Queen Mary, University of London

B. Sc. Examination by course unit 2006

MAS309 Coding Theory – model solutions

Tuesday 23rd May

2.30 p.m.

Duration: 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.

Question 1. Suppose $\mathcal{C}$ is a code of length n over the q-ary alphabet A.

(a) [Bookwork] What does it mean to say that $\mathcal{C}$ is t-error-detecting? What does it mean to say that $\mathcal{C}$ is t-error-correcting? Prove that if $\mathcal{C}$ is $2t$-error-detecting, then $\mathcal{C}$ is t-error-correcting. (You may assume the triangle inequality.) [4]

Solution: $\mathcal{C}$ is t-error-detecting if there do not exist words $w, x \in \mathcal{C}$ with $d(w,x) \leqslant t$. $\mathcal{C}$ is t-error-correcting if there do not exist words $v \in A^n$ and $w, x \in \mathcal{C}$ such that $w \neq x$ and

$$d(v,x) \leqslant t, \qquad d(w,x) \leqslant t.$$

Suppose $\mathcal{C}$ fails to be t-error-correcting. Then there are v, w, x as above. By the triangle inequality, we have

$$d(w,x) \leqslant d(v,x) + d(w,x) \leqslant t + t = 2t,$$

and so $\mathcal{C}$ is not $2t$-error-detecting. Hence if $\mathcal{C}$ is $2t$-error-detecting, then it is t-error-correcting.

(b) [Bookwork] If x is a codeword in $\mathcal{C}$, define the sphere $S(x,t)$, and prove that the number of words in $S(x,t)$ is

$$\binom{n}{0} + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}.$$ [7]

Solution:

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

We claim that the number of words w such that $d(w,x) = i$ is $(q-1)^i\binom{n}{i}$. The result will then follow by summing over $i = 0, 1, \ldots t$.

If w is a word such that $d(w,x) = i$, then there are exactly i positions where w and x differ. There are n positions altogether, so the i positions may be chosen in $\binom{n}{i}$ different ways. For each of these positions, we must then choose the symbol which appears in w. We may choose any of the q symbols in A except the symbol appearing in x in this position, which gives us $q-1$ choices. We make this choice independently for each position, giving us q^i choices altogether for these i symbols. Hence we have $(q-1)^i\binom{n}{i}$ ways to choose w altogether.

(c) [Bookwork] Deduce that if $\mathcal{C}$ is t-error-correcting, then

$$|\mathcal{C}| \leqslant \frac{q^n}{\binom{n}{0} + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}}.$$ [6]

Solution: If $\mathcal{C}$ is t-error-correcting, then the spheres $S(x,t)$ for $x \in \mathcal{C}$ must be disjoint. For if $w, x \in \mathcal{C}$ and $v \in S(x,t) \cap S(w,t)$ then we have $d(v,w) \leqslant t$ and $d(v,x) \leqslant t$ which contradicts the fact 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

$$\begin{aligned}\left|\bigcup_{x\in\mathcal{C}} S(x,t)\right| &= \sum_{x\in\mathcal{C}} |S(x,t)| \\ &= \sum_{x\in\mathcal{C}} \left(\binom{n}{0} + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}\right) \\ &= |\mathcal{C}| \left(\binom{n}{0} + (q-1)\binom{n}{1} + \cdots + (q-1)^t\binom{n}{t}\right).\end{aligned}$$

But $\bigcup_{x\in\mathcal{C}} S(x,t)$ is a subset of A^n, which contains exactly q^n words. And so

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

which gives the result.

(d) [Bookwork] If $\mathcal{C}$ is a binary linear $[n,k]$-code, how many words are there in $\mathcal{C}$? Briefly justify your answer. [3]

Solution: There are 2^k words in $\mathcal{C}$. If $\{e_1,\dots,e_k\}$ is a basis for $\mathcal{C}$, then each word $v\in\mathcal{C}$ may be written uniquely in the form $\lambda_1 e_1+\cdots+\lambda_k e_k$ for $\lambda_1,\dots,\lambda_k\in\mathbb{F}_2=\{0,1\}$. So the number of words in $\mathcal{C}$ is the number of choices of the coefficients $\lambda_1,\dots,\lambda_k$. We have two different choices for each λ_i, and hence 2^k choices altogether.

