Solution of Question 1.

(a)

i It is straightforward to compute that

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

As a result,

$$1=\gcd\left(f\left(x\right),g\left(x\right)\right).$$

[5]

ii According to the previous part, it is clear that

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

Multiply both sides with 2. It holds that

$$1=(2x+2)\left(x^3+x+2\right)+\left(x^2+2x\right)\left(x^2+2x\right).$$

As a result,

$$\begin{aligned} a(x) &= 2x+2, \\ b(x) &= x^2+2x. \end{aligned}$$

[5]

(b)

i By Gaussian elimination, it is clear that

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

[2]

ii The corresponding parity-check matrix is given by

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

[2]

iii The syndrome vector is given by

$$\boldsymbol{y}_1 \boldsymbol{H}^T = [1\ 0\ 1]\,.$$

As a result, the error vector is given by $\boldsymbol{e} = [0\ 0\ 0\ 0\ 1\ 0\ 0]$ and the minimum distance decoder outputs $\hat{\boldsymbol{c}}_1 = [1\ 0\ 0\ 1\ 0\ 1\ 0]$. From the last four bits of $\hat{\boldsymbol{c}}_1$, it is clear that $\hat{\boldsymbol{m}}_1 = [1\ 0\ 1\ 0]$. [3]

iv The syndrome vector is given by

$$[0\ 0\ 0\ 0\ 0\ 0\ 1]\,\boldsymbol{H}^T = [1\ 1\ 0]\,.$$

Let c_5 and c_6 be the 5th and 6th symbols in $\boldsymbol{c}$. Then one has

$$[c_5\ c_6] \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = [1\ 1\ 0]\,.$$

It is clear that $[c_5\ c_6] = [1\ 1]$. Hence $\boldsymbol{c} = [0\ 0\ 0\ 0\ 1\ 1\ 1]$ and $\boldsymbol{m} = [0\ 1\ 1\ 1]$. [3]

Solutions of Question 2.

(a)

$$\begin{aligned} d(\mathcal{C}) &= \min_{c_1, c_2 \in \mathcal{C},\ c_1 \neq c_2} d(c_1, c_2) \\ &= \min_{c_1, c_2 \in \mathcal{C},\ c_1 \neq c_2} d(c_1 - c_2) \\ &= \min_{c \in \mathcal{C},\ c \neq 0} d(c), \end{aligned}$$

where the last step follows from the facts that $c_1 - c_2 \neq \mathbf{0}$, $c_1 - c_2 \in \mathcal{C}$ (by linearity), and $\{c_1 - c_2 : c_1, c_2 \in \mathcal{C},\ c_1 \neq c_2\} = \{c : c \in \mathcal{C},\ c \neq \mathbf{0}\}$ (this can be verified by simply taking $c_2 = \mathbf{0}$). [2]

(b)

- The "only if" part. Let $d(\mathcal{C}) = d$. There exists a codeword c such that $\mathrm{wt}(c) = d$. This implies there exist d columns of $\boldsymbol{H}$ that are linearly dependent. Now take arbitrary $d-1$ columns of $\boldsymbol{H}$. If they are linearly dependent, then there exist a nonzero word c such that $c\boldsymbol{H}^T = \mathbf{0}$ and $\mathrm{wt}(c) = d - 1$. This contradicts the assumption that $d(\mathcal{C}) = d$. As a result, all $d - 1$ columns of $\boldsymbol{H}$ are linearly independent.
- The "if" part. Since $c\boldsymbol{H}^T = \mathbf{0}$ and every $d - 1$ columns of $\boldsymbol{H}$ are linearly independent, it holds that $\min\ \mathrm{wt}(c) > d - 1$. At the same time, since there exist d columns of $\boldsymbol{H}$ that are linearly dependent, the corresponding coefficients give a nonzero codeword $c \in \mathcal{C}$ such that $\mathrm{wt}(c) = d$. Hence, $d(\mathcal{C}) = d$. [6]

(c) Note that $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$. Since each column of $\boldsymbol{H}$ is of length $n - k$, any $n-k+1$ columns of $\boldsymbol{H}$ must be linearly dependent. As a result, $d \leq n-k+1$.

