Final copy

EE4-07
EE9SO11

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2011

MSc and EEE/ISE PART IV: MEng and ACGI

CODING THEORY

Tuesday, 3 May 2:30 pm

Time allowed: 3:00 hours

There are SIX questions on this paper.

Answer FOUR questions.

All questions carry equal marks

Any special instructions for invigilators and information for candidates are on page 1.

Examiners responsible First Marker(s) : W. Kim
Second Marker(s) : C. Ling

INFORMATION FOR CANDIDATES

Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$ be a field with 2^4 elements with primitive element α. We identify $(a,b,c,d) \in \mathbb{B}^4$ with $a\alpha^3 + b\alpha^2 + c\alpha + d \in F$.

0	1	α	α^2	α^3	α^4	α^5	α^6
0000	0001	0010	0100	1000	0011	0110	1100
α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1011	0101	1010	0111	1110	1111	1101	1001

The following table is for addition of α^r and α^s in $F = \mathrm{GF}(2^4)$. In order to find $\alpha^6 + \alpha^4$, look up the intersection of the column of 6 row and the row of 4, which reads 12. This shows $\alpha^6 + \alpha^4 = \alpha^{12}$.

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	*	4	8	14	1	10	13	9	2	7	5	12	11	6	3
1	4	*	5	9	0	2	11	14	10	3	8	6	13	12	7
2	8	5	*	6	10	1	3	12	0	11	4	9	7	14	13
3	14	9	6	*	7	11	2	4	13	1	12	5	10	8	0
4	1	0	10	7	*	8	12	3	5	14	2	13	6	11	9
5	10	2	1	11	8	*	9	13	4	6	0	3	14	7	12
6	13	11	3	2	12	9	*	10	14	5	7	1	4	0	8
7	9	14	12	4	3	13	10	*	11	0	6	8	2	5	1
8	2	10	0	13	5	4	14	11	*	12	1	7	9	3	6
9	7	3	11	1	14	6	5	0	12	*	13	2	8	10	4
10	5	8	4	12	2	0	7	6	1	13	*	14	3	9	11
11	12	6	9	5	13	3	1	8	7	2	14	*	0	4	10
12	11	13	7	10	6	14	4	2	9	8	3	0	*	1	5
13	6	12	14	8	11	7	0	5	3	10	9	4	1	*	2
14	3	7	13	0	9	12	8	1	6	4	11	10	5	2	*

1. a) Let Ham(3) be the code defined by the following check matrix:

$$H_3 := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

i) Find the dimension of Ham(3), and write down the generator matrix in standard form. [5]

ii) Assume that you have received the following message $v := (1010101)$ encoded via Ham(3). Determine whether v is a Ham(3)-codeword. If not, then find the most plausible correction of v. (Show your working for full marks.) [5]

b) Let $k \geqslant 3$ be an integer.

i) Define Ham(k). (Make sure to specify the block size of the code; i.e., how many binary bits form a codeword.) [5]

ii) Express the dimension of Ham(k) in terms of k. (Show your Show your working for full marks.) [3]

iii) Find the minimal distance of Ham(k). (Show your working for full marks.) [7]

2. Let $F := \mathrm{GF}(q)$ for some $q := 2^k$, and fix a primitive element $\alpha \in F$. We identify, as usual, a vector $(a_{k-1}, \cdots, a_0) \in \mathbb{B}^k$ with $a_{k-1}\alpha^{k-1} + \cdots + a_0 \in F$. *If you present a correct solution for the case when $F = \mathbb{B}$, you will receive half of the full credit.*

The *weight* of a vector $v = (v_1, \cdots, v_n) \in F^n$ is defined to be the number of non-zero v_i's. For $v, w \in F^n$, we define the distance $d(v,w)$ to be the weight of $v - w$.

Finally, for any $s \times r$ matrix M with entries in F, we also denote by $M : F^r \to F^s$ the F-linear map defined by the multiplication of M. Let I_m denote the $m \times m$ identity matrix (i.e., the diagonal matrix with all diagonal entries equal to 1).

a) For an F-linear code $C \subset F^n$, let $d(C)$ denote the minimal distance of C.

i) Show that C can *detect* all weight r errors if and only if $d(C) > r$. [4]

ii) Show that C can *correct* all weight r errors if and only if $d(C) > 2r$. [6]

b) Let $C \subset F^n$ be an F-linear code.

i) For a positive integer r, define r-perfectness for a F-linear code $C \subset F^n$. [3]

ii) Let $C \subset F^n$ be an r-perfect F-linear code with F-dimension m. Find a relation satisfied by n, m, r, and $q = |F|$. (*Hint:* Count the number of elements in $D_r(v) := \{w \in F^n \mid d(v,w) \leqslant r\}$ for $v \in C$.) [7]

iii) Show that BCH$(4,2)$ is not 2-perfect as a $\mathbb{B}$-linear code. Similarly, show that RS$(4,2)$ is not 2-perfect as a GF(2^4)-linear code. You may use standard facts about BCH- and RS- codes without proof. [5]

3. Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. By the *minimal polynomial of* $\beta \in F$, we mean the minimal polynomial of β over $\mathbb{B}$.

a) Find the minimal polynomial of α, α^3, α^5, α^7, respectively. (Show your working for full marks.) [10]

b) Factorise $X^{15} - 1 \in \mathbb{B}[X]$ into irreducible polynomials in $\mathbb{B}[X]$. [5]

c) Find (i) a generator polynomial, (ii) a check polynomial, and (iii) the binary dimension of the code, for each of BCH(4,2), BCH(4,3), and BCH(4,4). (You do *not* need to expand or simplify the answer, but for full marks your answer should *not* have a denominator.) [5]

d) Find the minimal distances of BCH(4,2), BCH(4,3), and BCH(4,4), respectively. [5]

