EE4-07

Solution of Question 1.

(a)

i It is straightforward to compute that

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

As a result,

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

[4]

ii According to the previous part, it is clear that

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

Multiply both sides with 2. It holds that

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

As a result,

$$a(x) = x,$$
$$b(x) = 2x^2 + 2x + 2.$$

[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 $r = ar_1 r + br_2 r$. By assumption $r_1 | (r_2 r)$, it is clear that r_1 divides the right hand side of the equation. Hence $r_1 | r$. [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, $g^{-1}(x)$ exits. 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 $0 \le x_1 < x_2 \le p-1$ and $b^{x_1} = b^{x_2}$. Then $b^{x_2}/b^{x_1} = b^{x_2-x_1} = 1$ which suggests that $\text{ord}(b) \le x_2 - x_1 < p-1$. 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 $\mathcal{B} = \{b^1, b^2, \cdots\}$ 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

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

[2]

iii When $\ell = k$, the matrix $\boldsymbol{M}$ is a Vandermonde matrix and hence its inverse exists. The vector $\boldsymbol{a}$ can be obtained from $\boldsymbol{a} = \boldsymbol{f}\boldsymbol{M}^{-1}$. 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)

$$d(\mathcal{C}) = \min_{\boldsymbol{c}\in\mathcal{C},\ \boldsymbol{c}\neq\boldsymbol{0}} \text{weight}(\boldsymbol{c}).$$

[2]

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

(c)

i By Gaussian elimination, it is clear that

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

[2]

ii

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

[2]

iii The syndrome vector is given by

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

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

iv The syndrome vector is given by

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

Let c_2 and c_4 be the 2nd and 4th symbols in $\boldsymbol{c}$. 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 $\boldsymbol{c} = [1\ 0\ 0\ 1\ 0\ 0\ 1]$ and $\boldsymbol{m} =$

[1 0 0 1]. [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

$$\boldsymbol{G}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

[2]

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

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

Solutions of Question 4.

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

(b)

i Let $\boldsymbol{c}_1 = \text{eval}(f_1)$ and $\boldsymbol{c}_2 = \text{eval}(f_2)$ where $\deg(f_1) \le k-1$ and $\deg(f_2) \le k-1$. Then $\alpha\boldsymbol{c}_1 + \beta\boldsymbol{c}_2 = \text{eval}(g)$ with $g = \alpha f_1 + \beta f_2$. Since $\deg(g) \le k-1$, $\text{eval}(g) \in \mathcal{C}$. [3]

ii A polynomial of degree $k-1$ can have at most $k-1$ zeros. Hence, $\forall \boldsymbol{c} \in \mathcal{C}$ s.t. $\boldsymbol{c} \neq 0$, $\boldsymbol{c} = \text{eval}(f)$ 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. $d \ge 13$. Note that $\alpha^1, \alpha^2, \cdots, \alpha^{12}$ are roots of $g(x)$. For any code $\boldsymbol{c} \in \mathcal{C}$, all the roots of $g(x)$ are the roots of the corresponding generating function $c(x)$. One has

$$\underbrace{\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{12} & \cdots & \alpha^{12(n-1)} \end{bmatrix}}_{\boldsymbol{A}} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \mathbf{0}.$$

Since every 12-column sub-matrix of $\boldsymbol{A}$ is a Vandermonde matrix and has full column rank, $d(\mathcal{C}) \ge 12 + 1 = 13$. [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 $H(U_2|y_1?u_1) = 0$ 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]