Edoardo Persichetti Test 3 Solutions

**Exercise 1** See Chapter 5, Theorem 1.

**Exercise 2** Let $q = 3$ and $n = 8$.

a) We have $C_0 = \{0\}$, $C_1 = \{1, 3\}$, $C_2 = \{2, 6\}$, $C_4 = \{4\}$ and $C_5 = \{5, 7\}$.

b) Therefore the multiplicative order of $q$ mod $n$ is 2.

c) The polynomial $x^n - 1$ splits entirely as $(x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2)$ over $\mathbb{F}_q$. We've seen in class that $x^2 + 1$ is not a good polynomial to use since we don't get a primitive root, while $x^2 + 2x + 2$ is good. So we define $\mathbb{F}_{q^m} = \mathbb{F}_9 = \{0, 1, \alpha, \dots, \alpha^7\}$ as seen in class[1].

d) We have $M^{(1)}(x) = (x - \alpha)(x - \alpha^3) = x^2 - (\alpha + \alpha^3) + \alpha^4 = x^2 - x + 2$ which is exactly our irreducible polynomial used to define the field (which makes sense since we're in the primitive case because $8 = 3^2 - 1$). Next is $M^{(2)}(x) = (x - \alpha^2)(x - \alpha^6) = x^2 - (\alpha^2 + \alpha^6) + \alpha^8 = x^2 + 1$. Then $M^{(4)}(x) = x - \alpha^4 = x - 2 = x + 1$. Finally (also, by exclusion) $M^{(5)}(x) = (x - \alpha^5)(x - \alpha^7) = x^2 - (\alpha^5 + \alpha^7) + \alpha^{12} = x^2 + x + 2$.

e) So we have $\theta_0 = 1 + x \cdots + x^7$ by definition. Also "trivial" is $\theta_4$ for which we have coefficients $\epsilon_i = \alpha^{-4i} = 2^i$ so we have $\theta_4 = 1 + 2x + x^2 + 2x^3 + x^4 \cdots + 2x^7$. The remaining ones are $\theta_1 = 2 + 2x + 2x^3 + x^4 + x^5 + x^7$, $\theta_2 = 2 + x^2 + 2x^4 + x^6$ and $\theta_5 = 2 + x + x^3 + x^4 + 2x^5 + 2x^7$.[2]

**Exercise 3** Let $q = 8 = 2^3$ and $n = 9$. Consider $\mathbb{F}_q$ as defined usually by $x^3 + x + 1$ and primitive element $\alpha$. Below is the index table for $\mathbb{F}_q$.

$\alpha^3 + \alpha + 1 = 0$

| element | exponent |
|---|---|
| 000 | – |
| 100 | 0 |
| 010 | 1 |
| 001 | 2 |
| 110 | 3 |
| 011 | 4 |
| 111 | 5 |
| 101 | 6 |

a) We have $C_0 = \{0\}$, $C_1 = \{1, 8\}$, $C_2 = \{2, 7\}$, $C_3 = \{3, 6\}$ and $C_4 = \{4, 5\}$.

b) Therefore the multiplicative order of $q$ mod $n$ is 2.

c) So $m = 2$ as determined in part b), and call $\beta$ an element of $\mathbb{F}_{q^m}$ of order $n$. Therefore the conjugates of $\beta$ are $\beta$ itself and $\beta^8$.

d) Indeed $p(x) = x^2 + \alpha x + \alpha$ is irreducible over $\mathbb{F}_q$ as it has no roots in the field. Thus we can use this to define the field in terms of a primitive root, say $\gamma$. Then for instance $\beta = \gamma^7$ is an element of order $n$ since clearly $\beta^9 = \gamma^{63} = 1$. Below we write the index table for $\mathbb{F}_{q^m}$ up to $\gamma^8$.

[1] Equivalently we could have used $x^2 + x + 2$ and then $M^{(1)}$ and $M^{(5)}$ are swapped.

[2] You should verify that in this case "idempotent" means $E(x) = E^3(x)$.

$\gamma^2 + \alpha\gamma + \alpha = 0$

| element | exponent |
|---|---|
| 00 | – |
| 10 | 0 |
| 01 | 1 |
| $\alpha\alpha$ | 2 |
| $\alpha^2\alpha^4$ | 3 |
| $\alpha^5\alpha^3$ | 4 |
| $\alpha^4 1$ | 5 |
| $\alpha\alpha^2$ | 6 |
| $\alpha^3 1$ | 7 |
| $\alpha 1$ | 8 |
| ... | ... |

Now, we have $\beta = \gamma^7 = \alpha^3 + \gamma$ and $\beta^8 = (\gamma^7)^8 = (\alpha^3 + \gamma)^8 = \alpha^{24} + \gamma^8 = \alpha^3 + (\alpha + \gamma)$, and therefore $Tr_{\mathbb{F}_q}(\beta) = \beta + \beta^8 = (\alpha^3 + \gamma) + (\alpha^3 + \alpha + \gamma) = \alpha$.

e) This is given by $H = (1\ \beta\ \beta^2 \ldots \beta^8)$ as this code has length exactly $(q^m - 1)/(q - 1) = 9 = n$.

f) Using the table described above and remembering $\beta = \gamma^7$ we can compute the remaining powers of $\beta$ and we get

$$\bar{H} = \begin{pmatrix} 1 & \alpha^3 & \alpha^5 \ldots & 1 \\ 0 & 1 & \alpha \ldots & 1 \end{pmatrix}$$

This parity-check matrix has 2 linearly independent rows thus we have dimension $k = 9 - 2 = 7$.

g) The minimal polynomial of $\beta$ is $M^{(1)}(x) = (x + \beta)(x + \beta^8) = x^2 + (\beta + \beta^8)x + \beta^9 = x^2 + \alpha + 1$.

h) This is also the generator polynomial of the code in question, so a generator matrix is given by its cyclic shifts i.e.

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

**Exercise 4** Let $g(x)$ be the generator polynomial of a binary cyclic code of length $n$.

a) Since $(x + 1) \mid g(x)$, any codeword is also a multiple of $x + 1$, and consequently has 1 as a root. Therefore, it must have an even number of non-zero coefficients. Thus, the code contains only codewords of even weight. $\square$

b) Remember that $g(x) \mid x^n + 1$. But $x^n + 1 = (x + 1)(1 + x + x^2 + \cdots + x^{n-1})$. Since $x + 1$ is **not** a factor of $g(x)$, it must divide $1 + x + x^2 + \cdots + x^{n-1}$, which means that the corresponding vector is a codeword. This is exactly the all-1s codeword $111 \ldots 1$. $\square$