Solution of Question 1.

(a) Both the polynomial rings $\mathbb{F}_3[y]/y^2+2$ and $\mathbb{F}_3[y]/y^2+1$ contain the same set of elements $\{0,\ 1,\ 2,\ y,\ y+1,\ y+2,\ 2y,\ 2y+1,\ 2y+2\}$. [4]

(b) Note that

$$y^2+2 = (y+2)(y+1),$$
$$y^2+1 = (y+2)(y+1)+2.$$

It is clear that the multiplicative inverse of $y+1$ does not exist in the polynomial ring $\mathbb{F}_3[y]/y^2+2$. In the polynomial ring $\mathbb{F}_3[y]/y^2+y+2$, because

$$\begin{aligned}2 &= \left(y^2+y+2\right) - (y+2)(y+1)\\ &\equiv 2(y+2)(y+1) \mod y^2+1\end{aligned}$$

it holds that $(y+1)^{-1} = y+2$. [6]

(c)

i). The cyclotomic cosets of 3 mod 8 are $\{0\}$, $\{1,3\}$, $\{2,6\}$, $\{4\}$, and $\{5,7\}$. [4]

ii). From the cyclotomic cosets of 3 mod 8, it is clear that the minimal polynomial of α^2 is given by

$$M^{(2)}(x) = \left(x-\alpha^2\right)\left(x-\alpha^6\right).$$

[2]

iii). To write $M^{(2)}(x)$ as a polynomial in $\mathbb{F}_3[x]$, we realize that $\alpha^6 \equiv \alpha+2 \mod \alpha^2+\alpha+2$, $\alpha^2 \equiv 2\alpha+1 \mod \alpha^2+\alpha+2$, and hence

$$\begin{aligned}M^{(2)}(x) &= (x-(2\alpha+1))(x-(\alpha+2))\\ &= x^2-(3\alpha+3)x+\left(2\alpha^2+2\alpha+2\right)\\ &= x^2+1.\end{aligned}$$

[4]

Solutions of Question 2.

(a) We focus on the mod n algebra. That $a, b \in \mathcal{S}$ implies that a^{-1} and b^{-1} exist. It is clear that $b^{-1} \cdot a^{-1}$ is the multiplicative inverse of $a \cdot b$. By the existence of the multiplicative inverse of $a \cdot b$, it can be concluded that $\gcd(ab,\ n) = 1$. [4]

(b) By default, we focus on the mod n algebra.
$a\mathcal{S} \subset \mathcal{S}$: $\forall b \in \mathcal{S}$, $a \cdot b \in \mathcal{S}$. This implies $a\mathcal{S} \subset \mathcal{S}$.
Now $\forall b_1 \neq b_2$ from the set $\mathcal{S}$, we shall prove that $ab_1 \neq ab_2$. Suppose that $ab_1 = ab_2$. Then $a(b_1 - b_2) = 0$. In other words, $b_1 - b_2 = a^{-1}(a(b_1 - b_2)) = 0$. Contradicts with the assumption that $b_1 \neq b_2$.
As a result, $|a \cdot \mathcal{S}| = |\mathcal{S}|$. Hence, $a \cdot \mathcal{S} = \mathcal{S}$. [5]

(c) The calculation of $|\mathcal{S}|$: Among all the integers $1 \leq i \leq p_1p_2 - 1$, only the following integers are not in $\mathcal{S}$:

$$\begin{array}{cccc} p_1 & 2p_1 & \cdots & (p_2-1)\,p_1 \\ p_2 & 2p_2 & \cdots & (p_1-1)\,p_2 \end{array}.$$

As a result, $|\mathcal{S}| = p_1p_2 - 1 - (p_1 - 1) - (p_2 - 1) = (p_1 - 1)(p_2 - 1) = t$.
For any $a \in \mathcal{S}$, from the fact that $a \cdot \mathcal{S} = \mathcal{S}$, one has

$$\prod_{x \in a \cdot \mathcal{S}} x = \prod_{y \in \mathcal{S}} y,$$

or equivalently |

$$a^t \prod_{y \in \mathcal{S}} y = \prod_{y \in \mathcal{S}} y.$$

Hence $a^t = 1$. [5]

(d)

i). Since $x \equiv y \bmod p_1$ and $x \equiv y \bmod p_2$, it is clear that $p_1 |\, (y - x)$ and $p_2 |\, (y - x)$. Hence, $\operatorname{lcm}(p_1, p_2) \mid (y - x)$, which implies that $p_1p_2 |\, (y - x)$. Therefore, $x \equiv y \bmod p_1p_2$. [3]

ii). Fix an $a \in \{0,\ 1,\ 2,\ \cdots,\ p_1p_2 - 1\}$.
We first show that $a^{de} \equiv a \bmod p_1$. If $p_1 | a$, then it is clear that $a^{de} \equiv a \bmod p_1$. If $p_1 \nmid a$, then by Fermat's Little Theorem $a^{p_1 - 1} \equiv 1 \bmod p_1$ and therefore $a^{de} \equiv a^{k(p_1-1)(p_2-1)+1} \equiv a \bmod p_1$.
Similarly $a^{de} \equiv a \bmod p_2$.

