IMPERIAL COLLEGE LONDON

Final

E4.07
CS7.23
SO11

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2010

MSc and EEE/ISE PART IV: MEng and ACGI

CODING THEORY

Wednesday, 5 May 10:00 am

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) Consider the Hamming code Ham(3) given 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 corresponding generator matrix of Ham(3) in standard form. (You do not need to explain why it works.) [3]

ii) Assume that $v \in \mathbb{B}^7$ is non-zero with at most two non-zero binary bits Show that $H_3 \cdot v \neq 0$. (*Hint:* Let $e_j \in \mathbb{B}^7$ be a vector whose jth entry is 1 and the other entries are zero. Then any vector $v \in \mathbb{B}^7$ with exactly two non-zero entries can be written as $v = e_i + e_j$ for some $i \neq j$.) [7]

iii) Show that the minimal distance of Ham(3) is 3. [5]

b) Define a code Ham$'(3)$ by adding an overall parity check bit; i.e. $(v_1, \cdots, v_7, v_8) \in \mathbb{B}^8$ is a codeword of Ham$'(3)$ if and only if $(v_1, \cdots, v_7)$ is a codeword of Ham(3) and $v_8 = v_1 + \cdots + v_7$.

i) Find a generator matrix and a check matrix of the extended code Ham$'(3)$ in standard form. [5]

ii) Find the minimal distance of Ham$'(3)$. [5]

2. Let $F := \mathrm{GF}(q)$ for some $q := 2^k$, and fix a choice $\alpha \in F$ of primitive element. 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.*

For $v, w \in F^n$, we let $d(v, w)$ denote the distance between v and w.

a) Define r-perfectness for an F-linear code $C \subset F^n$. [3]

b) For an F-linear code $C \subset F^n$, let $d(C)$ denote the minimal distance of C. In this part, we show that if C is r-perfect then $d(C) = 2r + 1$.

i) If $d(C) < 2r + 1$, then show that there is a vector $w \in F^n$ such that $d(0, w) \leqslant r$, and $d(v, w) \leqslant r$ for some nonzero vector $v \in C$. [3]

ii) If $d(C) > 2r + 1$, then produce a $w \in F^n$ such that there exist *no* codeword $v \in C$ such that $d(v, w) \leqslant r$. (*Hint:* Choose w such that $d(0, w) = r + 1$, and prove by contradiction.) [3]

c) Fix a vector $v \in F^{15}$. Let $N_{r,q}$ be the number of vectors $w \in F^{15}$ such that $d(v, w) \leqslant r$ for the fixed vector $v \in F^{15}$. Find a formula for $N_{r,q}$ and observe that this number does not depend on v. [5]

d) Show that if an F-linear code $C \subset F^{15}$ is r-perfect then we have the equality $N_{r,q} = q^{n-m} (= 2^{k(n-m)})$, where $N_{r,q}$ is defined in c) and m is the F-dimension of the code C. (*Hint:* Consider $D_r(v) := \{w \in F^{15} \mid d(v, w) \leqslant r\}$ for all elements $v \in C$.) [5]

e) Using d), show that $\mathrm{BCH}(4, 2)$ is not 2-perfect as a $\mathbb{B}$-linear code. Similarly, show that $\mathrm{RS}(4, 2)$ is not 2-perfect as a $\mathrm{GF}(2^4)$-linear code. You may use standard facts about BCH- and RS- codes without proof. [6]

3. Let $F = \mathrm{GF}(2^k)$ for some positive integer k. Throughout this question, $\beta \in F$ is a *non-zero* element. Recall the following definition:

Definition. The *order* of β, denoted by $\mathrm{ord}(\beta)$, is the smallest positive integer such that $\beta^{\mathrm{ord}(\beta)} = 1$.