(e) [Unseen] Suppose that $n^2+n+1\geqslant 2^l$ for some integer l, and that $\mathcal{C}$ is a binary linear $[n,k]$-code which is 2-error-correcting. Prove that $k<n-l+1$. [5]

Solution: By the above inequality, we have

$$\begin{aligned}|\mathcal{C}| &\leqslant \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}}\\ &= \frac{2^n}{1+n+\frac{n(n-1)}{2}}.\end{aligned}$$

Hence (applying the previous part) we have

$$2^k \leqslant \frac{2^n}{\frac{1}{2}(n^2+n+2)} < \frac{2^n}{\frac{1}{2}(2^l)} = 2^{n-l+1},$$

and so

$$k < n-l+1.$$

Question 2. In this question we work with the binary alphabet $A = \{0, 1\}$.

(a) [Bookwork] What is meant by a *binary* (n, M, d)*-code*? Define the constants $A_2(n, d)$. [2]

Solution: A binary (n, M, d)-code is a code over the alphabet $\{0, 1\}$ in which each codeword has length n, there are exactly M codewords and $d(v, w) \geqslant d$ for all distinct words $v, w \in \mathcal{C}$. $A_2(n, d)$ is the largest M for which a binary (n, M, d)-code exists.

[Marks: 1 for each part.]

Note: Some books require that an (n, M, d)-code have minimum distance exactly d. Candidates who use this definition will get the marks.

(b) [Similar to coursework] Suppose n, m and d are positive integers. Prove that

$$A_2(nm, dm) \geqslant A_2(n, d).$$ [6]

Solution: First we show that given a binary (n, M, d)-code, we can construct a binary (nm, M, dm)-code. Given a word $v \in \mathcal{C}$, let $v^{(m)}$ denote the word of length nm obtained by writing the word v m times. Define

$$\mathcal{C}^{(m)} = \{v^{(m)} \mid v \in \mathcal{C}\}.$$

By construction, each word in $\mathcal{C}$ has length nm. If v, w are distinct words in $\mathcal{C}$, then $v^{(m)}$ and $w^{(m)}$ are distinct, so the number of words in $\mathcal{C}^{(m)}$ equals the number of words in $\mathcal{C}$, i.e. M. It remains to show that the minimum distance of $\mathcal{C}^{(m)}$ is at least dm, i.e. that $d(x, y) \geqslant nm$ for all $x, y \in \mathcal{C}^{(m)}$ with $x \neq y$. We have $x = v^{(m)}$, $y = w^{(m)}$ for some $v, w \in \mathcal{C}$; since $\mathcal{C}$ has minimum distance at least d, v and w differ in at least d positions. This means that $v^{(m)}$ and $w^{(m)}$ differ in at least d of the first n positions, at least d of the next n positions, and so on, so that $d(v^{(m)}, w^{(m)}) \geqslant dm$.

If we choose an (n, M, d)-code $\mathcal{C}$ with $M = A_2(n, d)$, then we get an (nm, M, nd)-code. Therefore the largest possible (nm, N, nd)-code has $N \geqslant M$, i.e. $A_2(nm, dm) \geqslant A_2(n, d)$.

[Marks: 1 for knowing what construction they need to make, 2 for making it, 1 for each part of the proof, 1 for finishing off.]

(c) [Bookwork/Unseen] Suppose d is even. Explain how to construct a binary (n, M, d)-code from a binary $(n-1, M, d-1)$-code (you do not have to prove that your construction works). Illustrate by constructing a $(10, 6, 6)$-code from the code

$$\{000000111, 000111000, 111000000, 011011011, 101101101, 110110110\}.$$ [4]

Solution: Suppose $\mathcal{C}$ is a binary $(n-1, M, d-1)$-code. For each $v \in \mathcal{C}$, define the word $\overline{v}$ of length n by adding a symbol 0 or 1 to the end of v in such a way as to make the number of 1s even. Then the code $\{\overline{v} \mid v \in \mathcal{C}\}$ is an (n, M, d)-code.

The example:

$$\{0000001111, 0001110001, 1110000001, 0110110110, 1011011010, 1101101100\}.$$

[Marks: 2 for the construction, 2 for the example.]