4. Let F be a field with 2^k elements for some k. Note that F naturally contains a copy of $\mathbb{B}$. The aim of this problem is to factorise the minimal polynomial of $\beta \in F$ over $\mathbb{B}$ into linear factors with coefficients in F.

a) Let $f(t_1, \cdots, t_m)$ be a multi-variable polynomial in $t_1, \cdots, t_m$ with coefficients in $\mathbb{B}$; i.e.,

$$f(t_1, \cdots, t_m) = \sum_{r_1, \cdots, r_m = 0}^{n} c_{r_1, \cdots, r_m} t_1^{r_1} \cdots t_m^{r_m}$$

for some $c_{r_1, \cdots, r_m} \in \mathbb{B}$ and some non-negative integer n. Then for any $\beta_1, \cdots, \beta_m \in F$, show that $f(\beta_1^2, \cdots, \beta_m^2) = (f(\beta_1, \cdots, \beta_m))^2$. [3]

b) Let $\beta_1, \cdots, \beta_m \in F$, and let $a_0, \cdots, a_{m-1} \in F$ be such that

$$(X - \beta_1) \cdots (X - \beta_m) = X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0.$$

Show that $(X - \beta_1^2) \cdots (X - \beta_m^2) = X^m + a_{m-1}^2 X^{m-1} + \cdots + a_1^2 X + a_0^2$.
(*Hint*: Viewing a_i's as functions of β_j's, explain why one can apply a) to a_i's.)
[5]

c) Let $\beta \in F$, and let m be the smallest positive integer such that $\beta^{2^m} = \beta$. Show that (i) such m exists, and (ii) β^{2^j} are pairwise distinct for $j = 0, \cdots, m-1$.
[4]

d) Let β and m be as in c), and set $f_\beta(X) := \prod_{j=1}^{m} (X - \beta^{2^{j-1}})$. Then show that $f_\beta(X) \in \mathbb{B}[X]$; i.e., using the notation as in b), show that if $\beta_j = \beta^{2^{j-1}}$ then $a_i \in \mathbb{B}$ for all $i = 0, \cdots, m-1$. (*Hint*: Use b).) [5]

e) Show that $f_\beta(X)$, defined in d), is the minimal polynomial of β. [5]

f) Now let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$, and consider the BCH-codes BCH(4,2) and BCH(4,3) constructed using $\alpha \in F$ as a chosen primitive element. Express the generator polynomials of BCH(4,2) and BCH(4,3), respectively, as products of linear polynomials with coefficients in F. [3]

5. Let F be a field with 2^k elements and let $\alpha \in F$ be a primitive element.

a) For an $(n-m) \times m$ matrix A with entries in F, let $G := \begin{pmatrix} I_m \\ -A \end{pmatrix}$ and $H := (A \; I_{n-m})$. Show that $\mathrm{im}(G) = \ker(H)$; i.e., the code defined by the generator matrix G is the same as the code defined by the check matrix H. [4]

b) Factorise $X^{2^k-1} - 1$ into linear factors with coefficients in F. [3]

c) For any integer $t < (2^k - 1)/2$ let $\mathrm{RS}(k,t)$ denote the Reed-Solomon code that is constructed using $\alpha \in F$ as a chosen primitive element. Answer the following questions. (You may take for granted all the standard results on Reed-Solomon codes covered in the lectures.)

i) How many symbols (i.e., elements of F) constitutes a block of $\mathrm{RS}(k,t)$-codeword? And how many binary bits constitutes a block of $\mathrm{RS}(k,t)$-codeword? [1]

ii) Write down the generator and check polynomials for $\mathrm{RS}(k,t)$, as products of linear polynomials with coefficients in F. [1]

iii) Find the F-dimension and $\mathbb{B}$-dimension, respectively, of $\mathrm{RS}(k,t)$. [1]

iv) How many error symbols in a single block can always be corrected? [1]

v) What is the maximal length of error bursts that can always be corrected? [1]

d) Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$, and let $\mathrm{RS}(4,5)$ denote the Reed-Solomon code that is constructed using $\alpha \in F$ as a chosen primitive element. A generator polynomial for $\mathrm{RS}(4,5)$ is

$$X^{10} + \alpha^2 X^9 + \alpha^3 X^8 + \alpha^9 X^7 + \alpha^6 X^6 + \alpha^{14} X^5 + \alpha^2 X^4 + \alpha X^3 + \alpha^6 X^2 + \alpha X + \alpha^{10}.$$

Find the generator and check matrices, respectively, for $\mathrm{RS}(4,5)$ *in standard form.* [13]

6. Let $F := \mathbb{B}[\alpha]/\alpha^4+\alpha+1$ be a field with 2^4 elements. Throughout this question RS$(4,3)$ is the Reed-Solomon code constructed using $\alpha \in F$ as a chosen primitive element. We view any vector $v = (v_{14}, \cdots, v_1, v_0) \in F^{15}$ as a polynomial $v(X) := v_{14}X^{14} + \cdots + v_1X + v_0 \in F[X]$.