a) Show that $\mathrm{ord}(\beta)$ divides $2^k - 1$. (*Hint:* Using Euclid's algorithm for integers, show that if $\beta^r = 1$ then $\beta^{hcf(r,2^k-1)} = 1$, where $hcf(,)$ is the highest common factor.) [5]

b) Assume that $2^k - 1$ is a *prime number*; e.g. $k = 2, 3, 5$, etc. Deduce that any $\beta \in F \setminus \{0, 1\}$ is primitive. [5]

c) For the rest of this question, $2^k - 1$ is *not* necessarily a prime number. Let $\alpha \in F$ be a primitive element. For a positive integer $s < 2^k - 1$, show that $\mathrm{ord}(\alpha^s) = \frac{2^k-1}{hcf(s,2^k-1)}$. (*Hint:* You can grant that $\frac{2^k-1}{hcf(s,2^k-1)} = \frac{lcm(s,2^k-1)}{s}$ where $lcm(,)$ denotes the least common multiple.) [5]

d) Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$ be a field with 2^4 elements. (You may grant that $X^4 + X + 1 \in \mathbb{B}[X]$ is irreducible.) Show that α is a primitive element. [3]

e) Let $F := \mathbb{B}[\alpha]/\alpha^6 + \alpha + 1$ be a field with 2^6 elements. (You may grant that $X^6 + X + 1 \in \mathbb{B}[X]$ is irreducible.) Show that α is a primitive element. Also, show that $\alpha^5, \alpha^{11}, \alpha^{13}$ are primitive elements. [7]

4. For this question you may use without proof all the standard results on finite fields covered in class, but be sure to clearly state the result before you use it. It could be useful to label frequently used lemmas in your solution.

Let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$ be a field with 2^4 elements where α is a primitive element.

a) Define a minimal polynomial of an element $\beta \in F$ over $\mathbb{B}$. (You may give any of the equivalent definitions.) Show that the minimal polynomials of $\alpha, \alpha^3, \alpha^5$ are $X^4+X+1, X^4+X^3+X^2+X+1, X^2+X+1 \in \mathbb{B}[X]$, respectively. You may grant that these polynomials are irreducible. [4]

b) Put

$$\begin{aligned} g_{4,2}(X) &:= (X^4+X+1)(X^4+X^3+X^2+X+1) \in \mathbb{B}[X] \\ g_{4,3}(X) &:= (X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1) \in \mathbb{B}[X]. \end{aligned}$$

Show that $g_{4,2}(X)$ and $g_{4,3}(X)$ divide $X^{15}-1 \in \mathbb{B}[X]$. (Therefore, $g_{4,2}(X)$ and $g_{4,3}(X)$ define cyclic codes with block size 15. We call these cyclic codes BCH$(4,2)$ and BCH$(4,3)$, respectively.) [5]

c) As usual, identify a binary vector $v := (v_{14}, \cdots, v_0) \in \mathbb{B}^{15}$ with a binary polynomial $v(X) := \sum_{i=0}^{14} v_i X^i \in \mathbb{B}[X]$. For $t = 2, 3$, set

$$V_{4,t} := \begin{pmatrix} \alpha^{14} & \cdots & \alpha^2 & \alpha & 1 \\ (\alpha^{14})^2 & \cdots & (\alpha^2)^2 & \alpha^2 & 1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ (\alpha^{14})^{2t} & \cdots & (\alpha^2)^{2t} & \alpha^{2t} & 1 \end{pmatrix}$$

Explain why the $\mathbb{B}$-linear code with check matrix $V_{4,2}$ (respectively, $V_{4,3}$) coincides with the cyclic code with generator polynomial $g_{4,2}(X)$ (respectively, $g_{4,3}(X)$). [5]

d) Find the $\mathbb{B}$-dimensions of the codes BCH$(4,2)$ and BCH$(4,3)$. [4]

e) Find a generator matrix for BCH$(4,3)$ in standard form. (*Hint:* Systematic encoding. Note that $g_{4,3}(X) = X^{10}+X^8+X^5+X^4+X^2+X+1$.) [7]

5. The aim of this question is to compute the dimension of BCH$(6,t)$.

Let $F := \mathbb{B}[\alpha]/\alpha^6+\alpha+1$. You may take it for grant that $X^6+X+1 \in \mathbb{B}[X]$ is irreducible and α is a primitive element.

a) Show that for any $\beta \in F$ the degree of minimal polynomial of β is at most 6. (*Hint:* Since F is 6-dimensional vector space over $\mathbb{B}$, any 7 elements in F are linearly dependent over $\mathbb{B}$.) [3]

b) Show that the minimal polynomial of $\beta := \alpha^9$ is of degree 3. (*Hint:* compute β^3, β^2, β and express β^3 as a linear combination of $\{\beta^2, \beta, 1\}$.) [5]

c) For $i = 1,3,5,7,11,13$ and $d = 0,1,2,3,4,5$, express $(\alpha^i)^{2^d}$ as α^s with $0 \leqslant s \leqslant 62$ and fill in the blanks of the table below. (Note that $i \cdot 2^d$ could be bigger than 62.) Check that they are pairwise distinct for each i and d. (*Hint:* Note that α is *primitive*.)

