

EEEL-07

Solution of Question 1.

(a)

i It is straightforward to compute that

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

As a result,

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

[4]

ii According to the previous part, it is clear that

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

Multiply both sides with 2. It holds that

$$1 = x(x^3 + x^2 + 2) + (2x^2 + 2x + 2)(x^2 + 2).$$

As a result,

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

[4]

(b) By Bézout's identity, there exist $a, b \in \mathbb{Z}$ such that $1 = ar_1 + br_2$. Multiply both sides by r . One obtains that $r = ar_1r + br_2r$. By assumption $r_1 \mid (r_2r)$, it is clear that r_1 divides the right hand side of the equation. Hence $r_1 \mid r$. [2]

(c) Since $f(x) = (x + 1)(x + 1)$, $f(x)$ is reducible. [2]

(d) $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible. To justify it, one can try all possible polynomials $g(x)$ in $\mathbb{F}_3[x]$ of degree $0 < \deg(g) < 2$. As $f(x) = x \cdot x + 1$ and $f(x) = (x + 1)(x + 2) + 2$, we conclude that $f(x)$ is irreducible. [2]

(e)

- i Since f is irreducible, it holds that $\gcd(f, g) = 1$ for all $g \in \mathcal{R}$. By Bézout's identity, it holds that

$$1 = c(x)f(x) + d(x)g(x),$$

or $d(x)g(x) = 1 \bmod f(x)$. This proves the existence of g^{-1} . Hence \mathcal{R} is a field. [3]

- ii Suppose that $f(x)$ is reducible, i.e., there exist $g(x)$ and $h(x)$ such that $f(x) = g(x)h(x)$ and $1 \leq \deg(g(x)) < \deg(f(x))$ and $1 \leq \deg(h(x)) < \deg(f(x))$. Since \mathcal{R} is a field, $g^{-1}(x)$ exists. Hence $h(x) = (g^{-1}(x)g(x))h(x) = g^{-1}(x)f(x) = g^{-1}(x) \cdot 0 = 0 \bmod f(x)$. This contradicts that $1 \leq \deg(h(x))$. Hence $f(x)$ must be irreducible. [3]

Solutions of Question 2.

(a)

i Since $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$, one has $\text{ord}(3) = 6$. [2]

ii $\log_3 1 = 6, \log_3 2 = 2$, and $\log_3 3 = 1$. [2]

iii Since $2^1 = 2, 2^2 = 4, 2^3 = 1$, one has $\text{ord}(2) = 3$. [2]

iv $\log_2 1 = 3, \log_2 2 = 1$, and $\log_2 3$ does not exist. [2]

v Suppose that there exist x_1, x_2 such that $0 \leq x_1 < x_2 \leq p-1$ and $b^{x_1} = b^{x_2}$. Then $b^{x_2}/b^{x_1} = b^{x_2-x_1} = 1$ which suggests that $\text{ord}(b) \leq x_2 - x_1 < p-1$. This contradicts the definition of a primitive element b . The claim is therefore proved. [2]

vi The base b should be a primitive element. Suppose that b is not a primitive element. Then the set $\mathcal{B} = \{b^1, b^2, \dots\}$ contains only $\text{ord}(b)$ many elements with $\text{ord}(b) < p-1$. This means that for some element $y \in \mathbb{F}_p^*$, $\log_b y$ is not well defined. [2]

(b) Alice would like to store (i, b^{x_i}) on the server. [2]

(c)

i At least k pairs are needed. [2]

ii The linear system is given by

$$[a_0, a_1, \dots, a_{k-1}] \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_{i_1} & t_{i_2} & \dots & t_{i_\ell} \\ \vdots & \vdots & \ddots & \vdots \\ t_{i_1}^{k-1} & t_{i_2}^{k-1} & \dots & t_{i_\ell}^{k-1} \end{bmatrix} = [f(t_{i_1}), f(t_{i_2}), \dots, f(t_{i_\ell})].$$

[2]

iii When $\ell = k$, the matrix M is a Vandermonde matrix and hence its inverse exists. The vector \mathbf{a} can be obtained from $\mathbf{a} = \mathbf{f}M^{-1}$. When $\ell < k$, the number of equations is less than the number of unknowns. The solution of this linear system is not unique. [2]

Solutions of Question 3.

(a)

$$d(C) = \min_{c \in C, c \neq 0} \text{weight}(c). \quad [2]$$

(b) $d(C)$ is the minimum number of linearly dependent columns of H , i.e.,
 $d = \text{spark}(H).$ [2]

(c)

i By Gaussian elimination, it is clear that

$$G' = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \quad [2]$$

ii

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

iii The syndrome vector is given by

$$s_1 = y_1 H^T = [1 \ 0 \ 0].$$

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

iv The syndrome vector is given by

$$[1 \ 0 \ 0 \ 0 \ 0 \ 1] H^T = [1 \ 1 \ 1].$$

Let c_2 and c_4 be the 2nd and 4th symbols in c . Then one has

$$[c_2 \ c_4] \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [1 \ 1 \ 1].$$

