Queen Mary
University of London

Main Examination period 2017

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 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 shall 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: I. Tomašić

Question 1. [32 marks]

(a) Give the definitions of the following:

(i) a **code** of length n over an alphabet $\mathbb{A}$; **[1]**

(ii) the **distance** between two words; **[2]**

(iii) the **minimum distance** of a code; **[2]**

(iv) a q**-ary** (n, M, d)**-code**; **[2]**

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

(b) What does it mean to say that a code is t**-error-detecting**? **[2]**

(c) What does it mean to say that a code is t**-error-correcting**? **[3]**

(d) Suppose the minimum distance of a code is d. How many errors can the code detect? How many errors can it correct? **[3]**

(e) Prove or disprove the following statements, stating explicitly any theorems you use.

(i) $A_2(4, 2) \geq 4$. **[3]**

(ii) $A_2(8, 3) \geq 30$. **[6]**

(iii) $A_2(7, 4) \geq 9$. **[6]**

Question 2. [23 marks]

(a) (i) What is a **linear code** of length n over $\mathbb{F}_q$? **[1]**

(ii) What is a linear $[n, k, d]$-code over $\mathbb{F}_q$? **[2]**

(iii) What is a **generator matrix** of a linear code? How many rows and columns does a generator matrix of an $[n, k, d]$-code have? **[3]**

(b) Let C be a linear $[n, k, d]$-code over $\mathbb{F}_q$.

(i) What is the size of C? Prove your claim. **[4]**

(ii) State the **Singleton bound** for general (not necessarily linear) codes. **[2]**

(iii) State the **Singleton bound for linear codes**, relating the numbers n, k, d. Prove your statement, using parts (i) and (ii) of this question. **[4]**

(c) Let C be the linear code of length 4 over $\mathbb{F}_2$ spanned by the words 1100, 0011, 1010, 0101, 1001. Find a generator matrix of C. **[3]**

(d) Let D be the linear code given by

$$D = \{v \in \mathbb{F}_3^5 : v_1 + v_2 + 2v_3 + v_4 + 2v_5 = 0, v_1 + 2v_2 + v_3 + 2v_5 = 0\}.$$

Find a generator matrix for D. **[4]**

Question 3. [21 marks]

(a) Suppose C is a linear $[n,k]$-code over $\mathbb{F}_q$.

(i) What is the **dual code** $C^{\perp}$? **[2]**

(ii) What is a **parity-check matrix** for C? **[2]**

(iii) Suppose H is a parity-check matrix for C. State the **Minimum Distance Theorem for Linear Codes**, which explains how the minimum distance of C is related to the linear independence of the columns of H. **[2]**

(iv) What is the **syndrome** of a word $v \in \mathbb{F}_q^n$? **[2]**

(v) Explain how to construct a **syndrome look-up table** for C. **[2]**

(vi) Explain how to construct a nearest-neighbour decoding process for C using a syndrome look-up table. **[2]**

(b) Consider the binary code C with generator matrix

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

(i) Write down a parity-check matrix for C. **[2]**

(ii) Construct a syndrome look-up table for C and use it to decode the word 1010110. **[7]**

Question 4. [24 marks]

(a) What is a **perfect** code? **[2]**

(b) When is an $[n,k,d]$-code a **maximum distance separable** (MDS) code? **[2]**

(c) Define the q**-ary Hamming code** $\mathrm{Ham}(r,q)$ for $r > 0$ and a prime power q. **[4]**

(d) Let $C = \mathrm{Ham}(2,3)$ be the ternary Hamming code with parity-check matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

(i) Prove that C is self-dual, i.e., $C^{\perp} = C$. **[3]**

(ii) Find the minimum distance $d(C)$, explaining the method. **[4]**

(iii) Prove that C is perfect. **[4]**

(iv) Determine $A_3(4,3)$. Explain your reasoning. **[3]**

(v) Is C an MDS code? Justify your claim. **[2]**

End of Paper.