$(\alpha^i)^{2^d}$	$i=1$	$i=3$	$i=5$	$i=7$	$i=11$	$i=13$
$d=0$	α	α^3	α^5	α^7	α^{11}	α^{13}
$d=1$	α^2					
$d=2$	α^4					
$d=3$	α^8					
$d=4$	α^{16}					
$d=5$	α^{32}					

[5]

d) Show that the minimal polynomials of $\alpha, \alpha^3, \alpha^5, \alpha^7, \alpha^{11}, \alpha^{13}$ are pairwise distinct and that all of them are of degree 6. (*Hint:* See Part a), also. To show that the minimal polynomials are distinct, you can check that their roots are disjoint.) [7]

e) Find the degrees of generator polynomials of BCH$(6,6)$ and BCH$(6,7)$, respectively, and complete the following table by filling in the blanks.

	binary block size	$\mathbb{B}$-dimension of code	length of error-bursts that can be corrected
RS$(4,3)$	60		
RS$(4,4)$	60		
BCH$(6,6)$			
BCH$(6,7)$			

Here, RS(k,t) stands for Reed-Solomon code. You may use without proof standard results/formulas covered in lectures. [5]

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 the primitive element α.

Assume that you have received a lengthy message encoded via RS(4,3). But during transmission the signal momentarily faded, and you could not receive 16 binary bits. This affected the following two blocks of of 60 binary bits received:

$$\underbrace{[\cdots\ 0111\ 0101\ \overbrace{*\,*\,*\,*\ *\,*\,*\,*}^{8\text{ binary bits}}]}_{\text{block } d^{(1)}}\ \underbrace{[\overbrace{*\,*\,*\,*\ *\,*\,*\,*}^{8\text{ binary bits}}\ 1110\ 0010\ \cdots]}_{\text{block } d^{(2)}},$$

where $*$ denotes the erased bits. To decode, we regard erase bits as 0.

Using the usual identification, the words $d^{(1)}$ and $d^{(2)}$ respectively correspond to the following polynomials:

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

a) Write down the generator polynomial $g^{\mathrm{RS}}_{4,3}(X) \in F[X]$ for RS(4,3), and show that it divides $X^{15}-1$. You do not need to simplify the answer. [2]

b) The syndrome polynomials $s^{(1)}(z)$ and $s^{(2)}(z)$ for the received words $d^{(1)}(X)$ and $d^{(2)}(X)$, respectively, are as follows:

$$\begin{aligned} s^{(1)}(z) &= 0z^5+\alpha^2z^4+0z^3+\alpha^9z^2+\alpha^{13}z+\alpha^{11} \\ s^{(2)}(z) &= \alpha^8z^5+\alpha^9z^4+\alpha z^3+0z^2+0z+0 \end{aligned}$$

i) Explain how you obtain the syndrome polynomials $s^{(1)}(z)$ and $s^{(2)}(z)$ corresponding to $d^{(1)}(X)$ and $d^{(2)}(X)$. (You do not need to compute $s^{(1)}(z)$ and $s^{(2)}(z)$.) [2]

ii) Explain why, unlike BCH(4,3), it can happen that the $(2i)$th syndrome (i.e. the $(2i-1)$th coefficient of the syndrome polynomial) is not the square of the ith syndrome. [2]

iii) Determine whether any error has occurred in $d^{(1)}(X)$ and $d^{(2)}(X)$, and explain your reasoning. [2]

c) Let $s(z) := s^{(1)}(z)$, for simplicity. Find the corrected codeword for $d^{(1)}(X)$ via the decoding algorithm. Make sure to clearly label the error locator, the error evaluator, the error positions, and the error polynomial, as well. Did errors occur at the "expected" positions? If the decoding algorithm should fail to produce a corrected codeword, then explain in "practical" terms why it does not work. [12]

d) Repeat the previous part c) for $s(z) := s^{(2)}(z)$. If the decoding algorithm should fail to produce a corrected codeword, then explain in "practical" terms why it does not work. [5]

E4.07
CS7.23
2016
S11

CODING THEORY: FINAL EXAM SOLUTION

1. a) i)