Wansu is receiving a message consisting of one RS$(4,3)$-codeword.

a) Let $d(X)$ be the received word. Write down the formula for the corresponding syndrome polynomial $s(z)$. [3]

b) At the first attempt of transmission, Wansu received the following word:

$$d^{(1)}(X) = \alpha^{14}X^{14} + \alpha X^{13} + \alpha^2X^{12} + 0X^{11} + \alpha^2X^{10} + 0X^9 + \alpha^4X^8 + \alpha^2X^7 + 0X^6 + \alpha^6X^5 + \alpha^3X^4 + X^3 + \alpha^5X^2 + X + \alpha^9.$$

He computed the syndrome polynomial and obtained the following:

$$s^{(1)}(z) = 0z^5 + 0z^4 + 0z^3 + \alpha^5z^2 + \alpha^{14}z + \alpha^{13}.$$

i) Explain why you can conclude that an error has occurred during the first transmission. [2]

ii) Wansu tried to run the decoding algorithm to correct the error, but he failed. At which step does the algorithm fail to work? [5]

c) At the second attempt of transmission the signal faded before Wansu finished receiving the message, so he could not receive the last 4 binary bits. To run the decoding algorithm, he replaced the last 4 erased bits by 0 and set the following as the received message:

$$d^{(2)}(X) = \alpha^{14}X^{14} + \alpha X^{13} + \alpha^2X^{12} + \alpha^8X^{11} + \alpha^{12}X^{10} + \alpha^{12}X^9 + \alpha^5X^8 + \alpha^2X^7 + 0X^6 + \alpha^6X^5 + \alpha^3X^4 + X^3 + \alpha^{10}X^2 + \alpha^8X + 0$$

He computed the syndrome polynomial and obtained the following:

$$s^{(2)}(z) = 0z^5 + \alpha^5z^4 + \alpha^4z^3 + 0z^2 + \alpha^9z + \alpha^5.$$

i) Determine if the error has occurred. If so then run the decoding algorithm to find the corrected message (i.e., the transmitted codeword). Make sure to clearly label the error locator, the error evaluator, the error positions, and the error polynomial, as well. (You may set $s(z) := s^{(2)}(z)$ to simplify the notation.) [14]

ii) Let $c(X)$ denote the corrected message obtained in your solution of i). Assuming that $c(X)$ is equal to the originally transmitted message, find the error polynomial for the first received message; i.e., $d^{(1)}(X) - c(X)$. Explain in "practical" terms why the decoding algorithm failed to correct the first received message $d^{(1)}(X)$. [3]

Final Copy CE4-07 EE9S011

CODING THEORY: FINAL EXAM SOLUTION 2011

1. a) i) Note that $H_3 : \mathbb{B}^7 \to \mathbb{B}^3$ is surjective, because the standard basis for $\mathbb{B}^3$ is contained in the image of H_3; i.e., $H_3 \cdot e_5 = (100)$, $H_3 \cdot e_6 = (010)$, and $H_3 \cdot e_7 = (001)$. By rank-nullity theorem, therefore, we obtain that the dimension of Ham(3) is $7-3=4$.

By the relations between the generator and check matrices in standard form, the following matrix is the generator matrix in standard form:

$$G_3 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

[5]

ii) One can see that v is not a codeword beacuse $H_3 \cdot v = (110)$ is not zero. Since $H_3 \cdot e_3 = (110)$, we obtain that $H_3(v+e_3) = 0$; i.e., $v' := v + e_3$ is a Ham(3)-codeword. Since the minimal distance of Ham(3) is 3, v' is the nearest codeword to v. [5]

b) i) Let H_k be a $k \times (2^k - 1)$ matrix whose columns are all the non-zero vectors in $\mathbb{B}^k$. The code Ham(k) is the $\mathbb{B}$-linear code defined using H_k as a check matrix. (Equivalently, Ham(k) is the $\mathbb{B}$-linear subspace $\ker(H_k) \subset B^{2^k-1}$.) The block size is $2^k - 1$; i.e., $2^k - 1$ binary bits form a Ham(k)-codeword. [5]

ii) Note that $H_k : \mathbb{B}^{2^k-1} \to \mathbb{B}^k$ is surjective as all non-zero vectors of $\mathbb{B}^k$ appear as column vectors of H_k. So by rank-nullity theorem, the dimension of Ham(k) is $2^k - 1 - k$. [3]

iii) By construction of H_k, any two columns are distinct. On the other hand, one can find three columns that are linearly dependent; for example, $(1,0,0\cdots,0)^\top$, $(0,1,0,\cdots,0)^\top$, and $(1,1,0,\cdots,0)^\top$ are linearly dependent columns of H_3. So the minimal distance of Ham(k) is 3.

[7]

2. a) i) The "if" direction: Assume that $d(C) > r$. For $v, w \in F^n$ with $v \in C$ and $d(v,w) \leqslant r$, we clearly have $w \notin C$ because otherwise we obtain contradiction to our assumption $d(C) > r$.

The "only if" direction: Assume that there are $v, w \in C$ with $v \neq w$ and $d(v,w) \leqslant r$. Then w can be an error with weight $\leqslant r$ from v that cannot be detected. [4]

ii) The "if" direction: Assume $d(C) > 2r$, and let $v \in C$ and $w \in F^n$ be such that $d(v,w) = r$. We need to show $d(v',w) > r$ for any $v' \in C$ with $v' \neq v$. Assume, by contradiction, that there is $v' \in C$ with $v' \neq v$ such that $d(v',w) \leqslant r$. Then $d(v,v') \leqslant d(v,w) + d(v',w) \leqslant 2r$. But (since $v \neq v'$) this contradicts to our assumption on the minimal distance: $d(C) > 2r$.

