

B. Sc. EXAMINATION BY COURSE UNIT

MAS309 Coding Theory

5th June, 2008, 10:00 – 12:00

The duration of this examination is 2 hours.

*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 **FOUR** questions will be counted.*

Electronic calculators are not permitted.

**YOU ARE NOT PERMITTED TO START READING THIS QUESTION PAPER
UNTIL INSTRUCTED TO DO SO BY AN INVIGILATOR**

Question 1. This question concerns the two ternary codes

$$\mathcal{C}_0^n = \{x_1x_2 \dots x_n \in \mathbb{F}_3^n : x_1 + x_2 + \dots + x_n = 0 \pmod{3}\},$$

$$\mathcal{C}_1^n = \{x_1x_2 \dots x_n \in \mathbb{F}_3^n : x_1 + x_2 + \dots + x_n = 1 \pmod{3}\}.$$

(\mathcal{C}_0^n is the ternary “parity check” code of length n .)

- (a) What is meant by a *ternary* (n, M, d) -code? [3]
- (b) Prove that \mathcal{C}_0^n has 3^{n-1} codewords. [4]
- (c) Prove that \mathcal{C}_0^n has minimum distance 2. [5]
- (d) By exhibiting a suitable bijection $f : \mathcal{C}_0^n \rightarrow \mathcal{C}_1^n$ between the codes \mathcal{C}_0^n and \mathcal{C}_1^n , demonstrate that \mathcal{C}_0^n and \mathcal{C}_1^n are equivalent (as not necessarily linear) codes. Hence deduce that \mathcal{C}_1^n is a $(n, 3^{n-1}, 2)$ -code. [6]
(Hint: f need only change one coordinate.)
- (e) Prove that \mathcal{C}_0^n is a linear code, but that \mathcal{C}_1^n is *not* a linear code. [4]
- (f) Explain how the definition of equivalence of codes is usually tightened so that any code equivalent to a linear code is necessarily linear. [3]

Question 2. Suppose \mathcal{C} is a binary code of length n .

- (a) What does it mean for \mathcal{C} to be *t-error-correcting*? for \mathcal{C} to have *minimum distance d*? Prove that if \mathcal{C} has minimum distance at least $2t + 1$ then \mathcal{C} is *t-error-correcting*. (The converse is also true, but you are not required to prove this.) [5]
- (b) For x a codeword in \mathcal{C} , define the sphere $S(x, t)$, and prove that the number of words in $S(x, t)$ is

$$|S(x, t)| = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}. \quad [6]$$

- (c) Deduce that if \mathcal{C} is *t-error-correcting*, then

$$|\mathcal{C}| \leq \left\lfloor \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}} \right\rfloor. \quad [5]$$

- (d) Evaluate the bound from part (c) in the case $n = 7$ and $t = 1$. Show that the bound is attainable, i.e., that a 1-error-correcting binary code of length 7 with this number of words does exist. (Note. You may refer to any of the explicit codes described in the course.) [4]
- (e) Evaluate the bound from part (c) in the case $n = 7$ and $t = 2$. Show that the bound is *not* attainable, i.e., that no 2-error-correcting binary code of length 7 with this number of words exists. (Note. You may use any of the upper bounds of the course without proof.) [5]

Question 3. (a) Suppose \mathcal{C} is a binary (n, M, d) -code. Define

$$\mathcal{C}_0 = \{x_1x_2 \dots x_{n-1} : x_1x_2 \dots x_{n-1} 0 \in \mathcal{C}\}$$

and

$$\mathcal{C}_1 = \{x_1x_2 \dots x_{n-1} : x_1x_2 \dots x_{n-1} 1 \in \mathcal{C}\}$$

Thus \mathcal{C}_0 is obtained by taking all the codewords in \mathcal{C} that end in 0, and stripping off that final 0; and \mathcal{C}_1 is obtained in a similar manner from codewords that end in 1. Prove that \mathcal{C}_0 is a $(n-1, M_0, d)$ -code for some M_0 (and hence that \mathcal{C}_1 is a $(n-1, M_1, d)$ -code for some M_1). [6]