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

[3]

ii) Observe that $H_3 \cdot e_j$ is the jth column vector of H_3. Clearly $H_3 \cdot e_j \neq 0$ for any j. For any $i \neq j$ we have $H_3(e_i + e_j) = H_3 \cdot e_i + H_3 \cdot e_j \neq 0$ since any distinct two column vectors of H_3 are distinct. [7]

iii) The previous part shows that the minimal distance is strictly greater than 2, so it is enough to find a codeword with exactly three non-zero binary bits. Since the 4th column vector of H_3 is the sum of the 6th and 7th column vectors of H_3, so we have found a codeword $e_4 + e_6 + e_7 \in \mathbb{B}^7$ with exactly three non-zero bits. [5]

b) i) The generator matrix G_3' and the check matrix H_3' for $\mathrm{Ham}'(3)$ are

$$G_3' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \qquad H_3' = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

If $(v_1, \cdots, v_7)$ is a codeword for $\mathrm{Ham}(3)$, then there is (x_1, x_2, x_3, x_4) such that $(v_1, \cdots, v_7)^\top = G_3 \cdot (x_1, x_2, x_3, x_4)^\top$, where G_3 is the generator matrix for $\mathrm{Ham}(3)$. Writing out v_i in terms of $(x_1, \cdots, x_4)$, you can find that $\sum_{i=1}^{7} v_i = x_1 + x_3 + x_4$. This gives G_3' above, and since it's in standard from we obtain H_3' as well.

Alternatively, you may observe that $G_3' = \begin{pmatrix} 1 & & \\ & \ddots & \\ 1 & \cdots & 1 \end{pmatrix} G_3$. [5]

ii) The minimal distance of $\mathrm{Ham}'(3)$ is 4. Adding parity bit either increase or does not change the number of non-zero bits in a codeword, and if $v \in \mathbb{B}^7$ is a $\mathrm{Ham}(3)$-codeword with exactly 3 non-zero bits then the parity bit added is 1. So any non-zero codeword of $\mathrm{Ham}'(3)$ should have at least 4 non-zero bits. [5]

2. a) An F-linear code $C \subset F^n$ is *r-perfect* if for any $w \in F^n$ there exists a unique codeword $v \in C$ such that $d(v,w) \leqslant r$. [3]

b) i) Choose $v \in C$ such that $d(v,0) = d(C)$. If $d(v,0) \leqslant r$, then take $w = v$. If not, then let $w \in F^n$ be the vector obtained by replacing r non-zero symbols (or alphabets) in v by 0. Clearly we have $d(v,w) = r$, and we also have $d(0,w) \leqslant r$ because $d(v,0) \leqslant 2r$. [3]

ii) Assume, by contrary, that for any $w \in F^n$ there exists some codeword $v \in C$ such that $d(v,w) \leqslant r$. By assumption, for $w \in F^n$ with $d(0,w) = r+1$, there exists $v \in C$ such that $d(v,w) \leqslant r$. By triangular inequality we have $d(0,v) \leqslant d(0,w) + d(v,w) = 2r+1$, so $d(C) \leqslant 2r+1$. [3]

c) The number of $w \in F^{15}$ with $d(w,v) = n$ is precisely $(q-1)^n \binom{15}{n}$; indeed, there are $\binom{15}{n}$ choices of n positions where symbols of v and w differ, and at each of the n positions there are $(q-1)$ symbols to choose from. Therefore, we obtain:

$$N_{r,q} = \sum_{n=0}^{r} (q-1)^n \binom{15}{n} = 1 + (q-1)\binom{15}{1} + \cdots + (q-1)^r \binom{15}{r}.$$

[5]

d) By r-perfectness, we have $\bigcup_{v \in C} D_r(v) = F^{15}$ and $D_r(v) \cap D_r(v')$ is empty for any distinct codewords $v, v' \in C$. Since the F-dimension of C is m, we have $|C| = q^m$. Since $|D_r(v)| = N_{r,q}$ for any $v \in F^{15}$, we obtain the formula $q^m \cdot N_{r,q} = q^n$. [5]

e) If BCH$(4,2)$ were 2-perfect, then $N_{2,2}$ (i.e. with $r = 2$ and $q = 2$) has to be some power of 2. On the other hand $N_{2,2} = 1 + 15 + 15 \cdot 7$ is not even an even number. Similarly, $N_{2,16} = 1 + 15 \cdot 15 + 15^2 \cdot (15 \cdot 7)$ is not even an even number so RS$(4,2)$ cannot be 2-perfect. (In fact, $N_{2,q}$ is an odd number for any $q = 2^k$, so we have in fact shown that there is no 2-perfect F-linear code with F-block size 15 for any finite field F of characteristic 2.) [6]