The "only if" direction: Assume that there exist $v, v' \in C$ and $w \in F^n$ such that $d(v,w) \leqslant r$, $d(v',w) \leqslant r$, and $v \neq v'$. (In other words, we assume that there is an error with weight $\leqslant r$ that cannot be corrected.) Then by triangle inequality, we have $d(v,v') \leqslant d(v,w) + d(v',w) \leqslant 2r$. [6]

b) i) An F-linear code $C \subset F^n$ is called *r-perfect* if for any $w \in F^n$ there exists a unique codeword $v \in C$ such that $d(v,w) \leqslant r$. (Any equivalent definition will be accepted.) [3]

ii) The number of $w \in F^n$ with $d(w,v) = i$ is precisely $(q-1)^i \binom{n}{i}$; indeed, there are $\binom{n}{i}$ choices of i positions where symbols of v and w differ, and at each of the i positions there are $(q-1)$ symbols to choose from. Therefore, we obtain:

$$|D_r(v)| = \sum_{i=0}^{r} (q-1)^i \binom{n}{i} = 1 + (q-1)\binom{n}{1} + \cdots + (q-1)^r \binom{n}{r}.$$

Now observe that C is r-perfect if and only if $F^n = \bigcup_{v \in C} D_r(v)$ and $D_r(v) \cap D_r(v') = \emptyset$ for any distinct codewords $v, v' \in C$. So we obtain $|F^n| = \sum_{v \in C} |D_r(v)|$. Since $|F^n| = q^n$, $|C| = q^m$, and $|D_r(v)|$ does not depend on v, we obtain

$$q^n = q^m \cdot \sum_{i=0}^{r} (q-1)^i \binom{n}{i}.$$

Here, we set $\binom{n}{0} := 1$. [7]

iii) For BCH(4,2), we set $F = \mathbb{B}$ (so $q = 2$), $n = 15$, $m = 7$, and $r = 2$. If BCH(4,2) were 2-perfect, then $|D_2(v)|$ has to be some power of 2. On the other hand $|D_2(v)| = 1 + 15 + 15 \cdot 7$ is not even an even number.

For RS(4,2), we set $F = \mathrm{GF}(16)$ (so $q = 16$), $n = 15$, $m = 11$, and $r = 2$. If RS(4,2) were 2-perfect, then $|D_2(v)|$ has to be some power of 16. On the other hand $|D_2(v)| = 1 + 15 \cdot 15 + 15^2 \cdot (15 \cdot 7)$ is not even an even number. [5]

3. a) The minimal polynomial of α is X^4+X+1 because α is its zero by definition of $F := \mathbb{B}[\alpha]/\alpha^4+\alpha+1$ and X^4+X+1 is irreducible.

The minimal polynomials of α^3, α^5, and α^7 are respectively $X^4+X^3+X^2+X+1$, X^2+X+1, and X^4+X^3+1. There are a few ways to obtain this. One (rather inefficient) way to find minimal polynomial of any element $\beta \in F$ is the following:

- If $\beta \in \mathbb{B}$ then $X-\beta$ is the minimal polynomial.
- if $\beta \notin \mathbb{B}$, then express 1, β, β^2 as polynomials in α with degree $\leqslant 3$. (E.g., if $\beta = \alpha^5$ then $\alpha^5 = \alpha^2+\alpha$ and $(\alpha^5)^2 = \alpha^2+\alpha+1$.)
- Seek any $\mathbb{B}$-linear dependence relation for $\{1,\beta,\beta^2\}$. If there is one, then you obtain the minimal polynomial, which will be of degree 2. (E.g., if $\beta = \alpha^5$ then clearly $(\alpha^5)^2+\alpha^5+1 = 0$ so the minimal polynomial is X^2+X+1. On the other hand, if $\beta = \alpha^3$ or α^7, then you will fail to find any $\mathbb{B}$-linear dependence relation for $\{1,\beta,\beta^2\}$.)
- If you fail to find $\mathbb{B}$-linear dependence relation, then repeat the above procedures for $\{1,\beta,\beta^2,\beta^3\}$. If you still fail, then repeat for $\{1,\beta,\beta^2,\beta^3,\beta^4\}$, etc.

Here is a alternative and slicker way to find the minimal polynomials.

- Observe that $(\alpha^5)^3 = \alpha^{15} = 1$ by Fermat's little theorem. Hence, α^5 is a zero of X^3-1. But since $X^3-1 = (X-1)(X^2+X+1)$ and $\alpha^5 \neq 1$, we see that α^5 is a zero of X^2+X+1. Now note that X^2+X+1 is irreducible.
- Observe that $(\alpha^3)^5 = \alpha^{15} = 1$ by Fermat's little theorem. Hence, α^3 is a zero of X^5-1. But since $X^5-1 = (X-1)(X^4+X^3+X^2+X+1)$ and $\alpha^3 \neq 1$, we see that α^3 is a zero of $X^4+X^3+X^2+X+1$. Now note that $X^4+X^3+X^2+X+1$ is irreducible.
- The minimal polynomial of $\beta \in F$ is same as the minimal polynomial of β^2, so it is enough to find the minimal polynomial of $(\alpha^7)^2 = \alpha^{14} = \alpha^{-1}$. But since $\alpha^4+\alpha+1 = 0$, we obtain

$$0 = \alpha^{-4}(\alpha^4+\alpha+1) = 1+(\alpha^{-1})^3+(\alpha^{-1})^4.$$

Therefore, α^{-1} is a zero of X^4+X^3+1. And X^4+X^3+1 is irreducible.

