UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

5th set - Answers

Exercise 1. Let C be the linear code over $\mathbb{F}_9$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & \alpha & 1 \\ 0 & 1 & 1 & 1 & \alpha \end{pmatrix},$$

where α is a root of $X^2 + 1 \in \mathbb{F}_3[X]$. Find two non-zero codewords of C of minimum weight.

Answer. First, we note that $X^2 + 1$ is in fact irreducible over $\mathbb{F}_3$, since it has no roots in $\mathbb{F}_3$.

Next, it is clear that every pair of columns of H are linearly independent, whilst the three first columns of H are linearly dependent. It follows that $d(C) = 3$. Moreover, H is a generator matrix of $C^\perp$ and as a generator matrix, it is in standard form. It follows that a parity-check matrix of $C^\perp$, i.e., a generator matrix of C is

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 \\ 2\alpha & 2 & 0 & 1 & 0 \\ 2 & 2\alpha & 0 & 0 & 1 \end{pmatrix}.$$

It follows that two words of minimum weight are $w_1 = (2, 2, 1, 0, 0)$ and $w_2 = (2\alpha, 2, 0, 1, 0)$. □

Exercise 2. Let G and G' be generator matrices of the linear code C. Show that if both G and G' are in standard form then $G = G'$.

Answer. Set $k = \dim(C)$. Let g_i, g_i' be the i-th row of G and G' respectively. Since $G \neq G'$, we have that $g_\ell \neq g_\ell'$ for some ℓ. The facts that g_ℓ and g_ℓ' are both the ℓ-th rows of generator matrices in standard form and that $g_\ell \neq g_\ell'$, imply that

$$g_\ell - g_\ell' = (\underbrace{0, \dots, 0}_{k-\text{times}}, h_{k+1}, \dots, h_n) \in C \setminus \{\mathbf{0}\}.$$

However, the fact that C admits a generator matrix in standard form implies that the only codeword with zeros in all of its first k positions is the all-zero word, a contradiction. □

Exercise 3. Construct a binary code C of length 6 as follows: for every $(x_1, x_2, x_3) \in \mathbb{F}_2^3$, construct a 6-bit word $(x_1, x_2, x_3, x_4, x_5, x_6) \in C$, where

$$\begin{aligned} x_4 &= x_1 + x_2 + x_3, \\ x_5 &= x_1 + x_3, \\ x_6 &= x_2 + x_3. \end{aligned}$$

1. Show that C is a linear code.
2. Find a generator matrix and a parity-check matrix for C.
3. Decode the words $w_1 = 111111$ and $w_2 = 101010$.

Answer. It is clear that the typical codeword of C is of the form

$$c = x_1(1,0,0,1,1,0) + x_2(0,1,0,1,0,1) + x_3(0,0,1,1,1,1), \quad x_i \in \mathbb{F}_2.$$

It follows that $C = \langle 100110, 010101, 001111 \rangle$, which is clearly a linear code with generator matrix

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

Since G is in standard form, we can immediately construct a parity-check matrix of C in standard form as follows:

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

It follows that C is a binary $[6,3,3]$-code. We will now use cosets decoding to decode w_1 and w_2. First, we list the coset of C as follows, where the corresponding coset leaders are underlined:

$$\begin{aligned}
C + 000000 &= \{\underline{000000}, 100110, 010101, 001111, 110011, 101001, 011010, 111100\}, \\
C + 000001 &= \{\underline{000001}, 100111, 010100, 001110, 110010, 101000, 011011, 111101\}, \\
C + 000010 &= \{\underline{000010}, 100100, 010111, 001101, 110001, 101011, 011000, 111110\}, \\
C + 000100 &= \{\underline{000100}, 100010, 010001, 001011, 110111, 101101, 011110, 111000\}, \\
C + 001000 &= \{\underline{001000}, 101110, 011101, 000111, 111011, 100001, 010010, 110100\}, \\
C + 010000 &= \{\underline{010000}, 110110, 000101, 011111, 100011, 111001, 001010, 101100\}, \\
C + 100000 &= \{\underline{100000}, 000110, 110101, 101111, 010011, 001001, 111010, 011100\}, \\
C + 110000 &= \{\underline{110000}, 010110, 100101, 111111, \underline{000011}, 011001, 101010, \underline{001100}\}.
\end{aligned}$$

