEE 722 Error Correcting Codes." Each line of a file contains the three entries: $y_n^{(1)} \quad y_n^{(2)} \quad y_n^{(3)}$. Write a program to decode the received sequences using the Viterbi algorithm. Use a trellis storage depth of 32 branches. You can use your favorite programming language like C, MATLAB, FORTRAN, BASIC, etc.

5. For each file, arrange your decoded branches to form the serial bit stream:

$$\{z(0), z(1), z(2), z(3), \ldots\} = \{x_0^{(2)}, x_0^{(1)}, \quad x_1^{(2)}, x_1^{(1)}, \ldots, x_k^{(2)}, x_k^{(1)}, \ldots\}$$

   Form the new sequence $v(n) = z(n) + z(n-18) + z(n-23)$ for $n \geq 23$ where $+$ represents modulo 2 addition. How many 0's are in this new sequence for each file?

Problem Set 7
Trellis Coded Modulation (TCM) Project



The output of this convolutional encoder is attached to an 8-PSK modulator like in Ungerboeck's papers. Let $p_n = 4x_n^{(1)} + 2x_n^{(2)} + x_n^{(3)}$. Then the selected phase is

$$\theta_n = \frac{\pi}{4} p_n - \frac{\pi}{8}$$

These symbols are transmitted over an additive white Gaussian noise channel. The file `RC20DB.DAT` contains 1050 received symbols with a signal-to-noise ratio of 20 dB, the file `RC12DB.DAT` contains 1050 received symbols with a signal-to-noise ratio of 12 dB, the file `RC9DB.DAT` contains 1050 received symbols with an SNR of 9 dB, and the file `RC7DB.DAT` contains 1050 symbols with an SNR of 7 dB. Each line of these files consists of the x and y coordinates of the received noisy constellation point. The files can be found at `http://www.ee.umd.edu/~tretter`.

1. Make separate plots of the constellation points in the received data files.

2. Construct a state transition table for this 8-state encoder with nine columns consisting of:

   $$u_n^{(1)} \quad u_n^{(2)} \qquad s_n^{(1)} \quad s_n^{(2)} \quad s_n^{(3)} \qquad s_{n+1}^{(1)} \quad s_{n+1}^{(2)} \quad s_{n+1}^{(3)} \quad p_n$$

   This table can be used to implement the encoder.

3. Find the minimum squared free Euclidean distance d_f^2. Give a trellis path with this distance from the all 0 path. Compute the coding gain in dB relative to uncoded 4-PSK.

4. Let $S_n = 4s_n^{(1)} + 2s_n^{(2)} + s_n^{(3)}$. Construct a table showing for each state $S_n \in \{0, 1, \ldots, 7\}$, the four previous states S_{n-1} with branches converging on S_n and the corresponding branch symbols represented as p_n. The table should have 9 rows and 9 columns. The

first column should start with a blank followed by the integers 0, 1, ..., 7 going down the page. These are the current possible states S_n. The top row should start with a blank entry followed by 0 2 4 6 1 3 5 7 which are the previous possible states S_{n-1}. Enter the transmitted phase index, p_n, in the appropriate row and column for each allowable transition. Leave impossible transitions blank.

5. Assume the encoder was started in the 0 state, Write a program to decode the received sequence using the Viterbi algorithm with the squared Euclidean distance metric. Use a trellis storage depth of 32 branches. Decode the first 1000 branches of the received data files.

6. Arrange your decoded branches to form the serial bit stream:

$$\{z(0), z(1), z(2), z(3), \ldots\} = \{x_0^{(2)}, x_0^{(1)}, \quad x_1^{(2)}, x_1^{(1)}, \ldots, x_k^{(2)}, x_k^{(1)}, \ldots\}$$

   Form the new sequence $v(n) = z(n) + z(n-18) + z(n-23)$ for $n \geq 23$ where $+$ represents modulo 2 addition. How many 0's are in this new sequence? This item should be done for each of the received data files.

Problem Set 8

1. Let $1, a, a^2, \ldots, a^5$ be the elements of a cyclic group of order 6. Find the order of each element in the group and list all subgroups.

2. (a) Write out addition and multiplication tables for the field of integers $0, 1, \ldots, 4$ using addition and multiplication modulo 5.

   (b) For any prime number p and any integer a not divisible by p, prove that $a^{p-1} \equiv 1 \mod p$.

3. Consider the field of polynomials of degree 1 or less over GF(3) with multiplication defined as polynomial multiplication modulo $D^2 + 1$.

   (a) Prove that $D^2 + 1$ is irreducible over GF(3).

   (b) Find the addition and multiplication tables for this field.

Problem Set 9

1. Let $g(D) = D^3 + D + 1$ be the generator polynomial for a cyclic code over GF(2).
   (a) Find N, K, and $h(D)$.
   (b) Sketch the type A and B encoders.
   (c) List all possible codewords and check to see if a shift of any codeword is also a codeword.
   (d) Find a parity check matrix and determine $d_{\min}$ from the parity check matrix.
   (e) What well know type of code is this – Hamming, maximal-length, etc.?
2. Let $h(D) = D^3 + D^2 + 1$ be the check polynomial for a cyclic code over GF(2).
   (a) Is $h(D)$ primitive?
   (b) Sketch the block diagram of an encoder based on $h(D)$.
   (c) List all possible codewords.
   (d) How many codewords are there of each weight? What is $d_{\min}$?
   (e) What well know type of code is this – Hamming, maximal-length, etc.?

