E2 205 Error-Control Coding
Homework 3

Discussion: 2:00 PM, October 04, 2019

1. It is desired to construct a $[6,4]$ linear, binary block code having as large a minimum distance d as possible. Which of the two bounds, the Hamming bound or the Singleton bound, imposes the tighter restriction on d , i..e, which of the two bounds yields a smaller upper-bound on d ?

2. Show that the repetition code and the parity-check code are the only possible binary MDS codes of length $n = 7$. (Hint: Start by attempting to construct an $[n,k]$ MDS code by attempting to build up a parity-check matrix H for the code, one column at a time. Keep in mind that the parity-check matrix has $n-k$ rows and it is required that any $n-k$ columns of H be linearly independent.) **Note:** The same proof carries over to any length n. However, you are only required to do the case $n = 7$.

3. Use the Hamming, Gilbert-Varshamov and Plotkin bounds to determine the best upper and lower bounds on the maximum size of a binary block code of length $n = 15$ and minimum distance $d_{min} = 7$.

4. Show that the dual of an $[n,k]$ MDS code $\mathscr{C}$ is also an MDS code.

5. Derive the analogue of the Hamming bound as it applied to ternary codes, i.e., to codes having the ternary alphabet $\{0,1,2\}$.

6. In the fractional minimum distance δ vs rate $R(\delta)$ plot for binary codes, at what value of δ does the Hamming bound and the Plotkin bound crossover? Is there a value of δ for which either the Hamming or the Plotkin bound is better than the Elias bound?

7. Show that the dual of $[7,4,3]$ Hamming code is optimal with respect to Plotkin bound.

8. Consider standard-array decoding of the binary, linear $[4,2]$ code having parity-check matrix

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

   (a) How many single-error patterns can this code reliably correct ?

   (b) If the error pattern introduced by the channel is $[1\ 0\ 1\ 0]$, what is the residual error, i.e,, if $\underline{c}$, $\hat{\underline{c}}$ are the true and decoded codewords respectively, what is $\underline{c} + \hat{\underline{c}}$?

9. Consider the linear block code of length 5 and dimension 2 with the following generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

   (a) Choose as coset leaders the zero vector, all 5-tuples with weight 1 and $\{00011,\ 10001\}$. Construct the standard array together with syndromes for complete decoding. (The first row in this table should list the codewords and the first column to the left should contain all the coset leaders. The last column should list the corresponding syndromes.)

(b) Given that the received vector

$$\underline{r} = [1\ 1\ 1\ 0\ 1]^t,$$

what is the decoded codeword ? How many message bits are in error ? You may assume that the transmitted codeword is the all-zero codeword.

Repeat for the case

$$\underline{r} = [1\ 1\ 0\ 0\ 0]^t.$$

Again, you may assume that the transmitted codeword is the all-zero codeword.

(c) When the code is used only for the purposes for correcting error, what is the probability P_{we} of codeword error when the crossover probability of the BSC is $\varepsilon = 10^{-4}$?

10. Consider the standard array table of the $[5,3]$ linear block code having generator and parity-check matrices given by

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Messages are encoded via the encoding equation

$$[c_o, c_1, c_2, c_3, c_4]^t = [m_0, m_1, m_2]^t G.$$

The corresponding standard array table is provided below:

								syndrome
00000	10100	01010	10001	11110	00101	11011	01111	$[0\ \ 0]^T$
11000	01100	10010	01001	00110	11101	00011	10111	$[0\ \ 1]^T$
10000	00100	11010	00001	01110	10101	01011	11111	$[1\ \ 0]^T$
01000	11100	00010	11001	10110	01101	10011	00111	$[1\ \ 1]^T$

You may assume that transmission is across a binary symmetric channel (BSC) having crossover probability $\varepsilon < \frac{1}{2}$.

(a) What is the probability of undetected error P_{ue} of this code ?

(b) What is the probability that the sum $\sigma = m_0 + m_1 + m_2$ of the message bits will be decoded incorrectly ?

11. Prove that if $\mathscr{C}$ is an $[n,k,d]$ linear block code, and standard array decoding (syndrome decoding) is employed over a BSC with crossover probability ε only for the purposes of detecting error, then the probability P_{ue} of undetected error satisfies the upper bound,

$$P_{\text{ue}} \leq |\mathscr{C}|\, \varepsilon^d (1-\varepsilon)^{n-d}.$$

12. A linear block code $\mathscr{C}$ is used to accomplish error-correction over a Binary Symmetric Channel (BSC) with cross-over probability ε. The standard array is used to carry out maximum-likelihood decoding (MLD) of the code. Then the probability of codeword error P_{we} can be determined

    (a) just from knowing the weight distribution of the code

    (b) just from knowing the list of all coset leaders,

    (c) only if both the weight distribution of the code and the list of coset leaders is known

    (d) only if the entire standard array is provided.

    Identify the most appropriate answer(s).

13. The covering radius of a linear $[n,k]$ code $\mathscr{C}$ is the smallest integer ρ such that for any $\underline{x} \in \mathbb{F}_2^n$, there exists a codeword $\underline{c} \in \mathscr{C}$ such that

$$d_H(\underline{c},\underline{x}) \leq \rho.$$

    (a) How would you determine ρ from a standard array decoding table of the code ?

    (b) What is the covering radius of the $[7,4,3]$ Hamming code ?

14. Determine the Reed-Muller canonical expansion for the Boolean function in 4 variables (X_1,X_2,X_3,X_4) that corresponds to the vector having a 1 in location (1111) and zeros elsewhere.

15. Show that the Reed-Muller code $RM(0,m)$ is the repetition code.

16. Given

$\underline{X}$	= 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$r(\underline{X})$	= 0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	1

find using majority logic, the nearest codeword in $RM(1,4)$ to $r(\underline{X})$. You should interpret $\underline{X} = 4$ to mean $(X_1,X_2,X_3,X_4) = (0100)$ and $\underline{X} = 11$ to mean $(X_1,X_2,X_3,X_4) = (1011)$ and so on.

17. Find a generator matrix and a parity check matrix for the Reed-Muller code $RM(2,4)$.

18. Show that the dimension of $RM(r,m)$ is equal to the sum of the dimensions of $RM(r,m-1)$ and $RM(r-1,m-1)$.

19. A code is said to be self-dual if $\mathscr{C} = \mathscr{C}^{\perp}$.

    (a) Under what conditions on P is $\mathscr{C}$ having $G = [I \mid P]$ self-dual ?

    (b) Show that $RM(1,3)$ is a self dual code.

20. (From Lin-Costello) Form a generator matrix for the first-order RM code RM(l, 4) of length 16. What is the minimum distance of the code? Determine its parity-check sums and devise a majority-logic decoder for the code. Decode the received vector is $r = (0011001001110011)$.