Queen Mary University of London

Main Examination period 2023 – May/June – Semester B

MTH6018: Coding Theory

Duration: 2 hours

The exam is intended to be completed within **2 hours**. However, you will have a period of **2 hours** to complete the exam and submit your solutions.

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

All work should be **handwritten** and should **include your student number**. Only one attempt is allowed – **once you have submitted your work, it is final**.

In completing this assessment:

- You may use books and notes.
- You may use calculators and computers, but you must show your working for any calculations you do.
- You may use the Internet as a resource, but not to ask for the solution to an exam question or to copy any solution you find.
- You must not seek or obtain help from anyone else.

When you have finished:

- scan your work, convert it to a **single PDF file**, and submit this file using the tool below the link to the exam;
- e-mail a copy to **maths@qmul.ac.uk** with your student number and the module code in the subject line;

Examiners: I.D. Morris, A. Saha

Question 1 [13 marks].
Consider the two codes $\mathcal{C}$ and $\mathcal{D}$ over the alphabet $\mathbb{A} = \{\text{A, B, } \ldots, \text{ Y, Z}\}$ given by:

$$\mathcal{C} := \{\text{FRANCE, GREECE, LATVIA, SERBIA, SWEDEN}\}$$

and

$$\mathcal{D} := \{\text{ANGOLA, GAMBIA, MALAWI, UGANDA, ZAMBIA}\}.$$

(a) Compute the minimum distance of $\mathcal{C}$ and the minimum distance of $\mathcal{D}$. Justify your answer in each case. **[7]**

(b) For which values of $t > 0$, if any, are these two codes t-error-correcting? For which values are they t-error-detecting? In each case list **all** values of t for which this property holds. **[4]**

(c) Could the two codes $\mathcal{C}$ and $\mathcal{D}$ be equivalent? Give a brief justification for your answer. **[2]**

Question 2 [22 marks].
Recall that the **rate** of a q-ary (n, M, d)-code $\mathcal{C}$ is defined to be the quantity

$$R(\mathcal{C}) := \frac{\log M}{n \log q}.$$

(a) Let $\mathbb{A}$ be a q-ary alphabet and $\mathcal{D} \subseteq \mathbb{A}^n$ a q-ary (n, M, d)-code, where $d \geq 2$. Is it possible that we could have $R(\mathcal{D}) = 1$? Why, or why not? **[3]**

(b) If $\mathcal{E}$ is a linear $[n, k]$-code over $\mathbb{F}_q$, what is the rate of $\mathcal{E}$? More generally, which numbers in the range 0 to 1 can be the rate of a **linear** code of length n over $\mathbb{F}_q$ and which can not? Justify your answer with reference to a result from the course. **[4]**

(c) Write down the rate of the Reed-Muller code $\mathcal{R}(4, 7)$. **[3]**

(d) Write down the rate of the Hamming code $\text{Ham}(4, 8)$. **[3]**

(e) Let $\mathbb{A}$ be a q-ary alphabet and $\mathcal{C}_1 \subseteq \mathbb{A}^n$ a q-ary (n, M, d)-code, where $M \geq 2$. Recall that for any two words $u = u_1u_2 \cdots u_n$ and $v = v_1v_2 \cdots v_n$ in $\mathcal{C}_1$ we define $u||v$ to be the word $u_1u_2 \cdots u_nv_1v_2 \cdots v_n$. Define a new code by $\mathcal{C}_2 := \{u||v \colon u, v \in \mathcal{C}_1\}$.

(i) Show that $R(\mathcal{C}_2) = R(\mathcal{C}_1)$. **[5]**

(ii) Show that $d(\mathcal{C}_2) = d(\mathcal{C}_1)$. **[4]**

Question 3 [13 marks].
Decide which of the following statements are true and which are false. Give a brief justification for your answer in each case, stating which results from the course you use in your answer (if any).

(a) $A_4(3,3) > 4$ **[3]**

(b) $A_2(11,8) = 2$ **[5]**

(c) $A_4(8,5) > 236$. **[5]**

Question 4 [14 marks].
Consider the linear code $\mathcal{C}$ over $\mathbb{F}_3$ with generator matrix given by

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 2 & 2 & 0 & 0 \end{pmatrix}.$$

(a) Put the generator matrix G into standard form, making it clear at each stage which operations are being used. **[8]**

(b) Using the standard-form generator matrix obtained in your answer to (a), find a parity-check matrix H for a code equivalent to $\mathcal{C}$. **[3]**

(c) Is the parity-check matrix H which you constructed in (b) a parity-check matrix for the code $\mathcal{C}$ itself, or is it only a parity-check matrix for a code **equivalent** to $\mathcal{C}$? Justify your answer. **[3]**

Question 5 [10 marks].
Consider the following three matrices with entries in the field $\mathbb{F}_7$:

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

$$H_2 = \begin{pmatrix} 2 & 1 & 5 & 1 & 3 & 0 & 4 & 6 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$H_3 = \begin{pmatrix} 6 & 0 & 3 & 1 & 2 & 4 & 2 & 5 \\ 0 & 6 & 5 & 4 & 1 & 1 & 4 & 6 \end{pmatrix}.$$

For each of the three matrices H_1, H_2, H_3 decide whether or not that matrix is a parity-check matrix for (a version of) the Hamming code $\mathrm{Ham}(2,7)$. Justify your answer for each matrix. **[10]**

Question 6 [17 marks]. Consider the linear code $\mathcal{C}$ over $\mathbb{F}_2$ with parity-check matrix given by

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

(a) (i) Construct a syndrome lookup table for $\mathcal{C}$. Your answer should include any calculations involved in the construction. [**8**]

(ii) Use your syndrome lookup table to decode the word 01110. [**3**]

(b) (i) Give an example of a word in $\mathcal{C}$ which has weight 2. You should include any calculations or additional reasoning needed to justify your answer. [**3**]

(ii) Show that $\mathcal{C}$ cannot contain a word of weight 1. [**3**]

Question 7 [11 marks].
Consider the code $\mathcal{C}$ over $\mathbb{F}_7$ with the following parity-check matrix:

$$\begin{pmatrix} 0 & 1 & 3 & 0 & 1 \\ 4 & 4 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 3 \end{pmatrix}.$$

(a) Decide whether or not $\mathcal{C}$ is an MDS code. Give a brief justification for your answer. [**7**]

(b) Suppose that the above matrix is instead taken to be the parity-check matrix of a linear code $\mathcal{D}$ over $\mathbb{F}_5$. Is $\mathcal{D}$ an MDS code? Give a brief justification for your answer. [**4**]

End of Paper.