

## Solution of Question 1.

(a)

i In  $\mathbb{F}_2[x]$ ,  $x^2 + 1 = (x + 1)(x + 1)$ . Hence  $x^2 + 1 \in \mathbb{F}_2[x]$  is not irreducible. [2]

ii It is clear that  $x \nmid (x^2 + 1)$ . Further in  $\mathbb{F}_3[x]$ ,  
 $x^2 + 1 = (x + 1)(x + 2) + 2$  which implies  $(x + 1) \nmid (x^2 + 1)$  and  
 $(x + 2) \nmid (x^2 + 1)$ . Therefore  $x^2 + 1 \in \mathbb{F}_3[x]$  is irreducible. [2]

iii In  $\mathbb{F}_5[x]$ ,  $x^2 + 1 = (x + 2)(x + 3)$ . Hence  $x^2 + 1 \in \mathbb{F}_5[x]$  is not irreducible. [2]

(b)

i It is straightforward to compute that

$$\begin{aligned} x^3 + x + 1 &= (x + 4)(x^2 + x + 1) + x + 2, \\ x^2 + x + 1 &= (x + 4) \cdot (x + 2) + 3. \end{aligned}$$

As a result,

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

[3]

ii According to the previous part, it is clear that

$$\begin{aligned} 3 &= (x^2 + x + 1) - (x + 4)(x + 2) \\ &= (x^2 + x + 1) - (x + 4)((x^3 + x + 1) - (x + 4)(x^2 + x + 1)) \\ &= ((x + 4)^2 + 1)(x^2 + x + 1) + (4x + 1)(x^3 + x + 1) \\ &= (x^2 + 3x + 2)(x^2 + x + 1) + (4x + 1)(x^3 + x + 1) \end{aligned}$$

Multiply both sides with 2. It holds that

$$1 = (2x^2 + x + 4)(x^2 + x + 1) + (3x + 2)(x^3 + x + 1)$$

As a result,

$$\begin{aligned} a(x) &= 3x + 2, \\ b(x) &= 2x^2 + x + 4. \end{aligned}$$

[4]

(c)

i  $x^3 + x \equiv x^9$  and hence  $\text{ord}(x^3 + x) = \text{ord}(x^9) = 5$ .

(15  $\nmid$  9, 15  $\nmid$  18, 15  $\nmid$  27, 15  $\nmid$  36, 15  $\nmid$  45). [2]

ii  $x^2 + x + 1 \equiv x^{10}$  and hence  $\text{ord}(x^2 + x + 1) = 3$ . [2]

iii  $(x^3 + x)(x^2 + x + 1) = x^9 \cdot x^{10} = x^4$  and  $\text{ord}(x^4) = 15$ . Another way to see it is as follows. Since  $\text{gcd}(3, 5) = 1$ ,  $\text{ord}((x^3 + x)(x^2 + x + 1)) = \text{ord}(x^3 + x) \cdot \text{ord}(x^2 + x + 1) = 15$ . [3]

## Solutions of Question 2.

(a)

- i  $2^x = 2, 4, 8, 5, 10, 9, 7, 3, 6, 1$  when  $x = 1, 2, 3, \dots$ . Hence  $\text{ord}(2) = 10$  and 2 is a primitive element. [2]
- ii  $3^x = 3, 9, 5, 4, 1$  when  $x = 1, 2, 3, \dots$ . Hence  $\text{ord}(3) = 5$ . [2]
- iii  $\log_2 y = 1, 8, 2, 4$  when  $y = 2, 3, 4, 5$  respectively. [2]
- iv  $\log_3 y = \text{"not defined"}, 1, 4, 3$  when  $y = 2, 3, 4, 5$  respectively. [2]

(b)

- i (Book work) The complexity of computing  $b^x \bmod p$  is upper bounded by  $O(\log_2 p)$ . Decompose  $x$  into  $x = b_k 2^k + b_{k-1} 2^{k-1} + \dots + b_1 2^1 + b_0$ ,  $b_i \in \{0, 1\}$ . The binary string  $b_k b_{k-1} \dots b_0$  is actually a binary representation of  $x$ . With this binary representation, at most  $O(\log_2 p)$  operations are needed to compute  $b^x \bmod p$ : first compute  $b^1 = b$ ,  $b^2 = b \cdot b$ ,  $\dots$ ,  $b^{2^k} = b^{2^{k-1}} \cdot b^{2^{k-1}} \pmod{p}$  and then evaluate  $b^x = (b^{2^k})^{b_k} \cdot (b^{2^{k-1}})^{b_{k-1}} \dots b^{b_1} \cdot b^{b_0}$ . [3]
- ii (Book work) The complexity of computing  $\log_b y \bmod p$  is  $O(p)$ . This is because generally speaking the discrete logarithmic function can be only solved by exhaustive search. [1]

(c) The plain text is given as

A PICTURE IS WORTH A THOUSAND WORDS

The puzzle can be solved by an educated guess that  $G$  stands for  $A$ . [4]