[2]

(d) Take arbitrary $n - k$ columns of $\boldsymbol{H}$. Denote the indices by $i_1, i_2, \cdots, i_{n-k}$. The sub-matrix is given by

$$\boldsymbol{H}_{\mathcal{I}} = \begin{bmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{n-k}} \\ \alpha^{2\cdot i_1} & \alpha^{2\cdot i_2} & \cdots & \alpha^{2\cdot i_{n-k}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(n-k)\cdot i_1} & \alpha^{(n-k)\cdot i_2} & \cdots & \alpha^{(n-k)\cdot i_{n-k}} \end{bmatrix}.$$

Then

$$|H_{\mathcal{I}}| = \prod_{\ell=1}^{n-k} \alpha^{i_\ell} |V_L|,$$

where V_L is a standard Vandemonde matrix with $\beta_\ell = \alpha_{i_\ell}$ and $L = n - k$. Note that $\alpha \neq 0$ and $\beta_\ell \neq \beta_m$ for $\ell \neq m$. It holds that $|H_{\mathcal{I}}| \neq 0$ and every $n - k$ columns of $\boldsymbol{H}$ are linearly independent. Hence $d(C) = n - k + 1$ and it is MDS. [2]

(e) It is clear that $\boldsymbol{G}' = \boldsymbol{H}$, $\boldsymbol{H}' = \boldsymbol{G}$, $n' = n$, and $k' = n - k$. [2]

(f) It is clear that $d = n - k + 1$. We shall show that $d' = n' - k' + 1 = k + 1$ by contradiction. Suppose that $d' \leq k$. Then there must exist a *nonzero* codeword $\boldsymbol{c}' \in \mathcal{C}^{\perp}$ such that $\mathrm{wt}(\boldsymbol{c}') \leq k$ and the number of zero components in $\boldsymbol{c}'$ is at least $n - k$. Without loss of generality, assume that the last $n - k$ components of $\boldsymbol{c}'$ are zero. Write the generator matrix $\boldsymbol{G}' = \boldsymbol{H}$ in the form of $[\boldsymbol{A}\ \boldsymbol{B}]$ where $\boldsymbol{A} \in \mathbb{F}_q^{(n-k)\times k}$ and $\boldsymbol{B} \in \mathbb{F}_q^{(n-k)\times(n-k)}$. By the assumption that C is MDS, the matrix $\boldsymbol{B}$ is of full rank. Let $\boldsymbol{c}' = \boldsymbol{s}' \cdot \boldsymbol{G}' = \boldsymbol{s}' \cdot \boldsymbol{H} = [\boldsymbol{s}' \cdot \boldsymbol{A}\ \boldsymbol{s}' \cdot \boldsymbol{B}]$. That $\boldsymbol{s}' \cdot \boldsymbol{B} = \boldsymbol{0}$ implies that $\boldsymbol{s}' = \boldsymbol{0}$ and hence $\boldsymbol{c}' = \boldsymbol{0}$. This contradicts the assumption that $\boldsymbol{c}' \neq \boldsymbol{0}$. Hence $d' > k$. But by Singleton bound, $d \leq k + 1$. Therefore $d = k + 1$. [6]

Solutions of Question 3.

(a)

i Define $t = (p_1 - 1)(p_2 - 1)$. Choose d and e such that $1 < d, e < t$, $\gcd(d, t) = \gcd(e, t) = 1$, and $d \cdot e = 1 \bmod t$. With this choice, $\hat{m} = c^d = m^{de} = m^{qt+1} = m \bmod n$. [2]

ii If the factorisation $n = p_1 p_2$ is known, then one can compute $t = (p_1 - 1)(p_2 - 1)$ and use Euclidean algorithm to compute $d = e^{-1} \bmod t$. [2]

(b)

i Let $e = \tau(d) = b^d \bmod p$. Then the decryption process is given by

$$\hat{m} = y \cdot x^{-d} = m \cdot e^{dt} \cdot b^{-td} = m \bmod p.$$

[4]

ii

A. It is clear that $\tau(1) = b$ and $p \nmid \tau(1) = b$. Inductively assume that $p \nmid \tau(d-1)$ and we shall show that $p \nmid \tau(d)$. Note that $\tau(d) = \tau(1) \cdot \tau(d-1)$. By Euclid's Lemma, that $p | \tau(d)$ implies that either $p | \tau(1)$ or $p | \tau(d-1)$, both of which are false according to the assumptions. Hence, $p \nmid \tau(d)$. [3]

