CODING THEORY: PRACTICE EXAM

Remark (Please read before you begin). There are only **four** questions on this practice exam; but in the actual exam there will be six questions, and you can choose to answer four of them. In the actual exam, all questions (1. through 6.) carry equal marks but the marks assigned to sub-parts in each questions may be different. (They will add up to the same mark in each of 6 questions.) In the actual exam, marks for all sub-parts of questions are indicated. Finally, do *not* expect that the actual exam would look very similar to this practice exam, although working out this practice exam would certainly help.

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	$*$

Remark (Please read before you begin). If you are stuck on some proof-subquestion, you may skip it and move on to the next subquestion and you may use the statement you skip to prove. For example, if you skip 3. a), you may still use this result to solve 3. b). If you skipped 3. a) but correctly solve 3. b) granting 3. a), you will receive the full credit for 3. b) and only lose credits for 3. a) that you skipped. The same principle applies to all questions of the practice exam and the actual exam.

Finally, do NOT expect that the actual exam will copy this practice exam, even in any weak sense. (In particular, I discourage you to solely focus on solving this practice exam and ignore to revise the other course materials.) Just use this only as a check-up at the very end.

1. Let $F := \mathbb{B}[\alpha]/\alpha^3+\alpha+1$ be a field with 2^3 elements. (You may grant that X^3+X+1 is irreducible and $\alpha \in F$ is primitive.) As usual, we identify the column vectors $(1,0,0)^\top, (0,1,0)^\top, (0,0,1)^\top$ with $\alpha^2, \alpha, 1 \in F$ respectively.

a) Complete the following table:

0	1	α	α^2	α^3	α^4	α^5	α^6
000	001	010	100				

b) i) Consider

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

Under this identification between F and $\mathbb{B}^3$, rewrite the check matrix H_3 as a 1×7 matrix $H_{3,1}$ with entries in F.

ii) Identify a binary vector $v := (v_6, \cdots, v_0) \in \mathbb{B}^7$ with a binary polynomial $v(X) := \sum_{i=0}^{6} v_i X^i \in \mathbb{B}[X]$. Show that Ham(3) is a cyclic code, and find the generator polynomial and the check polynomial. Make sure to explain why the generator polynomial you found defines a *cyclic* code. (*Hint:* Interpret the condition $H_{3,1} \cdot v = 0$ in terms of $v(X)$.)

c) i) Write down a check matrix and a generator polynomial for RS$(3,2)$, and explain why they define the "same code", and explain why the generator polynomial you found defines a *cyclic* code..

ii) Using systematic encoding, find the generator matrix for RS$(3,2)$ in standard form.

2. Let $F := \mathrm{GF}(q)$ for some $q := 2^k$, and choose a primitive element $\alpha \in F$. We identify, as usual, a vector $(a_{k-1}, \cdots, a_0) \in \mathbb{B}^k$ with $a_{k-1}\alpha^{k-1} + \cdots + a_0 \in F$. *You can receive half of the full credit if you give a correct solution for the case when $k = 4$ and α is the usual choice of primitive element (i.e., $\alpha^4 + \alpha + 1 = 0$).*

a) Write down the check matrix $V_{k,t}$ for $\mathrm{RS}(k,t)$ for any "small enough" t (more precisely, for any t with $2t < q-1$).

b) We identify vectors of F^{q-1} with a polynomial over F with degree $< q-1$ in the usual way. Write down a generator polynomial $g^{\mathrm{RS}}_{k,t}(X) \in F[X]$ which defines the same code $\mathrm{RS}(k,t)$. (Be sure to justify that the polynomial code with this generator polynomial is $\mathrm{RS}(k,t)$, and check that that $g^{\mathrm{RS}}_{k,t}(X)$ divides $X^{q-1} - 1$, hence it defines a cyclic code over F.)

c) For any $v, w \in F^{q-1}$, let $d(v,w)$ denote the distance between v and w. In this part, we show that the minimal distance of $\mathrm{RS}(k,t)$ is precisely $2t+1$.

i) Show that no non-zero vector $v \in F^{q-1}$ with at most $2t$ non-zero symbols satisfies $V_{k,t}v = 0$. You may use the following fact without proof:

$$\det\left(\begin{bmatrix} \alpha^{i_{2t}} \\ \vdots \\ \alpha^{(2t)i_{2t}} \end{bmatrix} \cdots \begin{bmatrix} \alpha^{i_1} \\ \vdots \\ \alpha^{(2t)i_1} \end{bmatrix}\right) \neq 0$$

where $i_1, \cdots, i_{2t}$ are any distinct $2t$ numbers between 0 and $q-2$. (*Hint:* Show the following claim: if $v = (v_{q-2}, \cdots, v_0) \in F^{q-1}$ is such that $v_j = 0$ for any $j \neq i_1, \cdots i_{2t}$, then v is not a codeword of $\mathrm{RS}(k,t)$ unless $v = 0$.)

ii) Show that the minimal distance of $\mathrm{RS}(k,t)$ is precisely $2t+1$. (*Hint:* Any $2t+1$ vectors in F^{2t} are linearly dependent over F. Using this, show that there exists a codeword v with $d(v,0) = 2t+1$.)

iii) The minimal distance of $\mathrm{BCH}(k,t)$ is at least $2t+1$ but it does not have to be exactly $2t+1$. Explain why the argument of the previous part does not work for BCH-codes in general.