(b) Deduce that there exists a binary $(n-1, M', d)$ -code \mathcal{C}' with $M' \geq M/2$. [4]

(c) Now suppose, in addition, that d is odd. Describe how to construct from \mathcal{C}' a binary $(n, M', d+1)$ -code \mathcal{C}'' . (You do not need to prove that the \mathcal{C}'' has minimum distance $d+1$.) [4]

(d) The following is a binary $(10, 12, 5)$ -code:

$$\mathcal{C} = \left\{ \begin{array}{l} 0000000000, \\ 1010001110, \\ 1101000111, \\ 0110100011, \\ 1011010001, \\ 1101101000, \\ 1110110100, \\ 0111011010, \\ 0011101101, \\ 0001110110, \\ 1000111011, \\ 0100011101 \end{array} \right\}.$$

Use the constructions from the previous parts of the question to write down a binary $(10, 6, 6)$ -code \mathcal{C}'' . Briefly describe the process you went through in constructing \mathcal{C}'' from \mathcal{C} . [7]

(e) Is the code \mathcal{C} from the previous part linear? Briefly justify your answer. [4]

- Question 4.** (a) Explain what it means for \mathcal{C} to be a *linear* $[n, k]$ -code over \mathbb{F}_q . [4]
- (b) Define the *weight* $w(v)$ of a codeword v . Prove that the minimum distance of a linear code \mathcal{C} is equal to the minimum weight $w(v)$ of any non-zero codeword $v \in \mathcal{C}$. [5]
- (c) Suppose \mathcal{C} is an $[n, k]$ -code over \mathbb{F}_q . Explain what it means for a matrix G over \mathbb{F}_q to be a *generator matrix* for \mathcal{C} . How many rows and columns does G have? [4]
- (d) It is a theorem (which you are not asked to prove) that every linear code is equivalent to a code with generator matrix in “standard form”. Describe the *standard form* for a generator matrix. Illustrate the process of transforming a generator matrix to standard form by transforming the particular matrix

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

- (over \mathbb{F}_2) to standard form using the allowed matrix operations. Show each intermediate step of the process. [6]
- (e) Prove that there is a unique (up to equivalence) binary $[6, 2]$ -code with minimum distance 4. [6]
(Hint: Start with a generator matrix for the code in standard form. Argue that the condition on minimum distance places severe constraints on the matrix entries.)

- Question 5.** (a) Suppose \mathcal{C} is an $[n, k]$ -code over \mathbb{F}_q , with generator matrix G . Define the *dual code* \mathcal{C}^\perp of \mathcal{C} . Prove that \mathcal{C}^\perp is an $[n, n - k]$ -code. [6]
(Note: you may use standard results from linear algebra, provided they are correctly stated.)
- (b) Write down conditions involving matrices G and H that express the situation that H is a *parity-check matrix* for \mathcal{C} . What is the relationship between H and the dual code \mathcal{C}^\perp ? [3]
- (c) Given a matrix G in standard form, show how to write down a parity-check matrix H for the code \mathcal{C} generated by G . [4]
- (d) Write down a parity-check matrix H for the ternary $[4, 2]$ -code \mathcal{C} with generator matrix

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

- (Note that G is in standard form.) [3]
- (e) Construct a syndrome look-up table for H . Explain how the syndrome look-up table determines a decoding process for \mathcal{C} , and illustrate this process by decoding the word 2211. [9]

- Question 6.**
- (a) Define the quantity $A_q(n, d)$. [2]
 - (b) State (without proof) an inequality relating $A_q(n, d)$ and $A_q(n - 1, d - 1)$, for $n \geq d \geq 2$. Deduce the bound $A_q(n, d) \leq q^{n-d+1}$, for $n \geq d \geq 1$. [4]
 - (c) What is meant by the *redundancy* of a linear $[n, k]$ -code? What is meant by a *maximum distance separable code* (MDS code) of length n and redundancy r ? [3]
 - (d) Write down the parity-check matrix H of a linear $[8, 5, 4]$ -code over \mathbb{F}_7 , explaining the method you used to construct it. Which property of the matrix H ensures that the associated code has minimum distance 4? (You need not check that H indeed has this property.) [8]
 - (e) Deduce that $A_7(8, 4) = 7^5$. [3]
 - (f) Write down some codeword of weight 4 from the $[8, 5, 4]$ -code just constructed. Use it to identify a non-trivial linear relationship between four columns of the parity-check matrix H from part (d). [5]