(d) [Bookwork] State the Plotkin bound. (You should state both cases: d even and d odd.) [4]

Solution:

- If d is even and $n < 2d$, then

$$A_2(n,d) \leqslant 2\left\lfloor \frac{d}{2d-n} \right\rfloor.$$

- If d is odd and $n < 2d+1$, then

$$A_2(n,d) \leqslant 2\left\lfloor \frac{d+1}{2d+1-n} \right\rfloor.$$

(e) [Unseen] Write down a binary $(5,4,3)$-code, and prove that for all positive integers m,

$$A_2(5m,3m) = \begin{cases} 6 & \text{(if } m \text{ is even)} \\ 4 & \text{(if } m \text{ is odd)} \end{cases}.$$ [9]

Solution:

$$\{00000, 01101, 10110, 11011\}.$$

If m is even, then $3m$ is even and $5m < 2 \times 3m$, and so by Plotkin we have

$$A_2(5m,3m) \leqslant 2\left\lfloor \frac{3m}{6m-5m} \right\rfloor = 6.$$

Since a $(10,6,6)$-code exists, we have $A_2(10,6) \geqslant 6$. Hence by part (2b) we have $A_2(10m,6m) \geqslant 6$ for all m. So $A_2(5m,3m) = 6$ when m is even.

If m is odd, then $3m$ is odd and $5m < 2 \times 3m + 1$, and so by Plotkin we have

$$A_2(5m,3m) \leqslant 2\left\lfloor \frac{3m}{6m+1-5m} \right\rfloor \leqslant 4.$$

Since a $(5,4,3)$-code exists, we have $A_2(5,3) \geqslant 4$. By part (2b) we get $A_2(5m,3m) \geqslant 4$ for all m, and we deduce that $A_2(5m,3m) = 4$ when m is odd.

[Marks: 1 for the example code, 4 for the upper bounds, 4 for the lower bounds.]

Note: They've seen this $(5,4,3)$-code many times in lectures, so this part should present no trouble at all.

Question 3. (a) [Bookwork] Suppose $\mathcal{C}$ is a code of length n over the alphabet A. Explain what is meant by a *decoding process* for $\mathcal{C}$. Explain what is meant by a *nearest-neighbour decoding process* for $\mathcal{C}$. [3]

Solution: A decoding process is a function from A^n to $\mathcal{C}$. A nearest-neighbour decoding process is a function f from A^n to $\mathcal{C}$ such that

$$d(w, f(w)) \leqslant d(w, v)$$

for all $w \in A^n$ and $v \in \mathcal{C}$.

(b) [Unseen] Let $\mathcal{C}$ be the binary code

$$\{000, 011, 110\}.$$

Construct a nearest-neighbour decoding process for $\mathcal{C}$. [3]

Solution:

$$\begin{aligned} 000 &\mapsto 000 \\ 001 &\mapsto 000 \\ 010 &\mapsto 000 \\ 011 &\mapsto 011 \\ 100 &\mapsto 000 \\ 101 &\mapsto 011 \\ 110 &\mapsto 110 \\ 111 &\mapsto 011. \end{aligned}$$

(c) [Bookwork/Unseen] Now suppose $\mathcal{C}$ is a linear $[n, k]$-code over $\mathbb{F}_q$. Explain what is meant by a *coset* of $\mathcal{C}$. Explain what is meant by the *weight* of a word. Explain what is meant by a *coset leader*. Explain how to construct a Slepian array for $\mathcal{C}$, and how to use a Slepian array to construct a nearest-neighbour decoding process. Illustrate by constructing a Slepian array for the binary linear code

$$\mathcal{C} = \{0000, 0011, 0110, 0101\}.$$ [9]

Solution: A coset of $\mathcal{C}$ is a set of the form

$$w + \mathcal{C} = \{w + v \mid v \in \mathcal{C}\}$$

for $w \in \mathbb{F}_q^n$. The weight of a word is the number of non-zero symbols. A coset leader is a word which has the smallest weight of any word in the same coset. A Slepian array is a $q^{n-k} \times q^k$ array of words such that:

- the words in the first row are the distinct codewords in $\mathcal{C}$;
- the words in the first column are coset leaders, with one chosen from each coset;
- the word in the ith row and jth column equals the coset leader at the left of the ith row plus the codeword at the top of the jth column.

Given a Slepian array, we construct a decoding process f as follows: given a word $w \in \mathbb{F}_q^n$, find w in the array (it will appear exactly once). Define $f(w)$ to be the codeword at the top of the column containing w.

0000	0011	0110	0101
0001	0010	0111	0100
1000	1011	1110	1101
1001	1010	1111	1100

[Marks: 1 for a coset. 1 for weight. 1 for a coset leader. 2 for a Slepian array, 2 for the decoding process, 2 for the example.]

