Queen Mary
University of London

Main Examination period 2019

MTH6108 / MTH6108P: Coding Theory

Duration: 2 hours

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

You should attempt ALL questions. Marks available are shown next to the questions.

Calculators are not permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

Complete all rough work in the answer book and cross through any work that is not to be assessed.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any unauthorised notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiners: A. Saha

Question 1. [25 marks]

(a) Give the definitions of the following:

(i) a q-**ary alphabet**; **[1]**

(ii) a **word** of length n over an alphabet $\mathbb{A}$; **[2]**

(iii) the **Hamming space** $\mathbb{A}^n$; **[2]**

(iv) a q-**ary** (n,M,d)-**code**; **[3]**

(v) $A_q(n,d)$. **[2]**

(b) Let C be a ternary code of length 27 with 24 words and with minimum distance 6. Write down all the positive integers t for which C is t-**error-correcting**. (You do not need to justify your answer.) **[3]**

(c) For each of the following statements, state whether the statement is true or false. Justify your answers. (You may use any results from the module, as long as you state clearly which ones you are using.)

(i) $A_3(6,2) \leq 250$. **[4]**

(ii) $A_8(4,4) \geq 8$. **[4]**

(iii) $A_2(10,5) \geq 14$. **[4]**

Question 2. [25 marks]

(a) (i) Let $\mathbb{A} = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$, and let C and D be the codes over $\mathbb{A}$ given as below.

$$C = \{\heartsuit\heartsuit\diamondsuit\spadesuit, \heartsuit\diamondsuit\spadesuit\diamondsuit, \spadesuit\clubsuit\clubsuit\heartsuit\}, \quad D = \{\heartsuit\heartsuit\heartsuit\heartsuit, \diamondsuit\diamondsuit\diamondsuit\diamondsuit, \clubsuit\clubsuit\clubsuit\clubsuit\}$$

Determine, with justification, whether the codes C and D are **equivalent**. **[4]**

(ii) Let C and D be the **linear** codes over $\mathbb{F}_3$ given as below.

$$C = \{000, 001, 010, 011\}, \quad D = \{000, 200, 010, 210\}$$

Determine, with justification, whether the codes C and D are **equivalent as linear codes**. **[4]**

(b) Let $\mathbb{F}_q$ be a finite field and let C be a linear $[n,k]$ code over $\mathbb{F}_q$. Explain what is meant by

(i) the **dual code** $C^\perp$; **[2]**

(ii) a **parity-check matrix** for C; **[2]**

(iii) the **syndrome** of a word $w \in \mathbb{F}_q^n$. **[2]**

(c) Consider the linear code D over $\mathbb{F}_3$ given by

$$D = \{0000, 1011, 2022, 0121, 1102, 2110, 0212, 1220, 2201\}.$$

Answer the following questions (You are not required to show your working, but doing so may help you to gain marks if you make arithmetical errors.)

(i) What is the **dimension** of D? **[1]**

(ii) Write down a **generator matrix** for D. **[2]**

(iii) Write down a **parity-check matrix** for D. **[4]**

(iv) Write down a **syndrome look-up table** for D. **[4]**

Question 3. [25 marks]

(a) Define the **capacity** of a symmetric binary channel with symbol error probability p. **[2]**

(b) (i) Define the **rate** of a q-ary (n,M,d)-code. **[2]**

(ii) Let C be the linear code over $\mathbb{F}_2$ given by

$$C = \{v \in \mathbb{F}_2^5 : v_1 + v_2 + v_3 + v_4 + v_5 = 0\}.$$

Find the **rate** of C. (You are not required to show your working, but doing so may help you to gain marks if you make arithmetical errors.) **[3]**

(c) Let C be a code of length n over the alphabet $\mathbb{A} = \{0,1\}$. Define what is meant by a **nearest-neighbour decoding process** for C. **[3]**

(d) Let $C = \{000, 100, 111\}$ be a code over the alphabet $\mathbb{A} = \{0,1\}$ and suppose words are transmitted along a noisy symmetric channel with symbol error probability $1/3$.

(i) Write down a **nearest-neighbour decoding process** for C. **[4]**

(ii) Calculate the **word-error probability** for the word 111 in C for your chosen nearest-neighbour decoding process. **[4]**

(e) Let C be an $(n,2,n)$ code over $\mathbb{A} = \{0,1\}$. Prove that C is equivalent to the repetition code of length n. **[7]**

Question 4. [25 marks]

(a) Let C be the linear code over $\mathbb{F}_3$ given by

$$C = \{000, 011, 022, 102, 110, 121, 201, 212, 220\}.$$

Construct a **Slepian array** for C and use it to **decode** the word 222. (You do not have to show your working, but doing so may help you to gain marks if you make arithmetical errors.) **[6]**

(b) (i) Define the **binary Hamming code** $\mathrm{Ham}(r,2)$ for $r \geq 2$. **[4]**

(ii) Write down a **parity-check matrix** for $\mathrm{Ham}(3,2)$. **[3]**

(c) What is a **perfect** code? **[3]**

(d) What is the **redundancy** of a linear $[n,k]$ code? **[2]**

(e) When is an $[n,k,d]$-code a **maximum distance separable** (MDS) code? **[3]**

(f) Suppose $2 \leqslant r \leqslant q$. Explain how to construct an MDS code of length $q+1$ and redundancy r over $\mathbb{F}_q$ (there is no need to prove that your construction works). **[4]**

End of Paper.