THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Suggested Solution to Assignment 4

1. (a) Show that $x^3 + x^2 + 2$ is an irreducible polynomial in $\mathbb{Z}_3[x]$.

   (b) Suppose that F be the field defined by $\mathbb{Z}_3[x]/\langle x^3 + x^2 + 2\rangle$.
   If $\alpha = x^2 + x + 1, \beta = x^2 + 2 \in F$, find $\alpha + \beta$, $\alpha\beta$ and α^{-1}.

   Ans:

   (a) Let $f(x) = x^3 + x^2 + 2$. Then $f(0) = 2$, $f(1) = 1$ and $f(2) = 2$ which are all nonzero. $f(x)$ is a cubic polynomial without linear factor and so $f(x)$ is an irreducible in $\mathbb{Z}_3[x]$.

   (b) Note that $x^3 + x^2 + 2 \equiv 0 \pmod{x^3 + 2x^2 + 2}$, so $x^3 \equiv -x^2 - 2 \equiv 2x^2 + 1 \pmod{x^3 + 2x^2 + 2}$. Then, $\alpha + \beta = 2x^2 + x$ and

$$\begin{aligned}
\alpha\beta &= x^4 + x^3 + 3x^2 + 2x + 2 \\
&= x(x^3) + x^3 + 2x + 2 \\
&= x(2x^2 + 1) + (2x^2 + 1) + 2x + 2 \\
&= 2x^3 + 2x^2 + 3x + 3 \\
&= 2(2x^2 + 1) + 2x^2 \\
&= 6x^2 + 2 \\
&= 2
\end{aligned}$$

   By extended Euclidean algorithm, we have $1 = (x^2 + x + 1)(2x^2 + 1) + x(x^3 + x^2 + 2)$.
   Therefore, $(x^2 + x + 1)(2x^2 + 1) \equiv 1 \pmod{x^3 + x^2 + 2}$ and we have $\alpha^{-1} = 2x^2 + 1$.

2. The parity check matrix of [15,11] binary Hamming code is given by

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

   What are the decoded vectors if vector $y_1 = (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$ and
   $y_2 = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$ are received?

   Ans:

   We compute the syndrome $y_1 H^T = (1, 0, 0, 1)$ which is the fifth row of H^T. Therefore, the decoded vector is $c_1 = y_1 - e_5 = (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$.

   We alse compute the syndrome $y_2 H^T = (0, 1, 0, 0)$ which is the 13-th row of H^T. Therefore, the decoded vector is $c_1 = y_1 - e_{13} = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$.

3. Let $F = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ and let

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

be the generating matrix of a [5, 3] linear code C over the field F.

(a) Find a parity check matrix of C and show that the minimum distance $d(C)$ of C is 3.

(b) Show that C is a perfect code.

(c) What are the decoded vectors if vector $y_1 = (x, 1, 1 + x, x, 0)$ and $y_2 = (1, x, 1 + x, 1 + x, 1)$ are received?

Ans:

(a) $H = \begin{pmatrix} 1 & x & 1 & 1 & 0 \\ x & 1 & 1 & 0 & 1 \end{pmatrix}$ is a parity matrix of C.

Here, we denote the entry of H located at the i-th row and j-th column by h_{ij}.

Let $v \in C$ with $v \neq 0$. Then $\text{wt}(v) > 0$. Note that $vH^T = 0$, so

- if $\text{wt}(v) = 1$, then $v = ae_i$ for some nonzero $a \in F$ and $vH^T = ae_iH^T = (ah_{i1}, ah_{i2})$ which is nonzero (Contradiction).
- if $\text{wt}(v) = 2$, then $v = a_ie_i + a_je_j$ for some nonzero $a_i, a_j \in F$, $i \neq j$.
  We have $(0, 0) = vH^T = (a_ie_i + a_je_j)H^T = (a_ih_{i1} + a_jh_{j1}, a_ih_{i2} + a_jh_{j2})$, i.e.

$$\begin{pmatrix} h_{i1} & h_{j1} \\ h_{i2} & h_{j2} \end{pmatrix} \begin{pmatrix} a_i \\ a_j \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

  However, the det $\begin{pmatrix} h_{i1} & h_{j1} \\ h_{i2} & h_{j2} \end{pmatrix} \neq 0$ for all $i \neq j$ and so the above system may only have trivial solution, which contradicts to that a_i and a_j are nonzero.