Use the claim in Question 2(d)i). It can be concluded that $a^{de} \equiv a \bmod p_1 p_2$. [3]

Solution of Question 3.

(a)

i). The systematic generator matrix is given by

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

[2]

ii). The systematic parity check matrix is given by

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

[2]

iii). The minimum distance of the code C is 2. This is because there is no zero column in $\boldsymbol{H}$ ($d > 1$) and the first and third columns of $\boldsymbol{H}$ are the same ($d \leq 2$). [3]

(b) The code C is not a linear code. To verify it, consider the two codewords $\boldsymbol{c}_1 = [1, 1, 0, 0, \cdots, 0] \in C$ and $\boldsymbol{c}_2 = [0, 1, 1, 0, \cdots, 0] \in C$. It is clear that $\boldsymbol{c}_1 + \boldsymbol{c}_2 = [1, 2, 1, 0, \cdots, 0] \notin C$. [3]

(c)

i). For all $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \varphi^{-1}(0)$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q$,

$$\begin{aligned} \varphi(\lambda_1 \boldsymbol{v}_1 + \lambda_2 \boldsymbol{v}_2) &= (\lambda_1 \boldsymbol{v}_1 + \lambda_2 \boldsymbol{v}_2) \boldsymbol{H}^T \\ &= \lambda_1 \boldsymbol{v}_1 \boldsymbol{H}^T + \lambda_2 \boldsymbol{v}_2 \boldsymbol{H}^T \\ &= \mathbf{0} + \mathbf{0} = \mathbf{0}. \end{aligned}$$

Hence, $\lambda_1 \boldsymbol{v}_1 + \lambda_2 \boldsymbol{v}_2 \in \varphi^{-1}(0)$. [2]

ii). Any element from $\boldsymbol{v} + \varphi^{-1}(0)$ can be written as $\boldsymbol{v} + \boldsymbol{w}$ where $\boldsymbol{w} \in \varphi^{-1}(0)$. Since

$$\begin{aligned} \varphi(\boldsymbol{v} + \boldsymbol{w}) &= (\boldsymbol{v} + \boldsymbol{w}) \boldsymbol{H}^T \\ &= \boldsymbol{v} \boldsymbol{H}^T + \boldsymbol{w} \boldsymbol{H}^T \\ &= \boldsymbol{s} + \mathbf{0} = \boldsymbol{s}, \end{aligned}$$

it can be concluded that $\boldsymbol{v} + \varphi^{-1}(0) \subset \varphi^{-1}(\boldsymbol{s})$. [2]

iii). Let $\boldsymbol{w} \in \varphi^{-1}(\boldsymbol{s})$. Consider the vector $\boldsymbol{w} - \boldsymbol{v}$. Since $\varphi(\boldsymbol{w} - \boldsymbol{v}) = (\boldsymbol{w} - \boldsymbol{v}) \boldsymbol{H}^T = \boldsymbol{w}\boldsymbol{H}^T - \boldsymbol{v}\boldsymbol{H}^T = \boldsymbol{s} - \boldsymbol{s} = \boldsymbol{0}$, it holds that $\boldsymbol{w} - \boldsymbol{v} \in \varphi^{-1}(\boldsymbol{0})$ and hence $\boldsymbol{w} \in \boldsymbol{v} + \varphi^{-1}(\boldsymbol{0})$. [3]

iv). Suppose that $\varphi^{-1}(\boldsymbol{s}_1) \bigcap \varphi^{-1}(\boldsymbol{s}_2) \neq \phi$. Then there exists a $\boldsymbol{v} \in \mathbb{F}_q^n$ such that $\boldsymbol{v} \in \varphi^{-1}(\boldsymbol{s}_1) \bigcap \varphi^{-1}(\boldsymbol{s}_2)$. Hence $\varphi(\boldsymbol{v}) = \boldsymbol{s}_1$ and $\varphi(\boldsymbol{v}) = \boldsymbol{s}_2$, which is not possible. Therefore, $\varphi^{-1}(\boldsymbol{s}_1) \bigcap \varphi^{-1}(\boldsymbol{s}_2) = \phi$. [3]

Solutions of Question 4.