3. a) For any integer r, Euclid's algorithm provides integers u, v such that $ur + v(2^k - 1) = hcf(r, 2^k - 1)$. If $\beta^r = 1$ then

$$\beta^{hcf(r,2^k-1)} = \beta^{ur+v(2^k-1)} = (\beta^r)^u \cdot (\beta^{2^k-1})^v = 1,$$

by our assumption and Fermat's little theorem. So if $r = \mathrm{ord}(\beta)$, then r should be equal to $hcf(r, 2^k - 1)$ by minimality; i.e., $r | (2^k - 1)$. [5]

b) Note that β is primitive if and only if $\mathrm{ord}(\beta) = 2^k - 1$. By part a) and the assumption on $2^k - 1$, $\mathrm{ord}(\beta)$ is either 1 or $2^k - 1$. But $\mathrm{ord}(\beta) = 1$ exactly means $\beta = \beta^1 = 1$. [5]

c) We need to find the smallest positive number r such that $\alpha^{sr} = 1$. This is achieved exactly when $sr = lcm(s, 2^k - 1)$, since $\alpha^N = 1$ if and only if $(2^k - 1) | N$. Now, we have $r = \frac{lcm(s,2^k-1)}{s} = \frac{2^k-1}{hcf(s,2^k-1)}$. [5]

d) This is clear from the table at page 1 of the exam sheet. Alternatively, you may give the following simple argument. Since $2^4 - 1 = 15 = 3 \cdot 5$, it is enough to check that $\alpha, \alpha^3, \alpha^5 \neq 1$ by part a). Clearly, α and α^3 are not equal to 1, and $\alpha^5 = \alpha^2 + \alpha \neq 1$. [3]

e) Note that $2^6 - 1 = 63 = 3^2 \cdot 7$. By part a), it is enough to check that none of $\alpha, \alpha^3, \alpha^7, \alpha^9, \alpha^{21}$ is 1. Clearly, α and α^3 are not equal to 1. Using $\alpha^6 = \alpha + 1$,

we show

$$\begin{aligned}\alpha^7 &= \alpha^6\cdot\alpha = (\alpha+1)\alpha = \alpha^2+\alpha \neq 1\\ \alpha^9 &= \alpha^6\cdot\alpha^3 = (\alpha+1)\alpha^3 = \alpha^4+\alpha^3 \neq 1\\ \alpha^{21} &= (\alpha^6)^3\cdot\alpha^3 = (\alpha+1)^3\alpha^3 = (\alpha^3+\alpha^2+\alpha+1)\alpha^3\\ &= \alpha^6+\alpha^5+\alpha^4+\alpha^3 = \alpha^5+\alpha^4+\alpha^3+\alpha+1 \neq 1.\end{aligned}$$

Since $s = 5,11,13$ satisfy $hcf(s,63) = 1$, we have $\text{ord}(\alpha^s) = 63$ (i.e., α^s is primitive) for those s. [7]

4. The following lemmas will be frequently used, so we state them separately.

Lemma A. *For $f(X),g(X),h(X) \in \mathbb{B}[X]$, assume that $hcf(g(X),h(X)) = 1$. Then $g(X)h(X)|f(X)$ if and only if $g(X)|f(X)$ and $h(X)|f(X)$*

Lemma B. *For $\beta \in F$, the minimal polynomial of β divides $f(X) \in \mathbb{B}[X]$ if and only if $f(\beta) = 0$.*

a) *Solution 1:* You may define the minimal polynomial of $\beta \in F$ to be an irreducible polynomial $f(X)$ such that $f(\beta) = 0$. Since irreducibility of the polynomials are already known, you just need to check $\alpha^4+\alpha+1 = 0$, $(\alpha^3)^4+(\alpha^3)^3+(\alpha^3)^2+\alpha^3+1 = 0$ and $(\alpha^5)^2+\alpha^5+1 = 0$.