End of examination paper

Solutions

- Question 1.** (a) [Standard definition] A ternary (n, M, d) -code \mathcal{C} is one with M codewords over the alphabet \mathbb{F}_3 , all of length n , such that $\min\{d(u, v) : u, v \in \mathcal{C}, u \neq v\} \geq d$.
- (b) [Similar to a coursework question.] Choose $x_1, \dots, x_n \in \mathbb{F}_3$ arbitrarily: there are 3^{n-1} ways to do this. Now the final symbol x_n is uniquely determined by the condition

$$x_n = -(x_1 + \dots + x_{n-1}) \pmod{3}.$$

- (c) [Ditto.] Suppose \mathcal{C}_0^n had two codewords x, y at Hamming distance 1. Then x, y agree in $n-1$ positions, say $1, 2, \dots, n-1$, without loss of generality. So $x_1 = y_1, \dots, x_{n-1} = y_{n-1}$. But now

$$x_n = -(x_1 + \dots + x_{n-1}) = -(y_1 + \dots + y_{n-1}) = y_n,$$

a contradiction. So \mathcal{C}_0^n has minimum distance at least 2. There are clearly some pairs of words that achieve this distance, e.g., $0 \dots 000$ and $0 \dots 012$

- (d) [Unseen.] Let σ be the permutation $\sigma = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$. We claim that $f : \mathcal{C}_0^n \rightarrow \mathbb{F}_3^n$ defined by $f(x_1 \dots x_n) \mapsto x_1 \dots x_{n-1} \sigma(x_n)$ is a bijection between \mathcal{C}_0^n and \mathcal{C}_1^n . If $x = x_1 \dots x_n \in \mathcal{C}_0^n$, then

$$x_1 + \dots + x_{n-1} + \sigma(x_n) = x_1 + \dots + x_{n-1} + x_n + 1 = 1 \pmod{3},$$

and hence $f(x) \in \mathcal{C}_1^n$. To see f is a bijection, consider the explicit inverse $f^{-1}(x_1 \dots x_n) = x_1 \dots x_{n-1} \sigma^{-1}(x_n)$.

Equivalent codes have equal cardinality and equal minimum distance, so \mathcal{C}_1^n is a $(n, q^{n-1}, 2)$ -code.

- (e) [Application of definition.] First note that the zero vector $00 \dots 0$ is in the code. Suppose $x, y \in \mathcal{C}_0^n$, and consider $z = x + y$ (coordinatewise addition modulo 3). Then

$$z_1 + \dots + z_n = (x_1 + y_1) + \dots + (x_n + y_n) = (x_1 + \dots + x_n) + (y_1 + \dots + y_n) = 0 \pmod{3}.$$

So \mathcal{C}_0^n is closed under vector addition. Closure under scalar multiplication is automatic.

Consider $x = 00 \dots 01 \in \mathcal{C}_1^n$. Observe that $x + x = 00 \dots 02 \notin \mathcal{C}_1^n$. So \mathcal{C}_1^n is not closed under vector addition.

- (f) [Bookwork.] One of the operations used to define equivalence is

$$x_1 \dots x_n \mapsto x_1 \dots x_{i-1} \sigma(x_i) x_{i+1} \dots x_n,$$

for some permutation σ of \mathbb{F}_q . To ensure preservation of linearity, insist that σ is of the form $\sigma(\xi) = a\xi$, for some non-zero $a \in \mathbb{F}_q$.

