Queen Mary
University of London

B. Sc. Examination by course unit 2014

MTH6108 Coding Theory

Duration: 2 hours

Date and time: 05 June 2014, 10:00–12:00

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 may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best 4 questions answered will be counted.

Calculators are NOT permitted in this examination. The unauthorized use of a calculator constitutes an examination offence.

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

Important note: the Academic Regulations state that possession of unauthorized material at any time by a student who is under examination conditions is an assessment offence and can lead to expulsion from QMUL.

Please check now to ensure you do not have any notes, mobile phones or unauthorised electronic devices on your person. If you have any, then please raise your hand and give them to an invigilator immediately. Please be aware that 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. Disruption caused by mobile phones is also an examination 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 $\mathbb{A}$;

(ii) the *distance* between two words;

(iii) the *minimum distance* of a code; [5]

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

(v) $A_q(n,d)$.

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

(c) What does it mean to say that C 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? Prove your claims. [7]

(e) State and prove the *Hamming bound*. State precisely any lemma used in the proof. [5]

(f) Does there exist a binary 1-error-correcting code of length 7 and size 17? Explain. [3]

Question 2 (a) (i) What is a *linear code* of length n over $\mathbb{F}_q$?

(ii) What is a linear $[n,k,d]$-code over $\mathbb{F}_q$? [5]

(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?

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

(i) What is the size of C? Prove your claim.

(ii) State the *Singleton bound* for general (not necessarily linear) codes. [10]

(iii) State the *Singleton bound for linear codes*, relating the numbers n, k, d. Prove your statement, using the previous parts of this question.

(c) Let C be the linear code of length 5 over $\mathbb{F}_3$ spanned by the words 01120, 12012, 10102, 11222.

(i) Find a generator matrix of C.

(ii) What is the dimension of C? [4]

(d) Let D be the linear code given by

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

(i) Find a generator matrix for D.

(ii) What is the dimension of D? [6]

Question 3 (a) Suppose C is a linear $[n,k]$-code over $\mathbb{F}_q$.

(i) Define what is meant by a *coset* of C, and by a *leader* of a coset.

(ii) What is a *Slepian array* for C?

(iii) What is a *decoding process* for C? [6]

(iv) What is a *nearest-neighbour decoding process* for C?

(v) Explain how to use a Slepian array for C to construct a nearest-neighbour decoding process for C.

(b) Consider the ternary code C given by the generator matrix

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

(i) Write out all the codewords of C and find the minimum distance of C. [5]

(ii) Write down a Slepian array for C. [7]

(iii) Use it to decode the word 1212. [2]

(iv) Is C a *perfect code*? Justify your answer. [5]

Question 4 (a) Suppose C is a linear $[n,k]$-code over $\mathbb{F}_q$.

(i) What is a *parity-check matrix* for C? How many rows and columns does it have?

(ii) Explain how to produce a parity-check matrix from a generator matrix in standard form.

(iii) What is the *syndrome* of a word $v \in \mathbb{F}_q^n$? [12]

(iv) Using syndromes, how can we check whether a word $v \in \mathbb{F}_q^n$ belongs to C?

(v) What is a *syndrome look-up table* for C?

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

(b) Construct a syndrome look-up table for the binary code with generator matrix

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

and use it to decode the word 10101. [13]

Question 5 (a) Give a precise statement of the *Plotkin bound*. [5]

(b) Define the *binary Hamming code* $\mathrm{Ham}(r,2)$ for $r \geq 0$. Explain why the definition makes sense. [5]

(c) Let $C = \mathrm{Ham}(3,2)$.

(i) Find a parity-check matrix for $C^{\perp}$. [5]

(ii) Compute $d(C^{\perp})$, the minimum distance of $C^{\perp}$. Explain your calculation. [3]

(iii) Does there exist a general (not necessarily linear) code D whose length and minimal distance are equal to those of $C^{\perp}$ and whose size is larger than the size of $C^{\perp}$? Justify your claims. [7]

Question 6 (a) Give the definition of the *redundancy* of a linear code. [2]

(b) Suppose C is a linear code over $\mathbb{F}_q$, and 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. [3]

(c) Give the definition of a *maximum distance separable* (MDS) code of length n and redundancy r. [3]

(d) Let $a_1, \ldots, a_m$ be distinct elements of $\mathbb{F}_q$ and $2 \leq k \leq m$. Prove that any k columns of the matrix

$$\begin{bmatrix} 1 & \cdots & 1 & 0 \\ a_1 & \cdots & a_m & 0 \\ \vdots & & \vdots & \vdots \\ a_1^{k-1} & \cdots & a_m^{k-1} & 1 \end{bmatrix}$$

are linearly independent. [5]

(e) Now suppose $2 \leq r \leq q$. Explain how to construct an MDS code of length $q+1$ and redundancy r. [5]

(f) Find a generator matrix of a $[6,2,5]$-code over $\mathbb{F}_5$. [7]

End of Paper