Solution 2: You may define the minimal polynomial of $\beta \in F$ to be the polynomial $f(X)$ with the smallest degree among nonzero polynomial which has β as a root. In this case, you additionally need to state that a polynomial $f(X) \in \mathbb{B}[X]$ with $f(\beta) = 0$ is a minimal polynomial of β if and only if $f(X)$ is irreducible (or prove this using Lemma B above.). [4]

b) By irreducibility, the highest common factor of any two of $X^4+X+1, X^4+X^3+X^2+X+1, X^2+X+1$ is 1. By Lemma A, it is enough to show that each of $X^4+X+1, X^4+X^3+X^2+X+1, X^2+X+1$ divides $X^{15}+1$.

On the other hand, X^4+X+1 is the minimal polynomial of α, and α is a root of $X^{15}+1$ by Fermat's little theorem. So by Lemma B we have $(X^4+X+1)|(X^{15}+1)$. We proceed similarly for the other two polynomials. [5]

c) Let $t = 2$ or $t = 3$. By writing out $V_{4,t}v = 0$, we obtain

$$\begin{aligned} v_{14}\alpha^{14}+\cdots v_1\alpha+v_0 &= 0\\ v_{14}(\alpha^2)^{14}+\cdots v_1\alpha^2+v_0 &= 0\\ &\vdots\\ v_{14}(\alpha^{2t})^{14}+\cdots v_1\alpha^{2t}+v_0 &= 0\end{aligned}$$

i.e., $v(\alpha) = \cdots = v(\alpha^{2t}) = 0$. On the other hand, we have we have

$$v(\alpha^{2i}) = \sum_{j=0}^{14} v_j\alpha^{2ij} = \sum_{j=0}^{14} v_j^2\alpha^{2ij} = \left(\sum_{j=0}^{14} v_j\alpha^{ij}\right)^2 = (v(\alpha^i))^2$$

since $v_i^2 = v_i$ and $(\beta+\gamma)^2 = \beta^2+\gamma^2$ for any $\beta,\gamma \in F$. This shows that $V_{4,t}v = 0$ if and only if $v(\alpha^i) = 0$ for all odd integers i from 1 up to $2t-1$. Now by Lemmas A and B, this is equivalent to requiring $g_{4,t}(X)|v(X)$. [5]

d) The $\mathbb{B}$-dimension of BCH$(4,2)$ is $15-\deg(g_{4,2}(X)) = 7$, and the $\mathbb{B}$-dimension of BCH$(4,3)$ is $15-\deg(g_{4,3}(X)) = 5$. [4]

e) First, perform the following long division:

$$\begin{aligned}
X^{14} &= (X^4+X^2+1)g_{4,3}(X)+X^9+X^7+X^4+X^3+X+1\\
X^{13} &= (X^3+X)g_{4,3}(X)+X^9+X^8+X^7+X^6+X^4+X^2+X\\
X^{12} &= (X^2+1)g_{4,3}(X)+X^8+X^7+X^6+X^5+X^3+X+1\\
X^{11} &= X\cdot g_{4,3}(X)+X^9+X^6+X^5+X^3+X^2+X\\
X^{10} &= g_{4,3}(X)+X^8+X^5+X^4+X^2+X+1
\end{aligned}$$

The systematic encoding takes X^4 to $X^{14}-(X^9+X^7+X^4+X^3+X+1)$, etc. Identifying $(a_4,\cdots,a_0)\in\mathbb{B}^5$ with $a_4X^4+\cdots+a+0\in\mathbb{B}[X]$, we can write this as the following matrix

$$\begin{pmatrix}
1&0&0&0&0\\
0&1&0&0&0\\
0&0&1&0&0\\
0&0&0&1&0\\
0&0&0&0&1\\
1&1&0&1&0\\
0&1&1&0&1\\
1&1&1&0&0\\
0&1&1&1&0\\
0&0&1&1&1\\
1&1&0&0&1\\
1&0&1&1&0\\
0&1&0&1&1\\
1&1&1&1&1\\
1&0&1&0&1
\end{pmatrix}$$

[7]

