E2 205 Error-Control Coding
Homework 2

Discussion: 2:00 PM, September 13, 2019

1. Consider the subset H of the real numbers $\mathbb{R}$ given by

$$H = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

where $\mathbb{Q}$ denotes the set of all rational numbers. Is H a field under the usual operations of real-number addition and multiplication ? Justify your answer.

2. Consider the collection of all functions $f : \mathbb{R} \to \mathbb{R}$. We define addition of functions in the usual way:

$$(f + g)(x) = f(x) + g(x), \quad x \in \mathbb{R}$$

and multiplication via composition:

$$(f \cdot g)(x) = f(g(x)), \; x \in \mathbb{R}$$

What can you say about the algebraic structure of the class of such functions under this pair of operations ?

3. Give examples of

   (a) a ring R without identity,

   (b) a ring R_I with identity that is not a division ring,

   (c) a non-commutative ring R_{NC},

   (d) a commutative ring R_C that is not an integral domain.

4. Let V be a vector space over a field $\mathbb{F}$ and let S_1, S_2 be subspaces of V. Define

$$S_1 + S_2 = \{x + y \mid x \in S_1, \; y \in S_2\}.$$

Show that $S_1 \cap S_2$ and $S_1 + S_2$ are subspaces of V.

5. Consider the set $S = \{0\} \bigcup \{\alpha^i \mid 0 \le i \le 6\}$ along with two operations addition and multiplication. Multiplication in the set S is performed as follows:

$$\alpha^i \cdot \alpha^j = \alpha^k, \; 0 \le i, j, k \le 6 \text{ where } k = i + j \pmod{7}$$

and

$$0 \cdot x = x \cdot 0 = 0, \text{ for any element } x \text{ in } S.$$

Also

$$0 + x = x + 0 = x, \text{ for any element } x \text{ in } S.$$

All other additions are governed by the table below:

$+$	1	α	α^2	α^3	α^4	α^5	α^6
1	0	α^3	α^6	α	α^5	α^4	α^2
α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^2	α^5	1	α^4	α^3	α	0

Is the set S together with the operations of addition and multiplication a field ? Show all your working and explain your answer.

6. Find a suitable generator matrix G for the linear block code whose parity-check matrix H is given by

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

Justify your method.

7. The matrix H is the (3×7) parity-check matrix of a $[7,4,3]$ Hamming code $\mathscr{C}$.

   (a) What are the parameters $[n,k,d_{min}]$ of the dual $\mathscr{C}^{\perp}$?

   (b) Let H_1 be the (4×7) matrix obtained by adding the all-1 row to the 3 rows of H:

$$H_1 = \begin{bmatrix} & & & H & & & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

   What are the parameters $[n,k,d_{min}]$ of the code $\mathscr{C}_1$ that is the nullspace of H_1 ?

8. For each of the parity-check matrices $H_i, i = 1,2,3$ given below, determine the minimum distances d_i of the associated binary linear code $\mathscr{C}_i$, as well as a pair of codewords $(\underline{a}_i, \underline{b}_i)$ belonging to $\mathscr{C}_i$, whose Hamming distance, $d_H(\underline{a}_i, \underline{b}_i)$, equals d_i.

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$H_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$H_3 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

9. Consider the linear block code $\mathscr{C}$ having generator matrix given by

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

   (a) What is the minimum distance of $\mathscr{C}$?

   (b) What is the minimum distance of the *dual* code $\mathscr{C}^{\perp}$?

10. (from Lin and Costello) Consider a $[8,4]$ linear code whose parity-check equations are given by

$$\begin{aligned} v_0 &= u_1 + u_2 + u_3 \\ v_1 &= u_0 + u_1 + u_2 \\ v_2 &= u_0 + u_1 + u_3 \\ v_3 &= u_0 + u_2 + u_3 \end{aligned}$$

where u_0, u_1, u_2, u_3 are the message symbols and v_0, v_1, v_2, v_3 are the parity-check symbols. Find generator and parity-check matrices for this linear code.