(a)

i). We first compute the syndrome:

$$yH^T = [0,1,1].$$

From the syndrome vector and the parity check matrix, it is clear that

$$e = [0,0,0,0,0,0,1],$$

which gives the most plausible transmitted codeword

$$\hat{x} = y - e = [0,1,0,1,1,1,0].$$

[5]

ii). The generator matrix of $\mathcal{H}_3^{\perp}$ is clearly H. [2]

(b)

i). It holds that

$$\begin{aligned} x \cdot c(x) &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \\ &\equiv c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} \bmod x^n - 1. \end{aligned}$$

From the definition of the cyclic code, since $[c_0, c_1, \cdots, c_{n-1}] \in C$, the codeword $[c_{n-1}, c_0, \cdots, c_{n-2}]$ is also in the code C. Clearly, $x \cdot c(x) \bmod x^n - 1$ is a generating function of a codeword in C. [3]

ii). Among all possible generating functions, we find the monic polynomial with least degree and set it as the generator polynomial $g(x)$. [2]

iii). Let $x^n - 1 = q(x)\, g(x) + r(x)$ where $\deg(r(x)) < \deg(g(x))$. Take the modulo $x^n - 1$ algebra with both sides of the equation. It holds $0 = q(x)\, g(x) + r(x)$. By linearity of cyclic codes, $r(x) \in C$. Suppose that $r(x) \neq 0$. Then there is a generating function in C with $\deg(r(x)) < \deg(g(x))$. This contradicts with the definition of $g(x)$. As a result, $r(x) = 0$ and hence $g(x) \mid x^n - 1$. [5]

iv). Let α be the primitive element in $\mathbb{F}_{q^m}$. Let $M^{(1)}(x), \cdots, M^{(\delta-1)}(x)$ be the minimal polynomials of $\alpha, \cdots, \alpha^{\delta-1}$ respectively. Construct the cyclic code by choosing the generator polynomial as

$$g(x) = \text{lcm}\left(M^{(1)}(x), \cdots, M^{(\delta-1)}(x)\right).$$

To show that the distance $d \geq \delta$, note that for any $\boldsymbol{c} \in \mathcal{C}$, the corresponding generating function $c(x)$ satisfies $g(x) \,|\, c(x)$. In other words, $c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{\delta-1}) = 0$. In the matrix format,

$$\underbrace{\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \cdots & \alpha^{(\delta-1)(n-1)} \end{bmatrix}}_{\boldsymbol{A}} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \mathbf{0}.$$

Note that any $\delta - 1$ columns in $\boldsymbol{A}$ are linearly independent. It can be concluded that $d \geq \delta$. [5]

Solutions of Question 5.

(a) For any $a \in \mathbb{F}_q \backslash \{0\}$, it holds that $\mathrm{ord}\,(a) \mid (q-1)$. When $q = 64$, $q-1 = 63$. All possible values of the order of an element in $\mathbb{F}_{64}$ are $1, 3, 7, 9, 21, 63$. As a result, for any element $a \in \mathbb{F}_q \backslash \{0, 1\}$, as long as

$$a^x \neq 1, \quad x \in \{3, 7, 9, 21\},$$

we conclude that a is primitive. The search space is much smaller. [7]

(b)

i). Firstly, since x_i's are distinct, the products

$$\prod_{\substack{1 \leq j \leq n \\ j \neq \ell}} \frac{x - x_j}{x_\ell - x_j}, \quad \ell = 1, 2, \cdots, n$$

are well defined (the denominators will never be zero). Secondly, the degree of the polynomial is $n-1$. This follows from the fact that each of the product is of degree $n-1$ in x. Finally, we evaluate $P(x_i)$. Note that if $\ell \neq i$, then term $x_i - x_i = 0$ will appear in the product $\prod_{j \neq \ell} (x - x_j)$. If $\ell = i$, then $\prod_{j \neq \ell} (x - x_j)\Big|_{x=x_i} = \prod_{j \neq i} (x_i - x_j)$. Hence,

$$\prod_{\substack{1 \leq j \leq n \\ j \neq \ell}} \frac{x - x_j}{x_\ell - x_j} = \begin{cases} 0 & \text{if } \ell \neq i, \\ 1 & \text{if } \ell = i. \end{cases}$$

This actually implies that $P(x_i) = y_i$, $i = 1, 2, \cdots, n$. [6]

ii). Let $P(x) = \sum_{\ell=0}^{n-1} a_\ell x^\ell$. That $P(x_i) = y_i$ implies that

$$\sum_\ell a_\ell x_i^\ell = y_i, \quad i = 1, 2, \cdots, n.$$

In a matrix form

$$\underbrace{\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}}_{\boldsymbol{y}} = \underbrace{\begin{bmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{bmatrix}}_{\boldsymbol{X}} \underbrace{\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}}_{\boldsymbol{a}}.$$

Note that the matrix $\boldsymbol{X} \in \mathbb{R}^{n \times n}$ is a Vandermonde matrix. It is of full rank when x_i's are distinct. The solution of $\boldsymbol{a}$ is unique. That is, the polynomial is unique. [7]