5. a) Since F is a 6-dimensional $\mathbb{B}$-vector space, any 7 elements are linearly dependent over $\mathbb{B}$, so in particular $\{1,\beta,\cdots,\beta^6\}$ is linearly dependent over $\mathbb{B}$. This $\mathbb{B}$-linear dependence gives you some polynomial $f(X)\in\mathbb{B}[X]$ of degree $\leqslant 6$ with $f(\beta)=0$, so necessarily the minimal polynomial has degree $\leqslant 6$. [3]

b) Since $\alpha^6=\alpha+1$, we have

$$\begin{aligned}
\beta^3 &= (\alpha^6)^4\alpha^3=(\alpha+1)^4\alpha^3=\alpha^7+\alpha^3=\alpha^3+\alpha^2+\alpha\\
\beta^2 &= (\alpha^6)^3=(\alpha+1)^3=\alpha^3+\alpha^2+\alpha+1\\
\beta &= \alpha^6\alpha^3=(\alpha+1)\alpha^3=\alpha^4+\alpha^3
\end{aligned}$$

From this, it is clear that $\beta^3+\beta^2+1=0$, and that β^2 cannot be expressed as a $\mathbb{B}$-linear combination of β and 1, so the polynomial with smallest degree which has β as a root is X^3+X^2+1. So the minimal polynomial of β is X^3+X^2+1. (Alternatively, observe that X^3+X^2+1 is irreducible and has β as a root.) [5]

c) If $i \cdot 2^d \geqslant 63$, use $\alpha^{63} = 1$ to reduce the exponent (Fermat's little theorem). Then we obtain the following.

$(\alpha^i)^{2^d}$	$i=1$	$i=3$	$i=5$	$i=7$	$i=11$	$i=13$
$d=0$	α	α^3	α^5	α^7	α^{11}	α^{13}
$d=1$	α^2	α^6	α^{10}	α^{14}	α^{22}	α^{26}
$d=2$	α^4	α^{12}	α^{20}	α^{28}	α^{44}	α^{52}
$d=3$	α^8	α^{24}	α^{40}	α^{56}	α^{25}	α^{41}
$d=4$	α^{16}	α^{48}	α^{17}	α^{49}	α^{50}	α^{19}
$d=5$	α^{32}	α^{33}	α^{34}	α^{35}	α^{37}	α^{38}

The elements in the table are all distinct, because α is primitive and the exponents are all distinct numbers between 0 and 62. [5]

d) Observe that for $\beta \in F$ and $f(X) \in \mathbb{B}[X]$, we have $f(\beta^2) = (f(\beta))^2$; indeed, if $f(X) = \sum_n a_n X^n$, then we have $f(\beta^2) = \sum_n a_n \beta^{2n} = (\sum_n a_n \beta^n)^2 = (f(\beta))^2$ because $a_n^2 = a_n$ and for any $\gamma, \gamma' \in F$ we have $(\gamma+\gamma')^2 = \gamma^2 + (\gamma')^2$.

It follows from the previous paragraph and the table in the previous part that if $\beta = \alpha^i$ for $i = 1,3,5,7,11,13$, then the minimal polynomial of β has at least 6 distinct roots: $\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32}$, so its degree is at least 6. Since the degree of the minimal polynomial of $\beta \in F$ is at most 6 by part a), we conclude that the degree is exactly 6 for any of the above choices.

For any distinct $i, j \in \{1,3,5,7,11,13\}$, the roots of the minimal polynomials of α^i and α^j are disjoint, as we saw in the previous table. So the minimal polynomials of α^i with $i \in \{1,3,5,7,11,13\}$ are pairwise distinct. [7]

e) Let $g_{6,t}(X)$ is the generator polynomial for BCH$(6,t)$, and recall that it is the product of *distinct* minimal polynomials of $\alpha, \alpha^3, \cdots, \alpha^{2t-1}$. We saw in parts b) and d) that minimal polynomials of $\alpha, \alpha^2, \cdots, \alpha^{13}$ are pairwise distinct and we know their degrees. Putting these together, we obtain that the minimal $\deg(g_{6,6}(X)) = 33$ and $\deg(g_{6,7}(X)) = 39$.

