THE UNIVERSITY OF MANCHESTER

CODING THEORY

FORMATIVE TEST

Release Date: Thursday 28th May 2020, 09:00
Submission Deadline: Thursday 4th June 2020, 09:00

Answer ALL THREE questions in Section A.Answer TWO of the THREE questions in Section B.

Electronic calculators may be used in accordance with the University regulations

---

IMPORTANT INSTRUCTIONS AND INFORMATION ABOUT THIS FORMATIVE TEST

- This assessment is for formative purposes only
    - No numerical feedback will be issued
    - This assessment will not contribute to your year average
    - Formative assessment will not be used by examination boards
- This assignment link will remain open for 7 days
- Please submit one file per submission.
    - For instance: if you have taken pictures of your written work and have several JPEG files, please combine them into one PDF Document
    - Students can convert multiple JPEG files into a single PDF file here: **http://www.elearning.fse.manchester.ac.uk/wp-content/uploads/2020/03/Hand-drawn-to-PDF.pdf**
- You do not need to include your name or student ID number on your submission. You will be logged into Bb9 using your personal log in and it will recognise this when you submit the assignment.
- If you are unable to submit work via Bb9 for technical reasons, please email: mathematics@manchester.ac.uk
- If you do not receive an email confirmation to confirm receipt of your submission, your attempt was unsuccessful, so please resubmit again.

SECTION A

Answer **ALL** questions in this section

A1.

(a) Let C be a linear code in $\mathbb{F}_q^n$. Explain what is meant by:

1. the weight $w(\underline{\mathrm{x}})$ of a vector $\underline{\mathrm{x}}$;
2. the weight $w(C)$ of C;
3. a generator matrix of C;
4. the inner product $\underline{\mathrm{x}} \cdot \underline{\mathrm{y}}$ of vectors $\underline{\mathrm{x}}$, $\underline{\mathrm{y}}$;
5. the dual code $C^{\perp}$.

(b) If H is a matrix with n columns over $\mathbb{F}_q$, prove that $C = \{\underline{\mathrm{x}} \in \mathbb{F}_q^n \mid \underline{\mathrm{x}} H^T = \underline{0}\}$ is a linear code.

(c) Let E_5 denote the binary even weight code of length 5. Write down a generator matrix of E_5.

(d) Write down a generator matrix of $(E_5)^{\perp}$. Identify the code $(E_5)^{\perp}$ by its well-known name.

A2.

(a) State the Distance Theorem for linear codes.

Let C be the binary linear code with parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$.

(b) State the length and the dimension of C.

(c) Using the Distance Theorem, find the minimum distance $d(C)$ of C.

(d) How many errors can the code detect?

(e) How many errors can the code correct?

(f) Find three vectors of weight 1 with pairwise distinct syndromes.

(g) Using (f), write down a set of coset leaders. Calculate the table of syndromes, and decode the vectors 000101 and 111000 using syndrome decoding.

(h) If the code C is transmitted down a binary symmetric channel with bit error rate r, write down a formula for $P_{\mathrm{corr}}(C)$, the probability that a received vector is decoded correctly.

A3.

(a) Define projective $(r-1)$-space, $\mathbb{P}_{r-1}(\mathbb{F}_q)$.

(b) Define a Hamming code $\mathrm{Ham}(r,q)$.

(c) Write down, without proof, formulas for the length n, dimension k and minimum distance d of $\mathrm{Ham}(r,q)$.

(d) Let C be a $\mathrm{Ham}(2,3)$ code. In the following, you may quote any result from the course without proof:

1. Write down a generator matrix for C.
2. Show that C is a self-dual code, that is, $C^{\perp} = C$.
3. Show that $\mathrm{Ham}(r,q)$ is not a self-dual code if $r > 2$.

SECTION B

Answer **TWO** of the three questions in this section.

B4.

(a) Define the Hamming sphere $S_t(\underline{u})$ with centre $\underline{u}$ and radius t in the vector space $\mathbb{F}_q^n$.

(b) Write down a formula for $\#S_t(\underline{u})$, the number of elements in $S_t(\underline{u})$.

(c) Let C be a code in $\mathbb{F}_q^n$. Show that if $t < \frac{d(C)}{2}$, $\underline{u}, \underline{v} \in C$, $\underline{u} \neq \underline{v}$, then $S_t(\underline{u}) \cap S_t(\underline{v}) = \varnothing$.

(d) State and prove the Hamming bound for the number M of elements of a code in $\mathbb{F}_q^n$ of minimum distance d.

(e) Show that a k-dimensional linear code in $\mathbb{F}_2^n$ of minimum distance 3 satisfies $k \leq n - \log_2(n+1)$.

(f) Define what is meant by a perfect code.

(g) State without proof for which pairs (q, d) where q is a prime there exists a perfect q-ary code of minimum distance d. Name a perfect code corresponding to each pair.

B5. In this question, we assume that vectors in $\mathbb{F}_q^n$ are identified with polynomials, in, $\mathbb{F}_q[x]$, of degree less than n in the usual way.

(a) What is a cyclic code? What are the properties required of a polynomial $g(x) \in \mathbb{F}_q[x]$ to be a generator polynomial of some cyclic code of length n over $\mathbb{F}_q$?

(b) Given that $g(x)$ is the generator polynomial of a cyclic code C in $\mathbb{F}_q^n$, write down a generator matrix for C in terms of the coefficients of g.

You are given that, in $\mathbb{F}_3[x]$,

$$x^8 - 1 = (x^5 - x^4 + x - 1)(x^3 + x^2 + x + 1).$$

(c) Write down a generator polynomial and a check polynomial for a ternary cyclic code D of length 8 and dimension 5.

In the rest of the question, D refers to the code that you obtained in part (c).

(d) Let $a, b, c \in \mathbb{F}_3$ be such that the vector $ab00000c$ is a codeword of D. Show that $a = b = c = 0$.

(e) Does D contain codewords of weight 2? If so, write down a codeword of D of weight 2.

B6.

(a) Let C_1, C_2 be linear codes in $\mathbb{F}_q^n$.

1. Define the code $|C_1|C_2|$.
2. Prove that $d(|C_1|C_2|) \geq \min\{2d(C_1), d(C_2)\}$.

(b) Define the rth order Reed-Muller code $R(r, m)$ in terms of Boolean functions.

(c) Explain why $R(r+1, m+1) = |R(r+1, m)|R(r, m)|$.

(d) Give an example of a Reed-Muller code $R(r, m)$ which has relative distance $\delta = 0.5$.

(e) You are given that C is some linear code in $\mathbb{F}_2^n$ which has relative distance $\delta > 0.5$ and contains the codeword $11\ldots1$ (where all n bits are 1). Prove that $\dim C = 1$.

END OF FORMATIVE TEST