[10]

b) Recall that for any $f(X) \in \mathbb{B}[X]$ and $\beta \in F$, if $f(\beta) = 0$ then the minimal polynomial of β divides $f(X)$. By Fermat's little theorem, $X^{15}-1$ is divisible by $X-1$, X^4+X+1, $X^4+X^3+X^2+X+1$, X^2+X+1, and X^4+X^3+1. On the other hand, all the above polynomials are pairwise coprime, so $X^{15}-1$ is divisible by the product of them; i.e.,

$$(X-1)(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)(X^4+X^3+1),$$

which is a monic polynomial of degree 15. Therefore, it has to be equal to $X^{15}-1$. [5]

c) (i) The generator polynomials are:

$$\begin{aligned}
\text{BCH}(4,2) &: (X^4+X+1)(X^4+X^3+X^2+X+1)\\
\text{BCH}(4,3) &: (X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)\\
\text{BCH}(4,4) &: (X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)(X^4+X^3+1).
\end{aligned}$$

(ii) Using the answer of b), we obtain the following check polynomials:

$$\begin{aligned}
\mathrm{BCH}(4,2) &: (X-1)(X^4+X^3+1)(X^2+X+1)\\
\mathrm{BCH}(4,3) &: (X-1)(X^4+X^3+1)\\
\mathrm{BCH}(4,4) &: (X-1).
\end{aligned}$$

(iii) Finally, the dimension of $\mathrm{BCH}(4,t)$ is 15 minus the degree of the generator polynomial, so we obtain

$$\begin{aligned}
\dim \mathrm{BCH}(4,2) &= 15-8=7\\
\dim \mathrm{BCH}(4,3) &= 15-10=5\\
\dim \mathrm{BCH}(4,4) &= 15-14=1.
\end{aligned}$$

[5]

d) In case of $\mathrm{BCH}(4,2)$ (respectively, $\mathrm{BCH}(4,3)$) we can find a codeword with weight 5 (respectively, with weight 7); namely, the generator polynomial:

$$\begin{aligned}
\mathrm{BCH}(4,2) &: X^8+X^7+X^6+X^4+1\\
\mathrm{BCH}(4,3) &: X^{10}+X^8+X^5+X^4+X^2+X+1.
\end{aligned}$$

Since the minimal distance of $\mathrm{BCH}(4,t)$ is $\geqslant 2t+1$, the minimal distances of $\mathrm{BCH}(4,2)$ and $\mathrm{BCH}(4,3)$ are respectively 5 and 7.

Since $\dim \mathrm{BCH}(4,4)=1$, there is only one non-zero codeword; namely, the generator polynomial. But the generator polynomial is $(X^{15}-1)/(X-1)=X^{14}+X^{13}+\cdots+X+1$, so the minimal distance of $\mathrm{BCH}(4,4)$ is 15. [5]

4. a) Let $f(t_1,\cdots,t_m)=\sum_{r_1,\cdots,r_m=0}^{n} c_{r_1,\cdots,r_m} t_1^{r_1}\cdots t_m^{r_m}$ for some $c_{r_1,\cdots,r_m}\in\mathbb{B}$. Then for any $\beta_1,\cdots,\beta_m\in F$,

$$\begin{aligned} f(\beta_1^2,\cdots,\beta_m^2) &= \sum_{r_1,\cdots,r_m=0}^{n} c_{r_1,\cdots,r_m}(\beta_1^2)^{r_1}\cdots(\beta_m^2)^{r_m} \\ &= \sum_{r_1,\cdots,r_m=0}^{n} c_{r_1,\cdots,r_m}(\beta_1^{r_1}\cdots\beta_m^{r_m})^2 \\ &= \sum_{r_1,\cdots,r_m=0}^{n} (c_{r_1,\cdots,r_m})^2(\beta_1^{r_1}\cdots\beta_m^{r_m})^2 \\ &= \left(\sum_{r_1,\cdots,r_m=0}^{n} c_{r_1,\cdots,r_m}\beta_1^{r_1}\cdots\beta_m^{r_m}\right)^2 \\ &= (f(\beta_1,\cdots,\beta_m))^2. \end{aligned}$$

Here we used that $(c_{r_1,\cdots,r_m})^2=c_{r_1,\cdots,r_m}$ for any $c_{r_1,\cdots,r_m}\in\mathbb{B}$, and $(\gamma+\delta)^2=\gamma^2+\delta^2$ for any $\gamma,\delta\in F$. [3]

b) One can view a_i's as functions of $\beta_1,\cdots,\beta_m$. For conceptual clarity, let us write $a_i=a_i(\beta_1,\cdots,\beta_m)$. If we show that $a_i(\beta_1,\cdots,\beta_m)$ is a multi-variable polynomial functions of $\beta_1,\cdots,\beta_m$ with coefficients in $\mathbb{B}$, then we may apply a) and obtain $a_i(\beta_1^2,\cdots,\beta_m^2)=(a_i(\beta_1,\cdots,\beta_m))^2$.

It is therefore enough to show that $a_i(\beta_1,\cdots,\beta_m)$ is a multi-variable polynomial functions of $\beta_1,\cdots,\beta_m$ with coefficients in $\mathbb{B}$. But since $a_i(\beta_1,\cdots,\beta_m)$ is constructed by "collecting" the coefficients of X^i, it is a sum of products of $m-i$ elements among $\{\beta_1,\cdots,\beta_m\}$. Therefore, one may write $a_i(\beta_1,\cdots,\beta_m)$ as a *polynomial* in $\beta_1,\cdots,\beta_m$ whose nonzero coefficients are all 1.