- Question 2.** (a) [Bookwork] \mathcal{C} is t -error-correcting if there do not exist words $x \in A^n$ and $u, v \in \mathcal{C}$ such that $u \neq v$, $d(u, x) \leq t$ and $d(v, x) \leq t$. ($d(u, x)$ is Hamming distance between u and x .) \mathcal{C} has minimum distance d if the minimum of $d(u, v)$ over all $u, v \in \mathcal{C}, u \neq v$, is d . Suppose \mathcal{C} fails to be t -error-correcting. Then there exist x, u, v as above. By the triangle inequality, $d(u, v) \leq 2t$ and \mathcal{C} does not have minimum distance $2t + 1$.

- (b) [Bookwork, specialised to the binary alphabet.]

$$S(x, t) = \{y \in A^n \mid d(x, y) \leq t\}.$$

Suppose y is a word with $d(x, y) = s$. Then y differs from x in exactly s positions. There are $\binom{n}{s}$ choices for these positions. Since we are working with the binary alphabet, y is completely determined by this choice of s positions. The total number of words in $S(x, t)$ is now obtained by summing over $0 \leq s \leq t$.

- (c) [Ditto] If \mathcal{C} is t -error-correcting, then the spheres $S(v, t)$ for $v \in \mathcal{C}$ must be disjoint. (The existence of $u, v \in \mathcal{C}$ and $x \in S(u, t) \cap S(v, t)$ would contradict the assumption that \mathcal{C} is t -error-correcting.)

The size of the union of disjoint sets is the sum of their sizes, and so we get

$$\left| \bigcup_{v \in \mathcal{C}} S(v, t) \right| = \sum_{v \in \mathcal{C}} |S(v, t)| = |\mathcal{C}| \left(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t} \right).$$

But $\bigcup_{v \in \mathcal{C}} S(v, t)$ is a subset of $\{0, 1\}^n$, which contains exactly 2^n words. And so

$$|\mathcal{C}| \left(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t} \right) \leq 2^n,$$

which gives the result.

- (d) [Judicious choice of example code from the course.] Substituting $n = 7, t = 1$, we obtain an upper bound of $M \leq 2^7/(1 + 7) = 16$ on the maximum number M of words in a 1-error-correcting code of length 7. This bound is achieved by the Hamming code $\text{Ham}(3, 2)$, which is a binary $[2^r - 1, 2^r - r - 1]$ -code with $r = 3$. Thus $\text{Ham}(3, 2)$ has $2^{2^3-3-1} = 16$ codewords of length $2^3 - 1 = 7$.
- (e) [Judicious choice of upper bound from the course.] Substituting $n = 7, t = 2$, we obtain an upper bound of $M \leq \lfloor 2^7/(1 + 7 + 21) \rfloor = 4$ on the maximum number M of words in a 2-error-correcting code of length 7. But the Plotkin bound is stronger in this case: $M \leq 2 \lfloor (d+1)/(2d-n+1) \rfloor = 2 \lfloor 6/(10-7+1) \rfloor = 2$, where $d = 2t + 1 = 5$ is minimum distance (see part (a)).

- Question 3.** (a) [Bookwork. This part and the next lead the student through a lemma from the notes, specialised to binary codes.] Take two distinct codewords $x_1 \dots x_{n-1}, y_1 \dots y_{n-1} \in \mathcal{C}_0$. By construction, $x_1 \dots x_{n-1} 0$ and $y_1 \dots y_{n-1} 0$ are codewords of \mathcal{C} , and so

$$d(x_1 \dots x_{n-1} 0, y_1 \dots y_{n-1} 0) \geq d.$$

Hence $|\{i : 1 \leq i \leq n-1 \text{ and } x_i \neq y_i\}| \geq d$, and

$$d(x_1 \dots x_{n-1}, y_1 \dots y_{n-1}) \geq d.$$

But these codewords were chosen arbitrarily.