Therefore, $d(C) \geq 3$.

On the other hand, if $v = (0, 0, 1, 1, 1)$, then v is the third row of G which implies $v \in C$ and we have $\text{wt}(v) = 3$. Therefore, $d(C) = 3$.

(b) Note that the number of codewords $= 4^3$ and the number of vectors in a Hamming sphere of radius 1 centered at a codeword $= 1 + 5 \times 3 = 16 = 4^2$. Therefore,

$$\begin{aligned} & (\text{Number of code words}) \times (\text{Number of elements per sphere}) \\ = \; & 4^5 \\ = \; & \text{Number of vectors in } F^5 \end{aligned}$$

and it is a perfect code.

(c) We compute the syndrome $y_1H^T = (1, 1) = e_3H^T$. Therefore, the decoded vector is $c_1 = y_1 - e_3 = (x, 1, x, x, 0)$.

We alse compute the syndrome $y_2H^T = x(1, 1) = xe_3H^T$. Therefore, the decoded vector is $c_1 = y_1 - xe_3 = (1, x, 1, 1 + x, 1)$.

4. Let C be a linear code over $\mathbb{Z}_3$ generated by the matrix

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

(a) List all the codewords of C and show that the minimum distance $d(C)$ is 3.

(b) Find a parity check matrix of C and hence construct a table of coset leaders and syndromes.

(c) Use the table constructed in (b) to decode the received vector $(2, 0, 1)$.

Ans:

(a) Since there is only one row vector in G, namely $v = (1, 2, 1)$.

Therefore, $C = \text{span}\{v\} = \{cv : c \in \mathbb{Z}_3\} = \{(0, 0, 0), (1, 2, 1), (2, 1, 2)\}$.

Then, we have $d(C) = 3$.

(b) We have

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

as a parity check matrix.

We construct the following table:

(0,0,0)	(1,2,1)	(2,1,2)
(1,0,0)	(2,2,1)	(0,1,2)
(0,1,0)	(1,0,1)	(2,2,2)
(0,0,1)	(1,2,2)	(2,1,0)
(2,0,0)	(0,2,1)	(1,1,2)
(0,2,0)	(1,1,1)	(2,0,2)
(0,0,2)	(1,2,0)	(2,1,1)
(1,1,0)	(2,0,1)	(0,2,2)
(0,1,1)	(1,0,2)	(2,2,0)

where the first column consists of coset leaders and the first row consists of codewords. Then, we can construct the following table by using the parity check matrix H:

Coset Leaders	Syndromes
(0,0,0)	(0,0)
(1,0,0)	(1,2)
(0,1,0)	(1,0)
(0,0,1)	(0,1)
(2,0,0)	(2,1)
(0,2,0)	(2,0)
(0,0,2)	(0,2)
(1,1,0)	(2,2)
(0,1,1)	(1,1)

(Remark: Since we can correct up to 1 error, the second to seventh row should appear in your answer, but the last two rows of your table may be different from the answer provided.)

(c) Let $v = (2, 0, 1)$. Then, the syndrome is $vH^T = (2, 2)$ and the corresponding coset leader is $r = (1, 1, 0)$. Therefore, we decode it as $c = v - r = (1, 2, 1)$.

(Remark: The decoded result depends on your table constructed in (b).)

5. Suppose that F be the field defined by $\mathbb{Z}_2[y]/\langle y^4 + y + 1\rangle$. Let $\alpha = y$.

(You may assume the fact that $y^4 + y + 1$ is an irreducible polynomial in $\mathbb{Z}_2[y]$.)

(a) Show that α is a generator of the cyclic group $F^\times = F\backslash\{0\}$.

(Hint: Show that $\alpha^3, \alpha^5 \neq 1$.)

(b) Show that $x^{15} - 1 \in F[x]$ can be factorized as $(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{14})$.

(c) Show that $\alpha, \alpha^2, \alpha^4, \alpha^8$ are all zeros of $x^4 + x + 1 \in F[x]$ and $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ are all zeros of $x^4 + x^3 + x^2 + x + 1$.

(Hint: $(x^4 + x + 1)^2 = x^8 + x^2 + 1$ and $(x^4 + x + 1)^4 = (x^8 + x^2 + 1)^2 = x^{16} + x^4 + 1$.)

(d) If C is the linear code generated by $g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$, show that $d(C) \geq 5$.