(d)

- i (Book work) Alice computes  $ma^t \cdot (b^t)^{-a'} = m \bmod p$ . [2]
- ii ElGamal cryptography is much safer than Caesar cipher. Caesar cipher can be easily broken by frequency analysis. By introducing randomness, ElGamal cryptography is immune to frequency analysis. [2]

### Solutions of Question 3.

(a)

i It is straightforward to obtain

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

[2]

ii The generator matrix is given by

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

[2]

iii The syndrome vector is given by

$$\mathbf{s}_1 = \mathbf{y}_1 \mathbf{H}^T = [1 \ 1 \ 0],$$

hence

$$\hat{\mathbf{c}}_1 = [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1],$$

and

$$\hat{\mathbf{m}}_1 = [1 \ 0 \ 0 \ 1].$$

[3]

iv The syndrome vector is given by

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

Let  $c_1$  and  $c_5$  be the 1st and 5th symbols in  $\mathbf{c}$ . Then one has

$$[c_1 \ c_5] \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} = [1 \ 1 \ 0].$$

It is clear that  $[c_1 \ c_5] = [0 \ 1]$ . Hence  $\mathbf{c} = [0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0]$  and  $\mathbf{m} = [1 \ 1 \ 1 \ 0]$ .

[3]

(b)

i (Book work) Let  $t = \lfloor \frac{d-1}{2} \rfloor$ . The number of codewords is upper bounded by

$$M \leq q^n / \left( \sum_{i=0}^t \binom{n}{i} (q-1)^i \right). \quad [2]$$

ii The distance of the code in Part (a) is 3: this can be verified by that every two columns of  $\mathbf{H}$  are linear independent and there exists three columns of  $\mathbf{H}$  that are linearly dependent (for example columns 1,2, and 5). Therefore  $t = 1$ .

As  $q = 2$ ,  $q^n / \left( \sum_{i=0}^t \binom{n}{i} (q-1)^i \right) = 2^7 / (1 + 7) = 2^4$ . At the same time, the number of codewords in  $\mathcal{C}$  is  $2^4$ . Hence the code is a perfect code. [3]

iii (Book work) Singleton bound: for a linear code  $\mathcal{C} [n, k, d]$  it holds that  $d \leq n - k + 1$ . To prove it, note that the parity matrix of the linear code  $\mathcal{C} [n, k, d]$  has dimension  $(n - k) \times n$ . As a result, the minimum number of linearly dependent columns is upper bounded by  $n - k + 1$  which gives the code distance. [3]

iv The code in Part (a) has distance 3 which is less than  $n - k + 1 = 7 - 4 + 1 = 4$ . Hence, it is not MDS. [2]

## Solutions of Question 4.

(a)

- i (Book work) For any  $\mathbf{m} = [m_0, m_2, \dots, m_{K-1}] \in \mathbb{F}_q^K$ , define the polynomial  $f_{\mathbf{m}} = \sum_{k=0}^{K-1} m_k x^k$ . According to the definition of the evaluation mapping, the generated codeword is given by  $\mathbf{c}$  with  $c_i = \sum_{k=0}^{K-1} m_k (\alpha^i)^k = \sum_{k=0}^{K-1} m_k (\alpha^k)^i$ . Note that the  $i$ -th element of  $\mathbf{mG}$  is given by  $\sum_{k=0}^{K-1} m_k (\alpha^k)^i$  and that  $\mathbf{mG} = \mathbf{c} = \text{evaluation}(f_{\mathbf{m}})$ . It can be concluded that the matrix  $\mathbf{G}$  is a generator matrix of Reed-Solomon codes. [3]
- ii (Book work) The  $(i, j)$ -th element of  $\mathbf{GH}^T$ ,  $1 \leq \ell \leq k$  and  $1 \leq j \leq n-k$ , is given by

$$\begin{aligned} \sum_{\ell=0}^{n-1} \alpha^{(i-1)\ell} \alpha^{j\ell} &= \sum_{\ell=0}^{n-1} \alpha^{(i+j-1)\ell} = \frac{\alpha^{(i+j-1)n} - 1}{\alpha^{i+j-1} - 1} \\ &= \frac{1 - 1}{\alpha^{i+j-1} - 1} = 0, \end{aligned}$$

as  $\alpha^n = \alpha^{q-1} = 1$  by Fermat's little theorem. Hence  $\mathbf{GH}^T = \mathbf{0}$ . [3]

- iii (Book work) By definition  $\mathbf{s} = \mathbf{yH}^T = \mathbf{eH}^T$ , it holds that

$$s_j = \sum_{i=0}^{n-1} e_i \alpha^{i(j+1)} = \sum_{i \in \mathcal{I}} e_i \alpha^{i(j+1)}, \quad j = 0, 1, \dots, n-k-1.$$