(d) [Bookwork] What is a *generator matrix* for a linear $[n, k]$-code $\mathcal{C}$? What is a *parity-check matrix*? [3]

Solution: A generator matrix for $\mathcal{C}$ is a $k \times n$ matrix G whose rows form a basis for $\mathcal{C}$. A parity-check matrix is an $(n-k) \times n$ matrix H whose rows whose rows are linearly independent and such that $HG^{\mathrm{T}} = 0$ for a generator matrix G.

[Marks: 1 for generator, 2 for parity-check.]

Note: They can define a parity-check matrix in terms of the dual code, but they must define this.

(e) [Bookwork] If $\mathcal{C}$ is a linear code and H is a parity-check matrix for $\mathcal{C}$, what is the *syndrome* of a word w? [1]

Solution: The syndrome of w is the word wH^{T}.

(f) [Unseen] Let $\mathcal{C}$ be the ternary code with generator matrix

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

Construct a parity-check matrix and a syndrome look-up table for $\mathcal{C}$. Use your syndrome look-up table to decode the word 1111. [6]

Solution: A parity-check matrix is

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

A syndrome look-up table is

leader	syndrome
0000	00
0001	01
0002	02
0010	10
0020	20
1000	21
2000	12
0011	11
0022	22

The syndrome of 1111 is 22. The corresponding leader is 0022, so we decode 1111 as $1111 - 0022 = 1122$.

[Marks: 2 for the parity-check matrix, 3 for the table, 1 for the decoding.]

Question 4. (a) [Bookwork/Similar to coursework] Define the Hamming distance $d(v, w)$. Do there exist three words v, w, x of length 8 over the alphabet $\{0, 1\}$ such that

$$d(v, w) = d(v, x) = d(w, x) = 5?$$

Justify your answer. [4]

Solution: No. Let V be the number of i such that $v_i \neq w_i = x_i$. Let W be the number of i such that $w_i \neq v_i = x_i$. Let X be the number of i such that $v_i = w_i \neq x_i$. Since A contains only two symbols, we can't have $v_i \neq w_i \neq x_i \neq v_i$. So we have

$$\begin{aligned} 5 = d(v, w) &= V + W, \\ 5 = d(v, x) &= V + X, \\ 5 = d(w, x) &= W + X. \end{aligned}$$

Summing, we obtain

$$15 = 2(V + W + X),$$

which is absurd.

[Marks: 1 for definition, 3 for proof.]

(b) [Bookwork] Explain what it means for two codes of length n over an alphabet A to be equivalent. [3]

Solution: Define two operations on codes.

Operation 1: choose a permutation σ of $\{1, \dots, n\}$. For a word $v \in \mathcal{C}$, define

$$v_\sigma = v_{\sigma(1)} \dots v_{\sigma(n)}.$$

Now replace $\mathcal{C}$ with the code

$$\mathcal{C}_\sigma = \{v_\sigma \mid v \in \mathcal{C}\}.$$

Operation 2: choose $i \in \{1, \dots, n\}$ and a permutation f of A. For a word $v \in \mathcal{C}$, define

$$v_{f,i} = v_1 \dots v_{i-1}(f(v_i))v_{i+1} \dots v_n.$$

Now replace $\mathcal{C}$ with the code

$$\mathcal{C}_{f,i} = \{v_{f,i} \mid v \in \mathcal{C}\}.$$

Say that two codes are equivalent if we can get from one to the other by repeatedly applying Operations 1 and 2.

(c) [Bookwork] Prove that if $\mathcal{C}$ is equivalent to $\mathcal{D}$, then $|\mathcal{C}| = |\mathcal{D}|$. [6]

Solution: For Operation 1: suppose we have a permutation σ of $\{1, \dots, n\}$. We claim that the map

$$\phi : v \longmapsto v_\sigma$$

is a bijection from $\mathcal{C}$ to $\mathcal{C}_\sigma$, which will imply that $|\mathcal{C}| = |\mathcal{C}_\sigma|$. Certainly ϕ is surjective, since by definition $\mathcal{C}_\sigma$ is the image of ϕ. For injectivity, suppose that v and w are distinct words in $\mathcal{C}$. Then $v_j \neq w_j$ for some j. σ is a permutation, so $j = \sigma(i)$ for some $i \in \{1, \dots, n\}$. Hence

$v_{\sigma(i)} \neq w_{\sigma(i)}$, so v_σ and w_σ differ in position i, so are distinct. So ϕ is injective, and hence a bijection.

