THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Assignment 4 (Due date: 19 Apr, 2018)

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}.

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 $y_1 = (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$ and $y_2 = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$ are received?

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 $y_1 = (x, 1, 1 + x, x, 0)$ and $y_2 = (1, x, 1 + x, 1 + x, 1)$ are received?

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 $(2, 0, 1)$.

5. (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?

6. 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 $F^\times = F/\{0\}$.

(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 $d(C) \geq 5$.