3. Let F be a field with 2^k elements.

a) For any non-zero $\beta \in F$, consider a subset $F_\beta := \{\sum_n a_n \beta^n | \; a_n \in \mathbb{B}\}$.

i) Show that F_β is closed under addition and multiplication of F, and is a subfield of F.

ii) Show that F_β is the smallest subfield of F which contains β (i.e., any other subfield of F which contains β should contain F_β).

b) For this part, let $F := \mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. Find the smallest subfields of $\mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$ containing $\beta = \alpha^2 + \alpha$. Show that the smallest subfield of $\mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$ containing α is itself.

c) Let F be a field with q elements where $q = 2^k$.

i) Let k' be a positive integer which divides k, and let $q' := 2^{k'}$. (Note that q' divides q.) Consider the subset $F_{q'} := \{\gamma \in F | \; \gamma^{q'} = \gamma\}$. Show that $F_{q'}$ is closed under addition and multiplication of F, and is a subfield of F with q' elements.

ii) Let F' be any subfield of F with $2^{k'}$ elements. Show that k' divides k.

iii) Let $\alpha \in F$ be a primitive element (which exists by the primitive element theorem). Write down all the subfields of F in terms of α. Make sure to justify that they can be no other subfields. [1]

iv) Find all the subfields of $\mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$. Compare your answer with b).

[1] The same proof works if we replace $q = 2^k$ by $q = p^k$ for any prime number p.

4. Let $F := \mathbb{B}[\alpha]/\alpha^4+\alpha+1$ be a field with 2^4 elements. Throughout this question $\mathrm{RS}(4,3)$ is the Reed-Solomon code constructed using the primitive element α.

Assume that you have received a word which consists of 60 binary bits, we view this as a polynomial $d(X) \in F[X]$ with degree $\leqslant 14$ via the usual identification. Assume that you obtained:

$$d(\alpha) = \alpha^5, \qquad d(\alpha^2) = \alpha^3, \qquad d(\alpha^3) = \alpha^4, \qquad d(\alpha^4) = \alpha^3, \qquad d(\alpha^5) = d(\alpha^6) = 0$$

a) Show that any codeword for $\mathrm{RS}(4,3)$ is also a codeword for $\mathrm{RS}(4,2)$.

b) Assume that the transmitted message was encoded via $\mathrm{RS}(4,2)$.

i) Write down the syndrome polynomial $s(z)$ corresponding to $d(X)$, and determine if any error has occurred during transmission.

ii) Find the error polynomial via the decoding algorithm. Make sure to clearly label the error locator, the error evaluator, and the error positions, as well. If the decoding algorithm should fail to produce a corrected codeword, then explain in “practical” terms why it does not work.

c) Assume that the transmitted message was encoded via $\mathrm{RS}(4,3)$.

i) Write down the syndrome polynomial $s(z)$ corresponding to $d(X)$, and determine if any error has occurred during transmission.

ii) Find the error polynomial via the decoding algorithm. Make sure to clearly label the error locator, the error evaluator, and the error positions, as well. If the decoding algorithm should fail to produce a corrected codeword, then explain in “practical” terms why it does not work.

iii) Compare the above part with question b) ii). If any different phenomena occurred, explain the reason.

Remark. The following is a similar exercise to the one above, but has a very interesting and instructive feature. I strongly encourage you to do this: Redo the above question with the following syndromes:

$$d(\alpha) = 1, \quad d(\alpha^2) = \alpha^5, \quad d(\alpha^3) = \alpha^2, \quad d(\alpha^4) = \alpha^8, \quad d(\alpha^5) = 0, \quad d(\alpha^6) = \alpha^8$$

Remark. If you want to do more similar exercises, re-do the above question with the following syndromes:

$$d(\alpha) = d(\alpha^2) = 0, \quad d(\alpha^3) = \alpha^{13}, \quad d(\alpha^4) = \alpha^{11}, \quad d(\alpha^5) = \alpha^7, \quad d(\alpha^6) = \alpha^6$$

Here is another set:

$$d(\alpha) = \alpha^6, \quad d(\alpha^2) = (\alpha^3) = 0, \quad d(\alpha^4) = \alpha^3, \quad d(\alpha^5) = \alpha, \quad d(\alpha^6) = \alpha^{12}$$