B. Let $d_1, d_2 \in \mathbb{F}_p^*$ be such that $d_1 \neq d_2$. Without loss of generality, let $d_1 > d_2$. Define $e_1 = \tau(d_1)$ and $e_2 = \tau(d_2)$. Consider $e_1/e_2 = b^{d_1 - d_2} \bmod p$. Since $0 < d_1 - d_2 < p - 1$, $b^{d_1 - d_2} \neq 1$ by the fact that $\mathrm{ord}(b) = p - 1$. Hence $e_1 \neq e_2$ and the mapping τ is one-to-one. [3]

C. Denote the image set of τ by $\mathcal{E}$. It is clear $\mathcal{E} \subseteq \mathbb{F}_p^*$ from part A). Since the mapping is one-to-one, $|\mathcal{E}| = |\mathbb{F}_p^*| = p - 1$, which suggests that $\mathcal{E} = \mathbb{F}_p^*$ and the mapping is onto. [2]

iii Let $x = \mathrm{ord}(\beta)$. Write $p - 1 = q \cdot x + r$ for non-negative integers q and r such that $r < x$. By Fermat's little theorem and the definition of the order, it holds that

$$1 = \beta^{p-1} = \beta^{qx+r} = \beta^r \bmod p.$$

This implies that $r = 0$ otherwise it contradicts the definition of the order. Hence $x | (p - 1)$. [4]

Solutions of Question 4.

(a) In order to show $g(x)\,|c(x)$, write $c(x) = u(x)\,g(x) + r(x)$. By linearity of a cyclic code, $u(x)\,g(x) \in \mathcal{C}$ and $r(x) = c(x) - u(x)\,g(x) \in \mathcal{C}$. By the definition of $g(x)$, it is clear that $\deg(r(x)) = 0$. Hence $g(x)\,|c(x)$.

The uniqueness is proved by contradiction. Suppose that there exist two different monic polynomials $g_1(x) \neq g_2(x)$ of the same degree that generate $\mathcal{C}$. Then by linearity of a cyclic code, $g_1(x) - g_2(x) \in \mathcal{C}$. Note that $\deg(g_1(x) - g_2(x)) < \deg(g_1(x)) = \deg(g_2(x))$. This contradicts the definition of $g(x)$, which proves the uniqueness of $g(x)$. [5]

(b)

i The cyclotomic cosets are
$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$, and $C_7 = \{7, 14, 13, 11\}$. [5]

ii The generator polynomial of the constructed BCH code is given by

$$\begin{aligned} g(x) &= \mathrm{lcm}\left(M^{(1)}(x), M^{(2)}(x), \cdots, M^{(6)}(x)\right) \\ &= M^{(1)}(x) \cdot M^{(3)}(x) \cdot M^{(5)}(x), \end{aligned}$$

where

$$\begin{aligned} M^{(1)}(x) &= (x - \alpha)\left(x - \alpha^2\right)\left(x - \alpha^4\right)\left(x - \alpha^8\right), \\ M^{(3)}(x) &= \left(x - \alpha^3\right)\left(x - \alpha^6\right)\left(x - \alpha^{12}\right)\left(x - \alpha^9\right), \\ M^{(5)}(x) &= \left(x - \alpha^5\right)\left(x - \alpha^{10}\right). \end{aligned}$$

[5]

iii From the previous part,

$$\begin{aligned} h(x) &= M^{(0)}(x) \cdot M^{(7)}(x), \\ q(x) &= 0, \end{aligned}$$

where

$$\begin{aligned} M^{(0)}(x) &= x - 1, \\ M^{(7)}(x) &= \left(x - \alpha^7\right)\left(x - \alpha^{14}\right)\left(x - \alpha^{13}\right)\left(x - \alpha^{11}\right). \end{aligned}$$

[2]

iv The generator and parity-check matrices are respectively given by

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_d & & & & \\ & g_0 & g_1 & \cdots & g_d & & & \\ & & \ddots & & & \ddots & & \\ & & & g_0 & g_1 & \cdots & g_d \end{bmatrix},$$

and

$$H = \begin{bmatrix} h_\ell & h_{\ell-1} & \cdots & h_0 & & & & \\ & h_\ell & h_{\ell-1} & \cdots & h_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & h_\ell & h_{\ell-1} & \cdots & h_0 \end{bmatrix}.$$

[3]

Solutions of Question 5.

(a) It is clear that $\mathcal{R}_1 = \mathbb{F}_2^2$ is a linear code.