For Operation 2: suppose we have a permutation f of A and we have $i \in \{1, \dots, n\}$. We claim that the map

$$\phi : v \longmapsto v_{f,i}$$

is a bijection from $\mathcal{C}$ to $\mathcal{C}_{f,i}$, which will imply that $|\mathcal{C}| = |\mathcal{C}_{f,i}|$. Certainly ϕ is surjective, since by definition $\mathcal{C}_{f,i}$ is the image of ϕ. For injectivity, suppose that v and w are distinct words in $\mathcal{C}$. Then $v_j \neq w_j$ for some j. If $j \neq i$, then this means that $(v_{f,i})_j \neq (w_{f,i})_j$. If $j = i$, then since f is injective we have $f(v_i) \neq f(w_i)$. So $(v_{f,i})_i \neq (w_{f,i})_i$. In either case, $v_{f,i} \neq w_{f,i}$, so ϕ is injective.

So Operations 1 and 2 both preserve the number of words in a code, and so if two codes are equivalent, they have the same number of words.

Let $A = \{0, 1, 2\}$, and let $\mathcal{C} = \{0120, 1201, 1010\}$.

(d) [Similar to coursework] Find a code equivalent to $\mathcal{C}$ containing the word 1111 (and prove that it's equivalent to $\mathcal{C}$). [4]

Solution: Apply Operation 2, with $i = 2$ and

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

to get to the code

$$\{0220, 1101, 1010\}.$$

Now apply Operation 2 with $i = 3$ and

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

to get the code

$$\{0220, 1111, 1000\}.$$

(e) [Similar to coursework] Is $\mathcal{C}$ equivalent to the code $\mathcal{D} = \{0000, 0111, 2201\}$? Briefly justify your answer. [2]

Solution: No. $\mathcal{C}$ contains two words 0120 and 1201 with $d(0120, 1201) = 4$. $\mathcal{D}$ does not contain two words at distance 4. The equivalence operations preserve the distance between any pair of words, so $\mathcal{C}$ can't be equivalent to $\mathcal{D}$.

(f) [Bookwork] Explain what it means for two linear codes of length n over $\mathbb{F}_q$ to be equivalent. [2]

Solution: We define two operations on codes.

Operation 1: as above.

Operation 2′: Choose $i \in \{1, \dots, n\}$ and $a \in \mathbb{F}_q \setminus \{0\}$. For a word $v \in \mathcal{C}$, define

$$v_{a,i} = v_1 \dots v_{i-1}(av_i)v_{i+1} \dots v_n.$$

Now replace $\mathcal{C}$ with the code

$$\mathcal{C}_{a,i} = \{v_{a,i} \mid v \in \mathcal{C}\}.$$

We say that two linear codes are equivalent if we can get from one to the other by repeatedly applying Operations 1 and 2′.

Let $\mathcal{C}$ be the linear code $\{0000, 1210, 2120\}$ over $\mathbb{F}_3$.

(g) [Unseen] Find a linear code equivalent to $\mathcal{C}$ containing the word 0111 (and prove that it's equivalent to $\mathcal{C}$). [4]

Solution: Apply Operation 2′, with $i = 2$ and $a = 2$, to get the code

$$\{0000, 1110, 2220\}.$$

Now apply Operation 1, with

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

to get the code

$$\{0000, 0111, 0222\}.$$

Question 5. (a) [Bookwork] Suppose $\mathcal{C}$ is an (n, M, d)-code over the q-ary alphabet A and that $d > 1$. Show how to construct an $(n-1, M, d-1)$-code over A, and prove that it really is an $(n-1, M, d-1)$-code. [8]

Solution: For $v \in \mathcal{C}$, define the word $\overline{v}$ by deleting the last symbol in v. Then $\overline{\mathcal{C}} = \{\overline{v} \mid v \in \mathcal{C}\}$ is an $(n-1, M, d-1)$-code. Clearly each $\overline{v}$ has length $n-1$. If $v, w \in \mathcal{C}$ with $v \neq w$, then $d(v, w) \geqslant d$. Hence there are at least d positions where v and w differ. At most one of these can be the last position, so there are at least $d-1$ positions where $\overline{v}$ and $\overline{w}$ differ. So $d(\overline{v}, \overline{w}) \geqslant d-1$, so the minimum distance of $\overline{\mathcal{C}}$ is at least $d-1$. Also, if $v, w \in \mathcal{C}$ with $v \neq w$, then (since $d > 1$) we have $d(\overline{v}, \overline{w}) > 0$, so that $\overline{v} \neq \overline{w}$. So the number of words in $\overline{\mathcal{C}}$ is the number of words in $\mathcal{C}$, i.e. M.