It is clear that $[c_2 \ c_4] = [0 \ 1]$. Hence $c = [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]$ and $m =$

$$[1\ 0\ 0\ 1]. \quad [3]$$

(d)

i $n_2 = 8$. [1]

ii $k_2 = 4$. The dimension of \mathcal{C}_2 is the same as that of \mathcal{C} because there is one-to-one mapping between the codewords in \mathcal{C} and those in \mathcal{C}_2 . [1]

iii

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}. \quad [2]$$

iv $d(\mathcal{C}_2) = 4$. For any $\mathbf{c} \in \mathcal{C}$, let $\mathbf{c}_2 \in \mathcal{C}_2$ be the corresponding codeword of which the first seven bits are given by \mathbf{c} . That $d(\mathcal{C}_2) = 4$ can be obtained by observing that

- $\mathbf{c} = \mathbf{0} \Rightarrow \mathbf{c}_2 = \mathbf{0}$.
- $\text{wt}(\mathbf{c}) = 3 \Rightarrow \text{wt}(\mathbf{c}_2) = 4$.
- $\text{wt}(\mathbf{c}) \geq 3$, for all $\mathbf{c} \in \mathcal{C}$ and $\mathbf{c} \neq \mathbf{0} \Rightarrow \text{wt}(\mathbf{c}_2) \geq 4$ for all $\mathbf{c}_2 \in \mathcal{C}_2$ and $\mathbf{c}_2 \neq \mathbf{0}$. [2]

Solutions of Question 4.

(a) The parity-check matrix $H \in \mathbb{F}^{(n-k) \times n}$ contains $n - k$ rows. Every $n - k + 1$ columns must be linearly dependent. Hence $d \leq n - k + 1$. [3]

(b)

i Let $c_1 = \text{eval}(f_1)$ and $c_2 = \text{eval}(f_2)$ where $\deg(f_1) \leq k - 1$ and $\deg(f_2) \leq k - 1$. Then $\alpha c_1 + \beta c_2 = \text{eval}(g)$ with $g = \alpha f_1 + \beta f_2$. Since $\deg(g) \leq k - 1$, $\text{eval}(g) \in \mathcal{C}$. [3]

ii A polynomial of degree $k - 1$ can have at most $k - 1$ zeros. Hence, $\forall c \in \mathcal{C}$ s.t. $c \neq 0$, $c = \text{eval}(f)$ has weight at least $n - k + 1$. [3]

(c)

i $C_0 = \{0\}$, $C_1 = C_3 = \{1, 3, 9\}$, $C_2 = C_6 = \{2, 6, 18\}$, $C_4 = \{4, 12, 10\}$, $C_5 = \{5, 15, 19\}$, $C_7 = \{7, 21, 11\}$, $C_8 = \{8, 24, 20\}$. [4]

ii

A. $\deg(g) = |C_1| + |C_2| + |C_4| + |C_5| + |C_7| + |C_8| = 18$. [2]

B. $k = n - \deg(g) = 26 - 18 = 8$. [2]

C. $d \geq 13$. Note that $\alpha^1, \alpha^2, \dots, \alpha^{12}$ are roots of $g(x)$. For any code $c \in \mathcal{C}$, all the roots of $g(x)$ are the roots of the corresponding generating function $c(x)$. One has

$$\underbrace{\begin{bmatrix} 1 & \alpha & \dots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{12} & \dots & \alpha^{12(n-1)} \end{bmatrix}}_A \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = 0.$$

Since every 12-column sub-matrix of A is a Vandermonde matrix and has full column rank, $d(\mathcal{C}) \geq 12 + 1 = 13$. [3]

Solutions of Question 5.

(a)

i $p_Y(0) = p_Y(1) = \frac{1}{2}(1-p)$ and $p_Y(?) = p$. [3]

ii It is clear that $H(X|0) = H(X|1) = 0$ and $H(X|?) = 1$. [2]

iii Since $H(X|Y) = p$, $I(X;Y) = 1 - p$. [2]

(b)

i $p_{Y_1Y_2}(00) = p_{Y_1Y_2}(01) = p_{Y_1Y_2}(10) = p_{Y_1Y_2}(11) = \frac{1}{4}(1-p)^2$.
 $p_{Y_1Y_2}(?0) = p_{Y_1Y_2}(?1) = \frac{1}{2}p(1-p)$.
 $p_{Y_1Y_2}(0?) = p_{Y_1Y_2}(1?) = \frac{1}{2}p(1-p)$.
 $p_{Y_1Y_2}(??) = p^2$. [3]

ii If neither y_1 nor y_2 is ?, then we can identify u_2 and u_1 uniquely. Hence

$$H(U_1|00) = H(U_1|01) = H(U_1|10) = H(U_1|11) = 0.$$

If either y_1 or y_2 is ?, U_1 has equal probability to be 0 or 1. Hence

$$H(U_1|?0) = H(U_1|?1) = H(U_1|0?) = H(U_1|1?) = H(U_1|??) = 1. [3]$$

iii Since $H(U_1|Y_1Y_2) = 2p - p^2$, $I(U_1;Y_1Y_2) = 1 - 2p + p^2$. [2]

iv If $y_2 \neq ?$, then u_2 is uniquely identified. Hence $H(U_2|y_1y_2u_1) = 0$ if $y_2 \neq ?$.

If $y_2 = ?$ but $y_1 \neq ?$, we are still able to find u_2 via $y_1 = u_1 + u_2$. Hence

$$H(U_2|y_1?u_1) = 0 \text{ when } y_1u_1 \in \{0, 1\}^2.$$

If $y_1 = y_2 = ?$, $H(U_2|??u_1) = 1$. [3]

v Since $H(U_2|Y_1Y_2U_1) = p^2$, $I(U_2;Y_1Y_2U_1) = 1 - p^2$. [2]