Queen Mary
University of London

MTH6108 / MTH6108P: Coding Theory

Duration: 2 hours

Date and time: 3rd of June 2016, 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

Question 1.

(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) State the **Singleton bound**. **[2]**

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

(d) State the **Plotkin bound**. **[4]**

(e) Prove or disprove the following statements.

(i) $A_2(7,4) = A_2(6,3)$. **[3]**

(ii) $A_3(13,3) \geqslant 3^{11}$. **[3]**

(iii) $A_7(2,1) \geqslant 47$. **[3]**

(iv) $A_2(13,7) \geqslant 10$. **[3]**

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]**

(b) (i) Define the relation of **equivalence** between linear codes. **[4]**

(ii) How does it differ from the notion of equivalence between general (not necessarily linear) codes? **[2]**

(iii) Find an example of two codes which are equivalent as general codes, one of them is linear and the other is not linear. **[3]**

(c) Let C and D be linear codes over $\mathbb{F}_3$ with generator matrices

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix} \quad \text{and} \quad H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Prove that C and D are equivalent as linear codes. **[4]**

(d) Prove that a linear code equivalent to C (above) cannot contain the word 002. **[4]**

Question 3.

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

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

(ii) 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]**

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

(iv) What is a **syndrome look-up table** for C? **[2]**

(v) What is a **nearest-neighbour decoding process** 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 ternary code C with generator matrix

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

(i) Find a parity-check matrix for C. **[3]**

(ii) Construct a syndrome look-up table for C and use it to decode the word 1221. **[7]**

(iii) Compute the minimum distance $d(C)$, explaining the method. **[3]**

Question 4.

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

(b) Prove that $\mathrm{Ham}(r,q)$ is a **perfect** 1-error-correcting code. State precisely any lemma used in the proof. **[5]**

(c) Find a parity-check matrix for $\mathrm{Ham}(3,3)$. **[3]**

(d) What is the maximal dimension of a ternary 1-error-correcting linear code of length 13? Prove your claim. **[3]**

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

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

(g) Find a parity-check matrix for a $[6,3,4]$-code over $\mathbb{F}_5$. **[4]**

End of Paper.