If you want the actual formula, here it is:

$$a_i(\beta_1,\cdots,\beta_m)=\sum_{\substack{J\subset\{1,\cdots,m\}\\ |J|=m-i}}\left(\prod_{i\in J}\beta_i\right).$$

So if we may rewrite this as

$$a_i(\beta_1,\cdots,\beta_m)=\sum_{r_1,\cdots,r_m=0}^{1} c_{r_1,\cdots,r_m}\beta_1^{r_1}\cdots\beta_m^{r_m},$$

where $c_{r_1,\cdots,r_m}=1$ if $r_1+\cdots+r_m=m-i$, and $c_{r_1,\cdots,r_m}=0$ otherwise. For example, $a_{m-1}=\beta_1+\cdots+\beta_m$, $a_{m-2}=\beta_1\beta_2+\beta_1\beta_3+\cdots\beta_{m-1}\beta_m$ (if $m\geqslant 3$), and $a_0=\beta_1\cdots\beta_m$. (For the full mark, it is not required to present the formula for $a_i(\beta_1,\cdots,\beta_m)$.) [5]

c) By Fermat's little theorem, we have $\beta^{2^k}=\beta$ for any $\beta\in F$. This shows that m as in (i) exists, and that $m\leqslant k$.

Let m be the smallest positive integer such that $\beta^{2^m}=\beta$. Assume, by contrary, that $\beta^{2^i}=\beta^{2^j}$ for some $0\leqslant i<j\leqslant m$. Now we take 2^{m-i}th power on the both sides of the equation. On the left hand side, we obtain $(\beta^{2^i})^{2^{m-i}}=\beta^{2^m}=\beta$. On the right hand side, we obtain $(\beta^{2^j})^{2^{m-i}}=(\beta^{2^m})^{2^{j-i}}=\beta^{2^{j-i}}$. Therefore we obtain $\beta=\beta^{2^{j-i}}$ and $j-i<m$. This contradicts the minimality of m. [4]

d) Let $\beta_j=\beta^{2^{j-1}}$ for $j=1,\cdots,m$, and $a_i:=a_i(\beta_1,\cdots,\beta_m)$ for $i=0,\cdots,m-1$. First, note that $\prod_{j=1}^{m}(X-\beta_j)=\prod_{j=1}^{m}(X-\beta_j^2)$ because we have by construction $\beta_j^2=\beta_{j+1}$ for $j\neq m$ and $\beta_m^2=\beta_1$. Therefore $a_i=a_i^2$ (by comparing the ith

coefficients of the both sides), so a_i's are either 0 or 1. in other words, we have shown that $f_\beta(X) \in \mathbb{B}[X]$. [5]

e) Note that $f_\beta(\beta) = 0$ by construction, and we have shown that $f_\beta(X) \in \mathbb{B}[X]$ in the previous part. To show $f_\beta(X)$ is a minimal polynomial of β it is left to show that $f_\beta(X)$ has the smallest degree among all the binary polynomials with this property. For this, it is enough to show that for any $f(X) \in \mathbb{B}[X]$ such that $f(\beta) = 0$ we have $f_\beta(X) | f(X)$.

Assume that $f(X) \in \mathbb{B}[X]$ is such that $f(\beta) = 0$. Applying a) to the case when $m = 1$ and $t_1 = X$, we see that $f(\beta^{2^j}) = 0$ for any positive integer j; i.e., $X - \beta^{2^j}$ divides $f(X)$. But since $\beta^{2^{j-1}}$ are all distinct for $j = 1, \cdots, m$, the product $f_\beta(X) = \prod_{j=1}^{m}(X - \beta^{2^{j-1}})$ divides $f(X)$. [5]

f) Using the same notation as the previous parts, we have

$$\begin{aligned} f_\alpha(X) &= (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8) \\ f_{\alpha^3}(X) &= (X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}) \\ f_{\alpha^5}(X) &= (X-\alpha^5)(X-\alpha^{10}). \end{aligned}$$

The generator polynomials of BCH(4,2) and BCH(4,3) are respectively $f_\alpha(X) f_{\alpha^3}(X)$ and $f_\alpha(X) f_{\alpha^3}(X) f_{\alpha^5}(X)$. Therefore the generator polynomials of BCH(4,2) and BCH(4,3) are as follows:

$$\begin{aligned} \text{BCH}(4,2) &: (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)(X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}) \\ \text{BCH}(4,3) &: (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)(X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}) \\ &\quad (X-\alpha^5)(X-\alpha^{10}). \end{aligned}$$

[3]

5. a) Let $v = (v_1, \cdots, v_n) \in \mathbb{B}^n$, and set $w := (v_1, \cdots, v_m) \in \mathbb{B}^m$ and $w' := (v_{m+1}, \cdots v_n) \in \mathbb{B}^{n-m}$. By multiplying block matrices, one can easily see that

$$\begin{aligned} Hv &= \begin{pmatrix} A & I_{n-m} \end{pmatrix} \begin{pmatrix} w \\ w' \end{pmatrix} = Aw + w', \\ Gw &= \begin{pmatrix} I_m \\ -A \end{pmatrix} w = \begin{pmatrix} w \\ -Aw \end{pmatrix}. \end{aligned}$$

Therefore, $Hv = 0$ if and only if $w' = -Aw$ if and only if $v = Gw$. This shows that $\ker H = \operatorname{im} G$. [4]

b) By Fermat's little theorem, any nonzero $\beta \in F$ is a zero of $X^{2^k-1} - 1$. Therefore $\prod_{\substack{\beta \in F \\ \beta \neq 0}} (X - \beta)$ divides $X^{2^k-1} - 1$. But since both are monic polynomials of degree $2^k - 1$, we have

$$X^{2^k-1} - 1 = \prod_{\substack{\beta \in F \\ \beta \neq 0}} (X - \beta).$$

(This is sufficient for the full mark.)

