Exercise 1 - Basics of Algebra and Error-correcting Codes

Alegbra

Q1. Which of the following is a group?

- $(\{0,1,2,3\},+)$, $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\times)$;
- $(\mathbb{Q},+)$, $(\mathbb{Q},\times)$
- polynomials $\mathbb{Z}[x] = \{\sum_i a_i x^i\}$

Q2. List 3 examples of fields

Q3. Let $f(x) = x^4 + x + 1$ be the irreducible polynomial in $\mathbb{F}_2[x]$ and

$$\mathbb{F}_{2^4} = \mathbb{F}_2[x] \big/ (f(x)) = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 \,:\, a_i \in \mathbb{F}_2\}.$$

Assume each element in $\mathbb{F}_{2^4}$ is represented as (a_0, a_1, a_2, a_3) corresponding to polynomials $a_0 + a_1 x + a_2 x^2 + a_3 x^3$. Calculate the following multiplications:

- $(1,0,1,1) \otimes (1,0,0,1)$;
- $(0,1,0,1) \otimes (1,0,1,1)$

Q4. Prove that for any $\beta \in \mathbb{F}_{q^n}$, $\mathrm{Tr}(\beta) = \beta + \beta^q + \cdots + \beta^{q^{n-1}}$ belongs to $\mathbb{F}_q$

Linear Codes

Q1. For the $[7,4,3]_2$ Hamming code with a parity-check matrix

$$\begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} \end{bmatrix}$$

where the columns are indexed by integers $\mathbf{j}$ where its 2-ary expansion $j = j_0 + j_1 2 + j_2 2^2$ gives the column $[j_0, j_1, j_2]^\intercal$. The standard array is given by

- Build up the error-syndrome look up table and decode the following words: 0111101, 1110110, 0011011

Table 3.1: The Standard Array for a Code

Row 1	0000000	0111100	1011010	1100110	1101001	1010101	**0110011**	0001111
Row 2	1000000	1111100	0011010	0100110	0101001	0010101	1110011	1001111
Row 3	0100000	0011100	1111010	1000110	1001001	1110101	0010011	0101111
Row 4	0010000	0101100	1001010	1110110	1111001	1000101	0100011	0011111
Row 5	0001000	0110100	1010010	1101110	1100001	1011101	0111011	0000111
Row 6	0000100	0111000	1011110	1100010	1101101	1010001	0110111	0001011
Row 7	0000010	0111110	1011000	1100100	1101011	1010111	0110001	0001101
Row 8	0000001	0111101	1011011	1100111	1101000	1010100	0110010	0001110
Row 9	1100000	1011100	0111010	0000110	0001001	0110101	1010011	1101111
Row 10	1010000	1101100	0001010	0110110	0111001	0000101	1100011	1011111
Row 11	0110000	0001100	1101010	1010110	1011001	1100101	0000011	0111111
Row 12	1001000	1110100	0010010	0101110	0100001	0011101	1111011	1000111
Row 13	**0101000**	0010100	1110010	1001110	1000001	1111101	**0011011**	0100111
Row 14	0011000	0100100	1000010	1111110	1110001	1001101	0101011	0010111
Row 15	1000100	1111000	0011110	0100010	0101101	0010001	1110111	1001011
Row 16	1110000	1001100	0101010	0010110	0011001	0100101	1000011	1111111

- Check the standard array closely. Can we uniquely correct errors e with Hamming weight two? For which errors of weight two, we cannot uniquely correct?

Q2. Given a cyclic code C of length n with generator polynomial

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k-1}x^{n-k-1} + x^{n-k},$$

and parity-check polynomial $h(x) = (x^n - 1)/g(x) == h_0 + h_1 x + \cdots + h_{k-1}x^{k-1} + x^k$. Verify the following matrix

$$H = \begin{pmatrix} 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 & & & & \\ & 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 & & & \\ & & 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 & & \\ & & & & \ddots & \ddots & & \ddots & \ddots & \\ & & & & 1 & h_{k-1} & h_{k-2} & \cdots & h_1 & h_0 \end{pmatrix}$$

is a parity-check matrix of C.

Decoding of BCH codes

Let $\mathbb{F}_{2^4}$ be generated from the primitive polynomial $f(x) = x^4 + x + 1$. Let a binary $[15, 7, 5]_2$ BCH code have a generator polynomial

$$g(x) = (x^4 + x + 1) * (x^4 + x^3 + x^2 + x + 1).$$

Suppose Bob receives a word

$$\mathbf{r} = (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1).$$

- List the zeros β_j of $g(x)$ where $\beta_j = \alpha^j$

- Define an error polynomial of two terms:

$$e(x) = x^{i_1} + x^{i_2}$$

- Write down the evaluation of the error polynomial as

$$e(\beta_j) = e(\alpha^j) = \alpha^{ji_1} + \alpha^{ji_2} = \beta_{i_1}^j + \beta_{i_2}^j = \mathbf{r}(\beta_j) = s_j, \quad j = 1, 2, \ldots, 4$$

  Arrange $s_1, s_2, \ldots, s_8$ in a column, check their expressions according to the terms $\beta_{i_1}^j$ and $\beta_{i_2}^j$.

- Define an error locator polynomial

$$\sigma = (1 - \beta_{i_1} x)(1 - \beta_{i_2} x) = 1 + \sigma_1 x + \sigma_2 x$$

- Using the `https://en.wikipedia.org/wiki/Newton%27s_identities` to establish the system of linear equations

$$\begin{bmatrix} s_2 & s_1 \\ s_3 & s_2 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \end{bmatrix} = \begin{bmatrix} s_3 \\ s_4 \end{bmatrix}$$

- Solve the above equation and the corresponding error-locator polynomial $\sigma(x) = 0$ by exhausting α^j for $j = 1, 2, \ldots, 8$

- Correct the errors in the word r