We note that both w_1 and w_2 belong in the last coset, which admits three leaders, that is, in the case of incomplete decoding we request a retransmission. In the case of complete decoding, we may (arbitrarily) choose $e = 110000$ for both of them and decode to $c_1 = 001111$ and $c_2 = 011010$ respectively. $\square$

Exercise 4. Let C be the binary linear code with parity-check matrix

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

1. Write a generator matrix of C and find the parameters of C. How many errors does C correct?

2. Decode the words $w_1 = 110110$ and $w_2 = 011011$, using coset decoding.
3. Construct a syndrome look-up table and use it to decode the words $w_3 = 100100$ and $w_4 = 011101$.

Answer. We note that the parity-check matrix H is in standard form, so we can easily construct the following generator matrix in standard form:

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

From the parity-check matrix, it is clear that C is a binary $[6, 3, 3]$-code.

We shall now decode w_1 and w_2 using coset decoding. So, we list the cosets of C as follows, where the corresponding coset leaders are underlined:

$$\begin{aligned}
C + 000000 &= \{\underline{000000}, 100110, 010101, 001011, 110011, 101101, 011110, 111000\}, \\
C + 000001 &= \{\underline{000001}, 100111, 010100, 001010, 110010, 101100, 011111, 111001\}, \\
C + 000010 &= \{\underline{000010}, 100100, 010111, 001001, 110001, 101111, 011100, 111010\}, \\
C + 000100 &= \{\underline{000100}, 100010, 010001, 001111, 110111, 101001, 011010, 111100\}, \\
C + 001000 &= \{\underline{001000}, 101110, 011101, 000011, 111011, 100101, 010110, 110000\}, \\
C + 010000 &= \{\underline{010000}, 110110, 000101, 011011, 100011, 111101, 001110, 101000\}, \\
C + 100000 &= \{\underline{100000}, 000110, 110101, 101011, 010011, 001101, 111110, 011000\}, \\
C + 100001 &= \{\underline{100001}, 000111, 110100, 101010, \underline{010010}, \underline{001100}, 111111, 011001\}.
\end{aligned}$$

Observe that both w_1 and w_2 belong in the same coset that has the unique leader $e = 010000$, so we decode to $c_1 = 100110$ and $c_2 = 001011$ respectively.

Using the above list, we can construct the following syndrome look-up table[1]:

Coset leader	Syndrome
000000	000
000001	001
000010	010
000100	100
001000	011
010000	101
100000	110
100001	**111**

The last entry of the above is in **bold** to indicate that fact that the corresponding coset has multiple leaders. Next, we compute

$$S(w_3) = w_3 \cdot H^T = 010 \quad \text{and} \quad S(w_4) = w_4 \cdot H^T = 011.$$

From the syndrome look-up table, we get that the corresponding errors are $e_1 = 000010$ and $e_2 = 0010000$, so we decode to $c_1 = 100110$ and $c_2 = 010101$ respectively. □

[1]Note that the construction of the syndrome look-up table can also be done without the above list, as mentioned in the lectures.

Exercise 5. Prove that $A_2(5,4) = B_2(5,4) = 2$.

Answer. First, we observe that the binary code $C' = \langle 11110 \rangle$ is a linear binary $(5,2,4)$-code. It follows that

$$2 \leq B_2(5,4). \tag{1}$$

Now, let C be a binary code of length 5, such that $d(C) = 4$. Assume that $c = (c_1, c_2, c_3, c_4, c_5) \in C$. Since $d(C) = 4$, another codeword of C has to be one of $(c_1', c_2', c_3', c_4', c_5)$, $(c_1', c_2', c_3', c_4, c_5')$, $(c_1', c_2', c_3, c_4', c_5')$, $(c_1', c_2, c_3', c_4', c_5')$, $(c_1, c_2', c_3', c_4', c_5')$ or $(c_1', c_2', c_3', c_4', c_5')$, where $c_i' := 1 + c_i$. However, we easily check that for every pair of these words, their Hamming distance is at most 3. In other words, C can contain at most one of them. It follows that $|C| \leq 2$, which implies

$$A_2(5,4) \leq 2. \tag{2}$$

Equations (1) and (2), combined with the fact that $B_2(5,4) \leq A_2(5,4)$, yield the desired result. $\square$