Queen Mary
University of London

B. Sc. Examination by course unit 2015

MTH6108: Coding Theory

Duration: 2 hours

Date and time: 26 May 2015, 14:30–16:30

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 awarded 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 workings 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.

Examiner(s): I. Tomašić

© Queen Mary, University of London (2015)

Question 1. (a) Give the definitions of the following:

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

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

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

(b) How many errors can an (n,M,d)-code correct? **[2]**

(c) State and prove the *Singleton bound*. State precisely any lemma used in the proof. **[6]**

(d) State the *Hamming bound*. **[3]**

(e) State the *Plotkin bound*. **[3]**

(f) Prove or disprove the following statements.

(i) $A_2(8,4) \geq 18$. **[2]**

(ii) $A_7(3,3) \geq 6$. **[2]**

(iii) $A_2(10,5) \geq 14$. **[2]**

Question 2. (a) Give the definitions of the following:

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

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

(iii) the *weight* of a word. **[1]**

(b) Prove that the minimum distance of a linear code equals the minimum weight of a non-zero word. **[4]**

(c) Find an example of a non-linear code where the minimum distance is not equal to the minimum weight of a non-zero word. **[2]**

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

(i) What is a *Slepian array* for C? **[2]**

(ii) What is a *nearest-neighbour decoding process* for C? **[2]**

(iii) Explain how to use a Slepian array for C to construct a nearest-neighbour decoding process for C. **[2]**

(e) Consider the binary code C with generator matrix

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

(i) Write down a Slepian array for C and use it to decode the word 1001. **[6]**

(ii) Assuming that the symbol error probability is $\frac{1}{5}$, compute the word error probability for the word 1111. **[4]**

© **Queen Mary, University of London (2015)**

Question 3. (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

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

(i) Construct a syndrome look-up table for C and use it to decode the word 101010. **[8]**

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

Question 4. (a) Define the *binary Hamming code* $\mathrm{Ham}(r,2)$ for $r \geq 0$. **[3]**

(b) Find a generator matrix for $\mathrm{Ham}(3,2)$ and compute its minimum distance. **[6]**

(c) Find a generator matrix for a binary $[8,4,4]$-code. **[3]**

(d) State the *Singleton bound for linear codes*. **[2]**

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

(f) Prove that an $[n,k,d]$-code is MDS if and only if every set of $n-k$ columns in its parity-check matrix is linearly independent. **[5]**

(g) Is the code over $\mathbb{F}_5$ with parity-check matrix

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

an MDS code? Justify your answer. **[4]**

End of Paper.

© Queen Mary, University of London (2015)