IIIT-H
EC5.205: Introduction to Coding Theory
Spring-2024

Course instructors: Prasad Krishnan and Arti Yardi

Exam: End-sem
Total Marks: 60

Date: 28-Feb-2024
Time: 8:30 am to 10:30 am

Instructions:

- Answering all the questions is compulsory.
- All steps should be justified in detail.
- Clearly state the assumptions (*if any*) made that are not specified in the questions.

---

1. (7 marks) Let C_1 be a (n, k_1) binary linear block code with minimum distance d_1 and let C_2 be a (n, k_2) binary linear block code with minimum distance d_2. Consider the following set of vectors of length $2n$.

$$C = \left\{(\mathrm{v}, \mathrm{v}+\mathrm{w}) \middle| \forall \mathrm{v} \in C_1, \forall \mathrm{w} \in C_2\right\},$$

where $(\mathrm{v}, \mathrm{v}+\mathrm{w})$ denotes the concatenation of vectors v and $\mathrm{v}+\mathrm{w}$.

   (a) (3 marks) Prove that the set C is a binary linear block code with dimension $k = k_1 + k_2$. (Hint: Construct a generator matrix for this code using that of the codes C_1, C_2 , prove that it has full-rank.)

   (b) (4 marks) What will be the minimum distance of code C? Justify your answer.

2. (6 marks) Let H be the parity check matrix of a Hamming code of length $n = 2^m - 1$. Consider a matrix H' obtained by removing all columns of even weight from H. Let C be the code whose parity check matrix is H'.

   (a) (1+2 marks) Find the length and the *rate* of C.

   (b) (3 marks) Show that C can correct all single bit errors and detect all two-bit errors.

3. (17 marks) Consider a linear $(5, 3)$ code over $\mathbb{F}_4$ with the generator matrix given below

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

where α is a primitive element of $\mathbb{F}_4$.

   (a) (2 marks) Find the parity-check matrix of this code.

   (b) (2 marks) How many codewords are there in this code?

   (c) (3 marks) What is the minimum distance of the code? Let t denote the maximum number of errors this code can correct. What is t? (Note: You have to *prove* that the minimum distance is so much. Just claiming will not get you the marks).

(d) (6 marks=3+3) Check if this code is MDS. Is it also a perfect code ?

(e) (4 marks) Assume that the message vector $(1, \alpha, 1)$ was transmitted upon encoding. Show the correctness of decoding of the message vector transmitted, if exactly t errors occurred in the first t positions.
Note: Note that the error locations are specified in the question, but not the error values. You can assume any specific non-zero error values. However, you should assume the decoder gets only the received vector as its input (and of course it knows the codebook), not the error location or the error values.

4. (13 marks)

(a) (5 marks) Construct $\mathbb{F}_{32}$ (In other words, identify the appropriate irreducible polynomial, and express $\mathbb{F}_{32}$ using the same. In case of any polynomial you want to claim irreducibility of, you have to prove the claim).

(b) (3 marks) What are the possible orders of the elements in $\mathbb{F}_{32}$? Identify all the primitive elements of $\mathbb{F}_{32}$. (Hint: Recall a property of the order of any non-zero element in the finite field. Use that to identify the primitive elements also. There is no need to calculate all powers to obtain all elements explicitly, etc.)

(c) (5 marks) Construct an MDS code of length 30 over this field, which can correct upto 10 errors. (i.e., show generator or parity check matrix. Make sure you argue why it's full-rank and why it can correct upto 10 errors.)

5. (17 marks. Part (c) of this question can be done independently of other parts). A linear code C is said to be a *cyclic* code, if for each $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, the cyclically shifted vector $\sigma(c) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ also belongs to C.

(a) (3 marks) Show that, if we write the vector c as a polynomial $c(X) = \sum_{i=0}^{n-1} c_i X^i$, then the cyclically shifted vector $\sigma(c)$ has the polynomial representation

$$Xc(X)(\text{mod } (X^n - 1)).$$

(b) (4 marks) Recall the construction of a binary BCH code as done in the class. Show that a binary BCH code (as defined in the class) is indeed a cyclic code. (Note: You need not reprove lemmas proved in the class, for this question. You can use them as is. Probably (a) part is useful.)

(c) (7+3 = 10 marks) Construct a binary BCH code of length $n = 17$, which can correct double errors. Find its dimension. (Hint: To construct the code, you need to clearly specify how to identify the codebook using the polynomial technique. The exact polynomial which generates this code should be identified first, as a product of its linear factors. You should also argue with proof how the code is actually linear. You should also give arguments (relying upon statements proved in class) that it is a binary code also. For getting its dimension, you need the number of rows in a full parity check matrix of this code.)