Two hours

THE UNIVERSITY OF MANCHESTER

CODING THEORY

21 May 2018

14:00 – 16:00

Answer ALL THREE questions in Section A (40 marks in total). Answer TWO of the THREE questions in Section B (40 marks in total). If more than TWO questions from Section B are attempted, then credit will be given for the best TWO answers.

University approved calculators may be used

SECTION A

Answer **ALL** questions in this section (40 marks in total)

A1. (a) Define what is meant by:

— the *weight* $w(\underline{x})$ *of a vector* $\underline{x} \in \mathbb{F}_q^n$;

— a *linear code* C of length n over the field $\mathbb{F}_q$;

— the *weight* $w(C)$ *of a linear code* C;

— the *inner product* $\underline{x} \cdot \underline{y}$ of vectors $\underline{x}, \underline{y} \in \mathbb{F}_q^n$;

— the *dual code*.

(b) Consider the binary code $C = \{\underline{x} \in \mathbb{F}_2^n : \underline{x} \cdot \underline{x} = 0\}$ of length n where $n \geqslant 2$. Explain why C is a linear code. State without proof the cardinality, the dimension and the weight of C. Identify the code C by its well-known name.

[10 marks]

A2.

(a) Let an $(n-k) \times n$ check matrix H for a q-ary linear code C be given. What is meant by a *table of syndromes* for C? How many rows does such a table have? Explain how to decode a received vector using the table of syndromes.

From now on, let D be the binary linear code with parity check matrix $H = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$.

(b) Construct a table of syndromes for D and use it to decode the vector 11100.

(c) Use the table of syndromes constructed in (b) to show that if the code D is transmitted via $BSC(p)$, then the probability $P_{\mathsf{corr}}(D)$ that the received vector is decoded correctly is $(1-p)^3$.

(d) Write down the probability that an unencoded three-bit message, sent via $BSC(p)$, is received without errors. Compare this probability with $P_{\mathsf{corr}}(D)$ from part (c) and determine whether encoding three-bit messages using the code D improves *error correction* if transmitting via $BSC(p)$. Suggest one possible advantage and one disadvantage of using the code D versus transmitting unencoded messages of length 3.

[20 marks]

A3.

(a) Consider the Reed-Muller code $R(r, m)$ where $0 \leqslant r < m$. Write down the parameters $[n, k, d]_q$ of this code. State without proof which Reed-Muller code coincides with $R(r, m)^\perp$. Hence write down the condition on r and m equivalent to $R(r, m)$ being self-dual. Explain briefly why $R(r, m)$ is self-orthogonal, if and only if $r < m/2$.

(b) Use the result of (a) to prove that all Reed-Muller codes of dimension 2018 are self-orthogonal codes.

[10 marks]

SECTION B

Answer **TWO** of the three questions in this section (40 marks in total).
If more than TWO questions from this section are attempted, then credit will be given for the best TWO answers.

B4. (a) State without proof the *Hamming bound* for codes in $\mathbb{F}_q^n$ of minimum distance d. Define what is meant by a *perfect code*. Name a perfect code of minimum distance 9.

(b) Prove that if the minimum distance of a code is even, then the code is not perfect. You can use any other facts from the course without proof, but you should state the facts you use.

(c) Let $C \subseteq \mathbb{F}_q^n$ be a linear code. Define what is meant by a *generator matrix* of C. Assuming that C has a generator matrix G such that all rows of G have even weight: (i) Show that if $q = 2$, then C is not a perfect code. (ii) If $q = 3$, can such a code C be perfect? Justify your answer.

(d) A ternary linear code C has a generator matrix G with the following property: if the last row of G is removed, the remaining rows form a generator matrix of a ternary Golay code. Find all the possible values of the parameters $[n, k, d]_3$ of such codes C and justify your answer. Any results from the course can be used without particular comment. [20 marks]

B5. In this question, Z is the ternary linear code with generator matrix $\begin{bmatrix} 1 & 0 & 1 & 2 \\ 1 & 2 & 0 & 1 \end{bmatrix}$.

(a) What is meant by saying that a generator matrix G of a linear code $C \subseteq \mathbb{F}_q^n$ is in *standard form*? Given G in standard form, explain how one can find a generator matrix for the dual code $C^\perp$. Define what is meant by the *weight enumerator* $W_C(x, y)$.

(b) List the codevectors of Z and find the weight enumerator $W_Z(x, y)$ of Z.

(c) State the *MacWilliams identity* for q-ary linear codes. Using the MacWilliams identity, or otherwise, for each $i = 0, 1, 2, 3, 4$ calculate the number of codevectors of weight i in the dual code $Z^\perp$.

(d) Let $D \subseteq \mathbb{F}_q^{2q}$ be a linear code which consists of the zero vector and $(q-1)^3$ vectors of weight q. Show that $w(D^\perp) = 1$. Find all q for which a code D with these properties exists. [20 marks]

B6. (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) Factorise $x^3 - 1$ into irreducible polynomials in $\mathbb{F}_3[x]$. Hence list all the cyclic codes in $\mathbb{F}_3^3$, stating the cardinality, the minimum distance, a generator polynomial and a generator matrix for each code.

(c) Let C be a linear code. Prove that C is cyclic, if and only if $C^\perp$ is cyclic.

(d) For a prime p, let $I_p = \{(a_1, \ldots, a_{p-1}) \in \mathbb{F}_p^{p-1} \mid \sum_{i=1}^{p-1} i a_i = 0 \text{ in } \mathbb{F}_p\}$.

i. What are the odd primes p for which I_p is an MDS code?
ii. What are the odd primes p for which $I_p^\perp \subseteq I_p$?
iii. What are the odd primes p for which I_p is a cyclic code?

Justify your answer in each case. Any facts from the course can be freely used. [20 marks]

END OF EXAMINATION PAPER