- (b) Every codeword ends either with 0 or 1, so $M_0 + M_1 = M$. Thus $\max\{M_0, M_1\} \geq M/2$. If $M_0 \geq M_1$ choose $\mathcal{C}' = \mathcal{C}_0$ else $\mathcal{C}' = \mathcal{C}_1$. Either way, the number of codewords in \mathcal{C}' exceeds $M/2$.
- (c) [Bookwork.] For a codeword $x = x_1 \dots x_{n-1} \in \mathcal{C}'$, denote by \bar{x} the word $\bar{x} = x_1 \dots x_{n-1}a \in \{0, 1\}^n$, where $a \in \{0, 1\}$ is chosen so that the weight of \bar{x} is even. Then $\mathcal{C}'' = \{\bar{x} : x \in \mathcal{C}'\}$.
- (d) [Application of the above to a concrete example.] First select the codewords ending with 0, and strip off the 0:

$$\mathcal{C}' = \left\{ \begin{array}{l} 000000000, \\ 101000111, \\ 110110100, \\ 111011010, \\ 011101101, \\ 000111011 \end{array} \right\}.$$

Then pad out by one symbol to achieve even weight:

$$\mathcal{C}'' = \left\{ \begin{array}{l} 0000000000, \\ 1010001111, \\ 1101101001, \\ 1110110100, \\ 0111011010, \\ 0001110111 \end{array} \right\}.$$

By the previous parts, \mathcal{C}'' is a $(10, 6, 6)$ -code.

- (e) [Easy unseen part.] The number of codewords in \mathcal{C}'' is not a power of 2, so it cannot be linear.

Question 4. (a) [Basic definition.] An $[n, k]$ -code over \mathbb{F}_q is a vector subspace of \mathbb{F}_q^n of dimension k .

- (b) [Bookwork.] The weight $w(v)$ is the number of non-zero components in v .

Suppose that $0 \neq v \in \mathcal{C}$ is a non-zero codeword of minimum weight $w = w(v)$. Then $0^n \in \mathcal{C}$ and $d(0^n, v) = w(v)$. Thus the minimum distance $d(\mathcal{C})$ satisfies $d(\mathcal{C}) \leq w$. Conversely, suppose that $u, v \in \mathcal{C}$ are codewords satisfying $d(u, v) = d(\mathcal{C})$. Then, since \mathcal{C} is linear, $u - v \in \mathcal{C}$; moreover, $w(u - v) = d(\mathcal{C})$. Hence $w \leq d(\mathcal{C})$.

- (c) [Bookwork.] G is a generator matrix for \mathcal{C} if the rows of G form a basis for \mathcal{C} . Thus G has k rows and n columns. G is in standard form if $G = [I_k \mid A]$, where I_k is the $k \times k$ identity matrix, and A an unrestricted $k \times (n - k)$ matrix.
- (d) [Routine application of bookwork.] The matrix we start with is:

$$G = \begin{pmatrix} 1100 \\ 0011 \\ 1001 \end{pmatrix}.$$

The quickest way to standard form is to cyclicly permute the columns one place to the left to obtain

$$G' = \begin{pmatrix} 1001 \\ 0110 \\ 0011 \end{pmatrix}.$$

Then add row 3 to row 2:

$$G' = \begin{pmatrix} 1001 \\ 0101 \\ 0011 \end{pmatrix}.$$

- (e) [Unseen, but similar to a examples from the lectures or exercises.] We know that any $[6, 2]$ -code \mathcal{C} is equivalent to one in standard form:

$$G = \begin{pmatrix} 10x_1x_2x_3x_4 \\ 01y_1y_2y_3y_4 \end{pmatrix},$$

with $x_i, y_i \in \mathbb{F}_2$. Since \mathcal{C} has minimum distance 4, at most one x_i is zero, and at most one y_i is zero. Thus at least two of the undetermined columns must consist of two ones. Permuting these into positions 3 and 4 we obtain:

$$G' = \begin{pmatrix} 1011x'_3x'_4 \\ 0111y'_3y'_4 \end{pmatrix},$$

Since the sum of the two rows is a codeword, which must have weight at least 4, the only possibilities for the remaining two values are $x'_3 = y'_4 = 1$ and $x'_4 = y'_3 = 0$, or vice versa. By transposing the final two columns if necessary we obtain

$$G'' = \begin{pmatrix} 101110 \\ 011101 \end{pmatrix}.$$

Note that G'' is the generator matrix of a $[6, 2]$ -code of minimum distance 4. The matrix G was an arbitrary standard form generator matrix for a $[6, 2]$ -code. So there is a unique $[6, 2]$ -code of minimum distance 4 up to equivalence.