Now, since $\alpha \in F$ is a primitive element, we may write all non-zero elements as α^i for $i = 0, \cdots, 2^k - 2$, so we have

$$X^{2^k-1} - 1 = \prod_{i=0}^{2^k-2} (X - \alpha^i).$$

[3]

c) i) Recall that $\mathrm{RS}(k,t) \subset F^{2^k-1}$. So an $\mathrm{RS}(k,t)$-codeword consists of $2^k - 1$ symbols. And each symbol consists of k binary bits, an $\mathrm{RS}(k,t)$-codeword consists of $k(2^k - 1)$ binary bits. [1]

ii) The (monic) generator polynomial is $\prod_{i=1}^{2t} (X - \alpha^i)$. By b) the corresponding check polynomial is $\prod_{i=2t+1}^{2^k-1} (X - \alpha^i)$. (Note that $2t < 2^k - 1$ by assumption, so this expression makes sense.) [1]

iii) The (monic) generator polynomial is of degree $2t$, so the F-dimension of $\mathrm{RS}(k,t)$ is $2^k - 1 - 2t$. Since the $\mathbb{B}$-dimension is k times the F-dimension (as $F \cong \mathbb{B}^k$), the $\mathbb{B}$-dimension of $\mathrm{RS}(k,t)$ is $k(2^k - 1 - 2t)$. [1]

iv) It can correct up to t error symbols in a single block. [1]

v) An error burst of length up to $k(t-1)+1$ can always be corrected since it can always be placed within t symbols, [1]

d) Let us first find the generator matrix in standard form. For simplicity, let $g(X)$ denote the (monic) generator polynomial for $\mathrm{RS}(4,5)$. A generator matrix corresponds to an F-linear injective map $F^5 \to F^{15}$. (Recall that the $\mathbb{F}$-dimension of $\mathrm{RS}(4,5)$ is 5.) We identify $(w_4, \cdots, w_0) \in F^5$ with $w_4 X^4 + \cdots + w_0 \in F[X]$, and $(v_{,14}, \cdots, v_0) \in F^{15}$ with $v_{14} X^{14} + \cdots + v_0$. The standard encoding sends a polynomial $f(X) \in F[X]$ with degree $\leqslant 4$ to $X^{10} f(X) - r_f(X)$ where $r_f(X)$ is the remainder of $X^{10} f(X)$ modulo $g(X)$. Computing the standard encoding for

X^i for $i = 0, \cdots, 4$ we obtain

$$\begin{aligned}
X^4 &\mapsto X^{14} + \alpha^5 X^9 + \alpha^7 X^8 + \alpha^8 X^7 + \alpha^{14} X^6 + \alpha^{11} X^5 + \alpha^4 X^4 \\
&\quad + \alpha^7 X^3 + \alpha^6 X^2 + \alpha^{11} X + \alpha^6 \\
X^3 &\mapsto X^{13} + \alpha^{11} X^9 + \alpha^7 X^8 + \alpha X^7 + \alpha^4 X^6 + \alpha^{13} X^5 + \alpha^{14} X^4 \\
&\quad \alpha^{11} X^3 + \alpha^2 X^2 + \alpha^3 X + 1 \\
X^2 &\mapsto X^{12} + \alpha^5 X^9 + \alpha^8 X^8 + \alpha^{11} X^7 + \alpha^7 X^6 + \alpha^{13} X^5 + \alpha^{11} X^4 \\
&\quad + \alpha X^3 + \alpha X^2 + \alpha^9 X + \alpha^2 \\
X &\mapsto X^{11} + \alpha^7 X^9 + \alpha^6 X^8 + \alpha X^7 + \alpha^6 X^6 + \alpha^5 X^5 + X^4 \\
&\quad + \alpha^2 X^3 + \alpha^{10} X^2 + \alpha^{12} X + \alpha^{12} \\
1 &\mapsto X^{10} + \alpha^2 X^9 + \alpha^3 X^8 + \alpha^9 X^7 + \alpha^6 X^6 + \alpha^{14} X^5 + \alpha^2 X^4 \\
&\quad + \alpha X^3 + \alpha^6 X^2 + \alpha X + \alpha^{10}
\end{aligned}$$

Since $e_i \in F^5$ corresponds to X^{5-i} and its encoding gives the ith column of the generator matrix, the systematic encoding corresponds to the following matrix

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\alpha^5 & \alpha^{11} & \alpha^5 & \alpha^7 & \alpha^2 \\
\alpha^7 & \alpha^7 & \alpha^8 & \alpha^6 & \alpha^3 \\
\alpha^8 & \alpha & \alpha^{11} & \alpha & \alpha^9 \\
\alpha^{14} & \alpha^4 & \alpha^7 & \alpha^6 & \alpha^6 \\
\alpha^{11} & \alpha^{13} & \alpha^{13} & \alpha^5 & \alpha^{14} \\
\alpha^4 & \alpha^{14} & \alpha^{11} & 1 & \alpha^2 \\
\alpha^7 & \alpha^{11} & \alpha & \alpha^2 & \alpha \\
\alpha^6 & \alpha^2 & \alpha & \alpha^{10} & \alpha^6 \\
\alpha^{11} & \alpha^3 & \alpha^9 & \alpha^{12} & \alpha \\
\alpha^6 & 1 & \alpha^2 & \alpha^{12} & \alpha^{10}
\end{pmatrix}.$$