Problem Set 10

1. $f(D) = D^4 + D^3 + D^2 + D + 1$ is irreducible over GF(2). Let α be a root of $f(D)$.

   (a) Construct a table showing the representations of α^i for $i = 0, \ldots, 15$ as binary 4-tuples. Is $f(D)$ a primitive polynomial over GF(2)?

   (b) Calculate the minimal polynomials over GF(2) for $\alpha, \alpha^2, \alpha^3, \alpha^4$, and α^5.

2. The generator polynomial for a cyclic code over GF(2) is

$$g(D) = D^4 + D^3 + D^2 + D + 1$$

   (a) Find N, K, and $h(D)$.

   (b) Give generator and check matrices.

   (c) List all codewords and find $d_{\min}$.

   (d) Sketch type A and B encoders.

   (e) Sketch the block diagram for a decoder.

3. $f(D) = D^4 + D^3 + 1$ is irreducible over GF(2).

   (a) Find the representations as binary 4-tuples for $1, D, D^2, \ldots$ in GF(2^4), the field of polynomials modulo $f(D)$.

   (b) Find the minimal polynomials over GF(2) for each element in GF(2^4).

   (c) Is $f(D)$ primitive?

4. Let α be a root of $f(D) = D^4 + D^3 + 1$ in GF(2^4) and let $\beta = \alpha^5$.

   (a) Find the order of β.

   (b) Show that $\{0, 1, \beta, \beta^2\}$ form GF(2^2).

   (c) Find the minimal polynomial, $m(D)$, for α over GF(2^2).

   (d) Make a table showing the representations for α^i for $i = 0, 1, \ldots, 14$ in the form $c_0 + c_1\alpha$ where c_0 and c_1 are elements of GF(2^2).

Problem Set 11

The generator polynomial for a binary (63,57) Hamming code is $g(D) = D^6 + D + 1$. The class web site has three files (`word1.dat`, `word2.dat`, and `word3.dat`) containing received words with at most one error. Each line of a file consists of two numbers. The first is the bit location in the word and the second is the received bit value. Write a program to implement a decoder. Find the error location in each word, if any, and the transmitted codeword.

Problem Set 12

1. Let $f(D) = 1 + D + D^3$.

   (a) Prove $f(D)$ is irreducible over GF(2).

   (b) Make a table showing the 3-tuple representations of D^i mod $f(D)$ for $i = 0, \ldots, 7$.

   (c) Is $f(D)$ a primitive polynomial?

   (d) Factor $D^7 + 1$ into the product of irreducible polynomials over GF(2).

2. Let $g(D) = f(D)$ be the generator polynomial for a cyclic code over GF(2).

   (a) How many check and information symbols do the codewords have?

   (b) A received sequence is $y(D) = x(D) + e(D) = 1 + D + D^2 + D^3 + D^5 + D^6$.

      i. Find the syndrome $s(D) = y(D)$ mod $g(D)$.

      ii. Assume $e(D)$ is a single error. Find $e(D)$ and the transmitted codeword $x(D)$. (You can use the table for GF(2^3) generated in item 1(b).)

3. Let $h(D) = f(D)$ be the check polynomial for a cyclic code over GF(2).

   (a) Find the generator polynomial $g(D)$ for this code.

   (b) What are N and K for this code?

   (c) List all codewords as 7-dimensional row vectors.

   (d) What are the weights of the codewords and what is d_{min}?

   (e) Use the formulas for maximal-length codes to compute the number of runs of 1's and 0's of each possible length and check that this is true for your codewords.

   (f) Compute the cyclic autocorrelation function for a repeated non-zero codeword and also by the theoretical formula.

Problem Set 13

1. Let α be a root of $f(D) = D^4 + D + 1$, $m_0 = 1$, and $d = 7$.

   (a) Find N, K, $g(D)$, and $h(D)$ for the binary BCH code with these parameters.

   (b) Find H using the roots of $g(D)$.

   (c) Sketch type A and B encoders.

   (d) Repeat this problem for the BCH code over GF(2^4), that is, the Reed Solomon code over GF(2^4).

2. Two codewords from the binary code above are transmitted over a BSC. The received words are

$$\vec{Y_1} = (y_0, \ldots, y_{14}) = (111000100000101)$$

$$\vec{Y_2} = (011011000010010)$$

   Assuming that correctable errors have occurred, find the transmitted words.

3. Let $f(D) = D^3 + D + 1$ and $\alpha \in$ GF(2^3) be a root of $f(D)$.

   (a) Find $g(D)$ for the Reed-Solomon code over GF(2^3) with $m_0 = 1$, $d = 5$, and powers of root α.

   (b) A received word is $y(D) = \alpha^3 + \alpha D + D^2 + \alpha^3 D^3 + D^4 + \alpha^5 D^5$. Assume a correctable error occurred. Find $\sigma(D)$, $A(D)$, the error locators, the error values, and the transmitted codeword.

   (c) Repeat the previous item if $y(D) = \alpha^3 + \alpha D + D^2 + \alpha^3 D^3 + D^4 + \alpha^5 D^5 + \alpha^3 D^6$.

4. (a) Show that the all one's vector is always a codeword in BCH codes with $1 \leq m_0 < m_0 + d - 2 \leq N - 1$

   (b) Prove that the complement of any codeword is also a codeword in these codes for the binary case.

   (c) For these binary codes, find a relationship between the number of codewords of weight ℓ and the number of codewords of weight $N - \ell$.