Hence

[2/5]

$$\begin{aligned} S(z) &= \sum_{j=0}^{n-k-1} s_j z^j = \sum_{j=0}^{n-k-1} \sum_{i \in \mathcal{I}} e_i \alpha^{i(j+1)} z^j \\ &= \sum_{i \in \mathcal{I}} e_i \alpha^i \left( \sum_{j=0}^{n-k-1} (\alpha^i z)^j \right) \\ &\equiv \sum_{i \in \mathcal{I}} e_i \alpha^i \left( \sum_{j=0}^{\infty} (\alpha^i z)^j \right) \pmod{z^{n-k}} \\ &= \sum_{i \in \mathcal{I}} e_i \alpha^i \frac{1}{1 - \alpha^i z} \pmod{z^{n-k}}. \end{aligned}$$

[3/5]

- iv The key equation is given by

$$E(z) = L(z) S(z) \pmod{z^{n-k}}.$$

[2]

- (b) In order to have  $\alpha, \alpha^2, \dots, \alpha^6$  as roots of the generator polynomial  $g(x)$ , one can choose

$$g(x) = \prod_{i=1}^6 M^{(i)}(x).$$

The needed cyclotomic cosets are  $C_1 = \{1, 2, 4, 8, 16\}$ ,  $C_3 = \{3, 6, 12, 24, 17\}$ , [1/7]  
and  $C_5 = \{5, 10, 20, 9, 18\}$ , from which the minimal polynomials can be  
constructed accordingly. Hence the generator polynomial is given by [3/7]

$$\begin{aligned} g(x) &= M^{(1)}(x) M^{(3)}(x) M^{(5)}(x) \\ &= \prod_{i \in C_1} (x - \alpha^i) \prod_{i \in C_3} (x - \alpha^i) \prod_{i \in C_5} (x - \alpha^i). \end{aligned}$$

The degree of  $g(x)$  is 15. The dimension  $k$  of the constructed BCH code is given by  $k = n - \deg(g(x)) = 31 - 15 = 16$ . In the end, one constructs a BCH code with parameters  $[31, 16]$  and  $d \geq 7$ . [3/7]

Additional comments: One way to figure out the dimension  $k$  is as follows. Since the codeword length is  $n = 31$ , every codeword can be described by a polynomial of degree 30. The degree of the generator polynomial is 15. This suggests every codeword can be written as  $c(x) = m(x) \cdot g(x)$  with  $\deg(m(x)) \leq 15$ . A polynomial of degree 15 can be written as  $\sum_{i=0}^{15} a_i x^i$  which has 16 parameters. Hence the dimension of the constructed BCH code has dimension 16.

## Solutions of Question 5.

(a)

$$G_3 = \begin{bmatrix} G_2 & 0 \\ G_2 & G_2 \end{bmatrix}, \quad \text{where } G_2 = \begin{bmatrix} G_1 & 0 \\ G_1 & G_1 \end{bmatrix}.$$

Or more specifically

$$G_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

[3]

(b)  $I'_1 = I'_5 = 0.4096$ ,  $I'_2 = I'_6 = 0.9216$ ,  $I'_3 = I'_7 = 0.8704$ , and  $I'_4 = I'_8 = 0.9984$ .

As an example, we compute  $I'_1$  and  $I'_3$ . Since  $I''_1 = I''_3 = 0.64$ , the equivalent model is that  $U'_1$  and  $U'_3$  are the input of the basic building block of polar codes with a BEC channel of which the erasure probability is  $p' = 1 - 0.64 = 0.36$ . Hence  $I'_1 = 1 - 2p' + (p')^2 = 0.4096$  and  $I'_3 = 1 - (p')^2 = 0.8704$ .

[5]

(c) Since  $K = 5$ , we shall set  $U_1$ ,  $U_3$  and  $U_5$  to zero and use other  $U_i$ 's for encoding. Hence the generator matrix is given by

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

[4]



(d) Start with the initial matrix presentation and go backward. One obtains

$U$	$U'$	$U''$	$X$
?	?	1	1
?	?	0	0
?	?	?	0
?	?	?	?
0	0	1	1
0	0	0	0
1	1	1	1
0	0	0	0

Use the prior knowledge that  $U_1 = U_3 = 0$  (That  $U_5 = 0$  has been established.) and go forward. It can be verified that [4/8]

$U$	$U'$	$U''$	$X$
0	0	1	1
?	?	0	0
0	1	1	0
?	?	1	0
0	0	1	1
0	0	0	0
1	1	1	1
0	0	0	0

Go backward once more. It can be obtained that [2/8]

$U$	$U'$	$U''$	$X$
0	0	1	1
1	1	0	0
0	1	1	0
1	1	1	0
0	0	1	1
0	0	0	0
1	1	1	1
0	0	0	0

Hence, the transmitted codeword is given by [1 0 0 0 1 0 1 0] and the mes- [1/8]

sage  $\mathbf{m} = [U_2 \ U_4 \ U_6 \ U_7 \ U_8]$  is given by  $[1 \ 1 \ 0 \ 1 \ 0]$ .

[1/8]