Now, using a) we obtain the check matrix in standard form:

$$\begin{pmatrix}
\alpha^5 & \alpha^{11} & \alpha^5 & \alpha^7 & \alpha^2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha^7 & \alpha^7 & \alpha^8 & \alpha^6 & \alpha^3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha^8 & \alpha & \alpha^{11} & \alpha & \alpha^9 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha^{14} & \alpha^4 & \alpha^7 & \alpha^6 & \alpha^6 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha^{11} & \alpha^{13} & \alpha^{13} & \alpha^5 & \alpha^{14} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\alpha^4 & \alpha^{14} & \alpha^{11} & 1 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\alpha^7 & \alpha^{11} & \alpha & \alpha^2 & \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\alpha^6 & \alpha^2 & \alpha & \alpha^{10} & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\alpha^{11} & \alpha^3 & \alpha^9 & \alpha^{12} & \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\alpha^6 & 1 & \alpha^2 & \alpha^{12} & \alpha^{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

6. a) $s(z) = \sum_{i=1}^{6} d(\alpha^i) z^{i-1}$. [3]

b) i) An error has occurred because the syndrome polynomial $s^{(1)}(z)$ is not zero. [2]

ii) The degree of $s^{(1)}(z)$ is 2, which is smaller than 3. Hence the error locator polynomial produced by the "Euclid's algorithm step" is $l(z) = 1$ (meaning no error has occurred) while an error has occurred. [5]

c) i) Let $s(z) := s^{(2)}(z)$ for simplicity. An error has occurred because $s(z)$ is not zero.

Now, we run Euclid's algorithm for $s(z)$ and z^6:

Step 1 $z^6 = (\alpha^{10} z^2 + \alpha^9 z + \alpha^8) s(z) + r_1(z)$,
where $r_1(z) = \alpha^6 z^3 + \alpha^{14} z^2 + \alpha^{13} z + \alpha^{13}$.

Step 2 $s(z) = (\alpha^{14} z + \alpha^5) r_1(z) + r_2(z)$,
where $r_2(z) = \alpha^6 z^2 + \alpha^{13} z + \alpha^{11}$.

We stop the process since $\deg(r_2(z)) < 3$. Putting this all thgether, we get

$$\begin{aligned} r_2(z) &= s(z) + (\alpha^{14} z + \alpha^5) r_1(z) \qquad \ldots \text{Step2} \\ &= s(z) + (\alpha^{14} z + \alpha^5)\Big((\alpha^{10} z^2 + \alpha^9 z + \alpha^8) s(z) + z^6\Big) \qquad \ldots \text{Step1} \\ &\equiv (\alpha^9 z^3 + \alpha^2 z^2 + \alpha z + \alpha^6) s(z) \bmod z^6 \end{aligned}$$

(Alternatively, you may simply use the recursive formula for u_k and v_k, if you can remember it.) Therefore we get

$$\begin{aligned} l(z) &= \alpha^{-6}(\alpha^9 z^3 + \alpha^2 z^2 + \alpha z + \alpha^6) = \alpha^3 z^3 + \alpha^{11} z^2 + \alpha^{10} z + 1 \\ w(z) &= \alpha^{-6} r_2(z) = z^2 + \alpha^7 z + \alpha^5. \end{aligned}$$

The next step is to find all the roots of $l(z)$. Usually the only general method for this is "exhaustive search", but in our situation we have strong candidates for error positions; namely, $i = 0$ where the bits were erased. One can easily check that $l(1) = 0$ and $l'(1) \neq 0$ where $l'(z) = \alpha^3 z^2 + \alpha^{10}$ denotes the formal derivative. This shows that $z = 1$ is not a multiple root, so we carry on. The quotient of $l(z)$ by $(1 - z)$ is $1 + \alpha^5 z + \alpha^3 z^2$ so we need to find i and j such that $\alpha^i + \alpha^j = \alpha^5$ and $\alpha^{i+j} = \alpha^3$. By looking up the table, one can check $i = 1$ and $j = 2$ satisfies these conditions. So $1 + \alpha^5 z + \alpha^3 z^2 = (1 - \alpha z)(1 - \alpha^2 z)$, and $l(z) = (1 - z)(1 - \alpha z)(1 - \alpha^2 z)$. The error positions are $i = 0, 1, 2$.

Now we can obtain

$$\begin{aligned} e_0 &= w(1) 1^{-1} (1 - \alpha)^{-1} (1 - \alpha^2)^{-1} = \alpha^9 \\ e_1 &= w(\alpha^{-1}) \alpha^{-1} (1 - 1 \cdot \alpha^{-1})^{-1} (1 - \alpha^2 \cdot \alpha^{-1})^{-1} = \alpha^2 \\ e_2 &= w(\alpha^{-2}) \alpha^{-2} (1 - 1 \cdot \alpha^{-2})^{-1} (1 - \alpha \cdot \alpha^{-2})^{-1} = 1. \end{aligned}$$

From this, we find the error polynomial

$$e(X) = e_2 X^2 + e_1 X + e_0 = X^2 + \alpha^2 X + \alpha^9,$$

and the corrected word is:

$$\begin{aligned} d^{(2)}(X) + e(X) = {} & \alpha^{14} X^{14} + \alpha X^{13} + \alpha^2 X^{12} + \alpha^8 X^{11} + \alpha^{12} X^{10} + \alpha^{12} X^9 \\ & + \alpha^5 X^8 + \alpha^2 X^7 + 0 X^6 + \alpha^6 X^5 + \alpha^3 X^4 + X^3 + \alpha^5 X^2 + X + \alpha^9 \end{aligned}$$

[12]

ii) Let $c(X) := d^{(2)}(X) + e(X)$ denote the corrected codeword found in the previous part. Then the error polynomial for the first transmission is

$$e^{(1)}(X) = d^{(1)}(X) - c(X) = \alpha^8 X^{11} + \alpha^7 X^{10} + \alpha^{12} X^9 + \alpha^8 X^8$$

There are more than 4 error symbols (at positions $i = 8, 9, 10, 11$), so the decoding algorithm may fail. [3]