This question paper consists of 6 printed pages, each of which is identified by the reference MATH5153M01.

All calculators must carry an approval sticker issued by the School of Mathematics.

School of Mathematics

January 2018

MATH5153M01

Advanced Coding Theory

Time Allowed: 3 hours

You must attempt to answer 4 questions.
If you answer more than 4 questions, only your best 4 answers will be counted towards your final mark for this exam.
All questions carry equal marks.

1. Let F be a field. We write $\mathcal{M}_{n,m}(F)$ for the set of $n \times m$ matrices with entries in field F. For example

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_{2,5}(\mathbb{Z}_2)$$

(a) If F is a field of order q, what is the size of $\mathcal{M}_{n,m}(F)$?

(b) Associated to each $M \in \mathcal{M}_{n,m}(F)$ is the row space $R(M)$ of M. This is the vector space over F spanned by the rows of M (regarded as vectors). Under what conditions is M a generator matrix for a linear code; and what are the block length and dimension of the code it then generates?

(c) Write down the binary linear code C_1 with generator matrix

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

(d) Consider the following sets: $S_1 = \{000000, 000100, 100000\} \subset \mathbb{Z}_3^6$;

$$S_2 = \{0000, 0001, 1000, 1001\} \subset \mathbb{Z}_2^4;$$

$$S_3 = \{00000, 01110, 01000, 00110\} \subset \mathbb{Z}_2^5;$$

$$S_4 = \{0000, 0001, 1000, 1001\} \subset \mathbb{Z}_5^4.$$

Determine which of these are linear codes (giving the reasons for your answers).

(e) Define the minimum weight $w(C)$ for a code C over a symbol set that is a field. Prove that, for a linear code, the minimum distance $d(C)$ is equal to $w(C)$.

(f) Define $C^{\perp}$, the dual code to a linear code C. Prove that $C^{\perp}$ is also a linear code.

(g) A linear code is self-dual if $C^{\perp} = C$. Compute the dual of C_1 above, and hence or otherwise determine if it is self-dual.

(h) Find in standard form the generator matrix for a linear code $C \subseteq \mathbb{Z}_{11}^4$ such that C is self-dual.

2. Let Σ_q denote a set of symbols (an 'alphabet') of size q. That is, $|\Sigma_q| = q$. We shall assume that there is a 'zero' element $0 \in \Sigma_q$.

   (a) Explain carefully what is meant by the Cartesian product of two sets.

   We write $\Sigma_q^2 = \Sigma_q \times \Sigma_q$ for the Cartesian product of Σ_q with itself. Explain what is meant by the the n-th Cartesian power of Σ_q, denoted Σ_q^n. Illustrate your answer by writing out all elements of $\{0, 1\}^3$ explicitly, carefully explaining any notation you use.

   (b) A q-ary code of length n is a subset of Σ_q^n. How many of these are there (as a function of q and n).

   (c) i. Define the Hamming distance d on Σ_q^n.

   ii. Note that $00...0 \in \Sigma_q^n$. How many elements of Σ_q^n have Hamming distance 2 or less from the element 00...0?

   iii. Define the minimum distance $d(C)$ of a code $C \subset \Sigma_q^n$.

   iv. Given that code C is 7 error correcting, what is the smallest that $d(C)$ could be.

   v. State the ball-packing bound on the size M of a q-ary (n, M, d)-code C.

   (d) For each of the following triples (n, M, d) construct, if possible, a binary (n, M, d)-code:

   $$(9, 2, 9) \qquad (3, 8, 1) \qquad (4, 8, 2) \qquad (8, 80, 3)$$

   If no such code exists, then prove it, stating any theorems used.

   (e) Suppose that the probability of error in transmission of a single digit down a symmetric channel is $p < 1/2$. Show that, given a particular message w received, and a codeword v such that $d(w, v)$ is minimal, then there is no better guess than v for the transmitted codeword.

3. (a) Let $\mathbb{Z}_4$ denote the set of integers modulo 4, together with the associated mod.4 arithmetic. Give the multiplication table for $\mathbb{Z}_4$. Explain why this number system of modulo 4 arithmetic does *not* form a field.

(b) Explain a way to construct a field of order 4. Write down the addition and multiplication tables for this field.

(c) Let $C \subset \mathbb{Z}_7^5$ be the linear code with generator matrix

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

i. By a suitable row permutation, bring this matrix G' into a standard form G. Hence write down a parity check matrix H for C.

ii. Compute the matrix $G.H^t$ (where H^t is the transpose of H). Interpret your result.

iii. Show that $d(C) = 3$.

iv. How many of the coset leaders of C have weight 1?

v. Codeword x is transmitted down a noisy channel, so that $y = 11254$ is received, with exactly one error having occured. What was the transmitted codeword x?

4. Let C be the binary linear code with generator matrix

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

(a) Construct a standard array for C.

(b) Decode the received message 1101 using your array.

(c) Code C is transmitted down a binary symmetric channel with symbol error probability $p = 0.01$, with the received vectors being decoded by the coset decoding method. Let x denote the sent word, and y the received word, so that $e = y - x$ is the transmission error vector. Then $P(e = 0000)$ denotes the probability of a codeword being transmitted without error. What is $P(e = 0000)$? Explain why the probability of a transmitted word being decoded correctly can be written as

$$P_{corr}(C) \;=\; P(e = 0000) + P(e = 1000) + P(e = 0100) + P(e = 1100)$$

(Hint: Here $P(e = 1100) = P(e = 1010)$ and so on.)
Calculate $P_{err}(C)$, the word error probability of the code; and $P_{undetec}(C)$, the probability of there being an undetected error in a transmitted word.

(d) Code C is again transmitted down a binary symmetric channel with symbol error probability $p = 0.01$, but is now used only for error detection. If an error is detected in a received vector, the receiving device requests retransmission of the codeword. Calculate $P_{retrans}(C)$, the probability that a single codeword transmission will result in a request to retransmit.

(e) Give the definition of the syndrome of a received word. Prove that two words have the same syndrome if and only if they lie in the same coset of the code C.

5. (a) Let F_q be a field of order q. Explain how we may think of a q-ary code of block length n as a subset of the ring $F_q[x]/(x^n - 1)$.

   Let $g(x) = x^3 + x^2 - x - 1 \in \mathbb{Z}_3[x]$ be the generator polynomial of a 3-ary [6,3] cyclic code C. Determine the generator polynomial $g^{\perp}(x)$ of the dual code $C^{\perp}$. Determine a parity check matrix and a generator matrix for C.

   (b) Suppose that $C_1, C_2 \subseteq F_q^n$ are cyclic codes.

   Let C denote the smallest linear code containing both C_1 and C_2. Show that C is cyclic. Let $g_1(x)$ and $g_2(x)$ be generator polynomials for C_1 and C_2 respectively. Prove that the monic polynomial that is the greatest common divisor of g_1 and g_2 is the generator polynomial for C.

   (c) Write down a parity check matrix H for the Hamming code $C = Ham(\mathbb{Z}_5^2)$ such that H has first column $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. For what values of the parameters n, k, d is this C an $[n, k, d]$-code. Determine a generator matrix for C.

End.