Suppose that $\mathcal{R}_m$ is a linear code. We shall show $\mathcal{R}_{m+1}$ is linear by considering linear combinations of two codewords $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ from $\mathcal{R}_{m+1}$. Since the code is defined on $\mathbb{F}_2$, we only need to consider the linear combination of the form $\boldsymbol{c}_1 + \boldsymbol{c}_2$.

If $\boldsymbol{c}_1 = [\boldsymbol{u}_1,\ \boldsymbol{u}_1]$ and $\boldsymbol{c}_2 = [\boldsymbol{u}_2,\ \boldsymbol{u}_2]$, then $\boldsymbol{c}_1 + \boldsymbol{c}_2 = [\boldsymbol{u}_1 + \boldsymbol{u}_2,\ \boldsymbol{u}_1 + \boldsymbol{u}_2]$. By linearity of $\mathcal{R}_m$, $\boldsymbol{c}_1 + \boldsymbol{c}_2 \in \mathcal{R}_{m+1}$.

If $\boldsymbol{c}_1 = [\boldsymbol{u}_1,\ \boldsymbol{u}_1 + \mathbf{1}]$ and $\boldsymbol{c}_2 = [\boldsymbol{u}_2,\ \boldsymbol{u}_2 + \mathbf{1}]$, then $\boldsymbol{c}_1 + \boldsymbol{c}_2 = [\boldsymbol{u}_1 + \boldsymbol{u}_2,\ \boldsymbol{u}_1 + \boldsymbol{u}_2] \in \mathcal{R}_{m+1}$.

If $\boldsymbol{c}_1 = [\boldsymbol{u}_1,\ \boldsymbol{u}_1]$ and $\boldsymbol{c}_2 = [\boldsymbol{u}_2,\ \boldsymbol{u}_2 + \mathbf{1}]$, then $\boldsymbol{c}_1 + \boldsymbol{c}_2 = [\boldsymbol{u}_1 + \boldsymbol{u}_2,\ \boldsymbol{u}_1 + \boldsymbol{u}_2 + \mathbf{1}]$, which is also in $\mathcal{R}_{m+1}$ by the definition of $\mathcal{R}_{m+1}$. The same is true if $\boldsymbol{c}_1 = [\boldsymbol{u}_1,\ \boldsymbol{u}_1 + \mathbf{1}]$ and $\boldsymbol{c}_2 = [\boldsymbol{u}_2,\ \boldsymbol{u}_2]$.

This finishes the proof. [5]

(b) It is straightforward to verify that

$$G_{m+1} = \begin{bmatrix} G_m & G_m \\ \mathbf{0} & \mathbf{1} \end{bmatrix},$$

where $\mathbf{0}$ is the all zero vector and $\mathbf{1}$ is the all one vector. [4]

(c) It is clear that for $\mathcal{G}_m$, $n = 2^m$ and $k = m + 1$. [3]

(d) We prove this part by mathematical induction.

When $m = 1$, $\mathcal{R}_m$ contains $\mathbf{0}$ and $\mathbf{1}$. All other codewords have weight $2^{m-1} = 1$.

Suppose that the claim is true for $\mathcal{R}_m$. We consider the code $\mathcal{R}_{m+1}$.

- Consider the codeword of the form $[\boldsymbol{u},\ \boldsymbol{u}]$ where $\boldsymbol{u} \in \mathcal{R}_m$. Clearly $\boldsymbol{u} = \mathbf{0}$ gives the all zero vector in $\mathcal{R}_{m+1}$ and $\boldsymbol{u} = \mathbf{1}$ gives the all one vector in $\mathcal{R}_{m+1}$.
  When $\boldsymbol{u}$ is neither $\mathbf{0}$ nor $\mathbf{1}$, weight $(\boldsymbol{u}) = 2^{m-1}$ and hence weight $([\boldsymbol{u},\ \boldsymbol{u}]) = 2^m = 2^{(m+1)-1}$.
- Consider the codeword of the form $[\boldsymbol{u},\ \boldsymbol{u} + \mathbf{1}]$ where $\boldsymbol{u} \in \mathcal{R}_m$. One has weight $([\boldsymbol{u},\ \boldsymbol{u} + \mathbf{1}]) = \text{weight}\,(\boldsymbol{u}) + (2^m - \text{weight}\,(\boldsymbol{u})) = 2^m$.

This proves the claimed result. [8]