The $\mathbb{B}$-dimension of BCH(k,t) is $2^k - 1 - \deg(g_{k,t}(X))$. It can correct t binary error bits. The F-dimension of RS(k,t) is $2^k - 1 - 2t$, so its $\mathbb{B}$-dimension is $k(2^k - 1 - 2t)$. It can correct t error symbols in a block. In particular, it can correct $k(t-1)+1$ binary bits of error-bursts. So we obtain:

	binary block size	$\mathbb{B}$-dimension of code	length of error-bursts that can be corrected
RS(4,3)	60	36	9
RS(4,4)	60	28	13
BCH(6,5)	63	30	~~5~~ 6
BCH(6,6)	63	24	~~6~~ 7

[5]

6. a) $g_{4,3}^{\mathrm{RS}}(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4)(X-\alpha^5)(X-\alpha^6)$. This divides $X^{15}-1$ because all of its roots are also roots of $X^{15}-1$ by Fermat's little theorem (and they did not occur with multiplicity). [2]

b) i) For $n = 1,2$, $s^{(n)}(z) = \sum_{i=1}^{6} d^{(n)}(\alpha^i) z^{i-1}$. [2]

ii) This is because $d^{(n)}(X)$ may have coefficients not in $\mathbb{B}$. If $d^{(n)}(X) = \sum_j a_j X^j \in F[X]$, then

$$\begin{aligned} d^{(n)}(\alpha^{2i}) &= \sum_j a_j \alpha^{2ij} \\ \left(d^{(n)}(\alpha^i)\right)^2 &= \left(\sum_j a_j \alpha^{ij}\right)^2 = \sum_j a_j^2 \alpha^{2ij} \end{aligned}$$

and they do not have to equal unless $a_j^2 = a_j$ for all j; i.e., $d^{(n)}(X) \in \mathbb{B}[X]$. [2]

iii) Since the syndrome polynomials for both are not zero, some error has occurred in both received words. [2]

c) Let $s(z) := s^{(1)}(z)$, for simplicity, and apply Euclid's algorithm for $s(z)$ and z^6:

Step 1 $z^6 = (\alpha^{13}z^2 + \alpha^5)s(z) + r_1(z)$ where $r_1(z) = \alpha^{11}z^3 + \alpha^4 z^2 + \alpha^3 z + \alpha$.
Step 2 $s(z) = (\alpha^6 z + \alpha^{14})r_1(z) + r_2(z)$ where $r_2(z) = \alpha^3 z^2 + \alpha z + \alpha^{12}$.

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

$$\begin{aligned} r_2(z) &= s(z) + (\alpha^6 z + \alpha^{14})r_1(z) \qquad \ldots \text{Step2} \\ &= s(z) + (\alpha^6 z + \alpha^{14})\Big((\alpha^{13}z^2 + \alpha^5)s(z) + z^6\Big) \qquad \ldots \text{Step1} \\ &\equiv (\alpha^4 z^3 + \alpha^{12}z^2 + \alpha^{11}z + \alpha)s(z) \bmod z^6 \end{aligned}$$

Therefore we get

$$\begin{aligned} l(z) &= \alpha^{14}(\alpha^4 z^3 + \alpha^{12}z^2 + \alpha^{11}z + \alpha) = \alpha^3 z^3 + \alpha^{11}z^2 + \alpha^{10}z + 1 \\ w(z) &= \alpha^{14} r_2(z) = \alpha^2 z^2 + z + \alpha^{11}. \end{aligned}$$

The next step is to find 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, $i = 0,1$ where the bits were erased. One can easily check that $l(1) = l(\alpha^{-1}) = 0$. By dividing $l(z)$ by $(1-z)(1-\alpha z)$, the quotient is $1-\alpha^2 z$ so the other root is α^{-2}. Hence the error positions are $0,1,2$.

Now we can obtain

$$\begin{aligned} e_0 &= w(1)(1-\alpha)^{-1}(1-\alpha^2)^{-1} = \alpha^{10} \\ e_1 &= w(\alpha^{-1})\alpha^{-1}(1-1\cdot\alpha^{-1})^{-1}(1-\alpha^2\cdot\alpha^{-1})^{-1} = \alpha^{12} \\ e_2 &= w(\alpha^{-2})\alpha^{-2}(1-1\cdot\alpha^{-2})^{-1}(1-\alpha\cdot\alpha^{-2})^{-1} = 1. \end{aligned}$$

From this, we find the error polynomial $e(X) = e_2X^2 + e_1X + e_0 = X^2 + \alpha^{12}X + \alpha^{10}$ and the corrected word:

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

[12]

d) Note that z^3 divides $s^{(2)}(z)$, so z^3 divides $r_i(z)$ for each step of Euclid's algorithm. Therefore we cannot produce an evaluator polynomial of degree < 3. Since the decoding algorithm always works if at most three symbols contains an error-bit, we conclude that at least 4 symbols that contains an error-bit. [5]