Ans:

(a) Note that $F^\times$ has 15 elements. Therefore, α is a generator if $\alpha^3, \alpha^5 \neq 1$. Clearly $\alpha^3 = y^3 \neq 1$ and $\alpha^5 = y^2 + y \neq 1$, so $\alpha = y$ is a generator of $F^\times$.

(b) Note that $\alpha^{15} = 1$.

Let $f(x) = x^{15} - 1 \in F[x]$. Then, for $i = 1, 2, \ldots, 14$, we have

$$f(\alpha^i) = (\alpha^i)^{15} - 1 = (\alpha^{15})^i - 1 = 1^i - 1 = 0.$$

Also, $f(1) = 0$, so $1, \alpha, \alpha^2, \ldots, \alpha^{14}$ are distinct roots of $f(x)$ while $f(x)$ is a monic polynomial of degree 15 which has at most 15 distinct roots. Therefore,

$$x^{15} - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{14}).$$

(c) Firstly, note that α is a zero of $x^4 + x + 1$, i.e. $\alpha^4 + \alpha + 1 = 0$. Then, we have

$$0 = (\alpha^4 + \alpha + 1)^2 = \alpha^8 + \alpha^2 + 1 + 2(\alpha^5 + \alpha^4 + \alpha) = \alpha^8 + \alpha^2 + 1 = (\alpha^2)^4 + \alpha^2 + 1.$$

Therefore, α^2 is also a zero of $x^4 + x + 1$. Repeating the above, we can show α^4 and α^8 are also zeros of $x^4 + x + 1$. By showing that α^3 is a zero of $x^4 + x^3 + x^2 + x + 1$ and using the above method, we can also show that $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ are all zeros of $x^4 + x^3 + x^2 + x + 1$.

(d) Note that $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^6)(x-\alpha^8)(x-\alpha^9)(x-\alpha^{12})$.

Therefore, $g(\alpha) = g(\alpha^2) = \cdots = g(\alpha^{1+3}) = 0$ and we have $d(C) \geq 2 + 3 = 5$.

6. (a) Show that $x^4 - 1 \in \mathbb{Z}_5[x]$ can be factorized as $(x-1)(x-2)(x-3)(x-4)$.

(b) Let $g(x) = (x-3)(x-4)$ and let C be the cyclic code C over $\mathbb{Z}_5$ generated by $g(x)$.

Show that $d(C) = 3$ and write down a generating matrix G and a parity check matrix H.

(c) What is the decoded vector if $y = (2, 2, 4, 2)$ is received?

Ans:

(a) Let $f(x) = x^4 - 1$. Then $f(1) = f(2) = f(3) = f(4) = 0$ and so 1, 2, 3, 4 are roots of $f(x)$. On the other hand, $f(x)$ is a monic polynomial of degree 4 which has at most 4 distinct roots, therefore, $f(x) = (x-1)(x-2)(x-3)(x-4)$.

(b) Let $\alpha = 2$. Then, $\alpha^2 = 4$, $\alpha^3 = 3$, so $x^4 - 1 = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)$ and $g(x) = (x-\alpha^2)(x-\alpha^3)$.

Therefore, $g(\alpha^2) = g(\alpha^{2+1}) = 0$ and we have $d(C) \geq 2 + 1 = 3$.

Note that $g(x) = x^2 + 3x + 2$ and we have a generating matrix

$$G = \begin{pmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \end{pmatrix}.$$

Note that $h(x) = (x^4-1)/g(x) = (x-1)(x-2) = x^2 + 2x + 2$, so we have a parity check matrix

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

Alternative method:

Note that $g(\alpha^2) = g(\alpha^3) = 0$, so we have a parity check matrix

$$H = \begin{pmatrix} 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

(c) Let $H = \begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 2 \end{pmatrix}$.

We have $yH^T = (4,4) = 2(2,2)$ where $(2,2)$ is the third row of H^T.

Therefore, we decode y as $c = y - 2e_3 = (2,2,2,2)$.

Alternative method:

Let $H = \begin{pmatrix} 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$.

We have $yH^T = (2,3) = (\alpha, \alpha^3)$ and so $3/2 = \alpha^2$. Therefore, the error located at the third digit.

Note that $yH^T = (2,3) = 2(1,4)$, where $(1,4)$ is the third row of H^T.

Therefore, we decode y as $c = y - 2e_3 = (2,2,2,2)$.