- Question 5.** (a) [Bookwork. As in the course notes, codewords are row vectors.] $\mathcal{C}^\perp = \{w : Gw^T = 0\}$. Define $\alpha : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^k$ by $\alpha(w) = Gw^T$. Then $\mathcal{C}^\perp = \ker \alpha$. By the Rank-nullity Theorem, $\dim \ker \alpha = n - \dim \text{Im } \alpha = n - k$, since G is of rank k .
- (b) [Bookwork.] The conditions are: $GH^T = 0$ and H has full rank $(n - k)$. H is a generator matrix for \mathcal{C}^\perp .
- (c) [Bookwork.] G is in standard form if $G = [I_k \mid A]$, where I_k is the $k \times k$ identity matrix, and A an unrestricted $k \times (n - k)$ matrix. If G has this form then the parity-check matrix is $H = [-A^T \mid I_{n-k}]$.
- (d) [Routine application.]

$$H = \begin{pmatrix} 1210 \\ 1101 \end{pmatrix}.$$

- (e) [Application of bookwork; similar to examples from class/notes/exercises.] Syndrome de-

coding table:

00	→	0000
01	→	0001
02	→	0002
10	→	0010
11	→	1000
12	→	0200
20	→	0020
21	→	0100
22	→	2000

Given a received word w , compute the syndrome Hw^T . Look up the syndrome in the table to find a coset leader u . The decoded codeword is then $w - u$.

If $w = 2211$ is received then the syndrome is 12 and the coset leader $u = 0200$. Then the decoded codeword is $2211 - 0200 = 2011$.

- Question 6.**
- (a) [Basic definition.] $A_q(n, d)$ is the maximum number of codewords in any code of length n and minimum distance d over \mathbb{F}_q .
 - (b) [Bookwork] $A_q(n, d) \leq A_q(n-1, d-1)$. By induction, $A_q(n, d) \leq A_q(n-d+1, 1)$. No code can contain more than q^n codewords, so $A_q(n-d+1, 1) \leq q^{n-d+1}$. Putting the two inequalities together, $A_q(n, d) \leq q^{n-d+1}$.
 - (c) [Definition.] The redundancy is $r = n - k$. An MDS code of redundancy r is one with minimum distance $r + 1$.
 - (d) [Bookwork, specialised to particular n, q, r .]

$$H = \begin{pmatrix} 11111110 \\ 01234560 \\ 01422411 \end{pmatrix}.$$

The first 7 columns are of the form $(1, a, a^2)'$ where a ranges over $\mathbb{F}_q = \mathbb{F}_7$. The final column is $(0, 0, 1)'$: more generally, the coordinate vector with a 1 in the final coordinate. The key property of H is every 3×3 submatrix has full rank. This ensures that no non-zero codeword can have weight less than or equal to 3.

- (e) [Easy use of parts (b) and (d).] The code defined by H has redundancy $r = 3$ and hence dimension $k = n - r = 8 - 3 = 5$. Thus the code has $q^k = 7^5$ codewords and $A_7(8, 4) \geq 7^5$. On the other hand, by part (b), $A_7(8, 4) \leq q^{n-d+1} = 7^{8-4+1} = 7^5$.
- (f) [Unseen, but straightforward. Requires understanding of the relationships between the various concepts.] By inspection, making use of the 0 entries in H , 51000015 is a codeword. (If the student doesn't take advantage of the structure of H , there is still time to solve a system of three equations in three unknowns. Or to put H into standard form and write down the generator matrix.) This codeword corresponds to the linear relation

$$5 \times \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 1 \times \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + 1 \times \begin{pmatrix} 1 \\ 6 \\ 1 \end{pmatrix} + 5 \times \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$