[Marks: 3 for construction, 5 for proof.]

(b) [Bookwork] Deduce that if $d > 1$, then $A_q(n, d) \leqslant A_q(n-1, d-1)$. [1]

Solution: Let $\mathcal{C}$ be an (n, M, d)-code with $M = A_q(n, d)$. Then we can construct an $(n-1, M, d-1)$-code, which means that the largest possible $(n-1, N, d-1)$ code has $N \geqslant M$, i.e. $A_q(n-1, d-1) \geqslant A_q(n, d)$.

(c) [Bookwork] Prove that $A_q(n, d) \leqslant q^{n-d+1}$ for $d \geqslant 1$. [3]

Solution: We use induction on d. For $d = 1$, we want $A_q(n, 1) \leqslant q^n$. But a code of length n is a subset of A^n, which contains only q^n words, so any code of length n contains at most q^n words. Suppose now that $d = \delta > 1$ and that the result is true for $d = \delta - 1$ (and all n). By the previous part, we have

$$A_q(n, d) \leqslant A_q(n-1, d-1)$$

and by induction, this is at most $q^{(n-1)-(d-1)+1} = q^{n-d+1}$.

(d) [Bookwork] What is meant by the *redundancy* of a linear $[n, k]$-code? What is meant by a *maximum distance separable (MDS)* code of length n and redundancy r? [2]

Solution: The redundancy of a linear $[n, k]$-code is the integer $r = n - k$. An MDS code of length n and redundancy r is a linear $[n, n-r, r+1]$-code.

(e) [Bookwork/Unseen] Write down a parity-check matrix for a linear $[6, 3, 4]$-code over $\mathbb{F}_5$. [5]

Solution: We begin by writing 5 columns of the form

$$\begin{matrix} 1 \\ x \\ x^2 \end{matrix},$$

one for each $x \in \mathbb{F}_5$. Then we write a column

$$\begin{matrix} 0 \\ 0 \\ 1 \end{matrix}.$$

We get

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{pmatrix}.$$

(f) [Unseen] Using matrix operations, put your parity-check matrix in standard form. [4]

Solution: Swap columns 1 and 4:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 3 & 1 & 2 & 0 & 4 & 0 \\ 4 & 1 & 4 & 0 & 1 & 1 \end{pmatrix}.$$

Multiply column 5 by 4:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 4 & 0 \\ 3 & 1 & 2 & 0 & 1 & 0 \\ 4 & 1 & 4 & 0 & 4 & 1 \end{pmatrix}.$$

Add row 2 to row 1:

$$\begin{pmatrix} 4 & 2 & 3 & 1 & 0 & 0 \\ 3 & 1 & 2 & 0 & 1 & 0 \\ 4 & 1 & 4 & 0 & 4 & 1 \end{pmatrix}.$$

Add row 2 to row 3:

$$\begin{pmatrix} 4 & 2 & 3 & 1 & 0 & 0 \\ 3 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Note: I've defined standard form for a parity-check matrix to be with the identity matrix at the right, but if they put the identity matrix at the left, that's OK.

(g) [Bookwork/Unseen] Hence write down a generator matrix for a linear $[6, 3, 4]$-code over $\mathbb{F}_5$. [2]

Solution:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 4 & 3 \\ 0 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

(For parts (e–g) you do not have to explain your method, but doing so may help you to gain marks if you make arithmetical errors.)

Question 6. For this question, you may assume any basic linear algebra you need, including the Rank–Nullity Theorem.

(a) [Bookwork] Suppose $\mathcal{C}$ is a linear $[n, k]$-code over $\mathbb{F}_q$. Define the dot product $v.w$, and the dual code $\mathcal{C}^\perp$. [2]

Solution: If $v = v_1 \dots v_n$ and $w = w_1 \dots w_n$, then

$$v.w = v_1w_1 + v_2w_2 + \cdots + v_nw_n.$$

The dual code is

$$\mathcal{C}^\perp = \{w \in \mathbb{F}_q^n \mid v.w = 0 \text{ for all } v \in \mathcal{C}\}.$$

(b) [Bookwork] If G is a generator matrix for $\mathcal{C}$, prove that $w \in \mathcal{C}^\perp$ if and only if $Gw^{\mathrm{T}} = 0$. (You may assume that the dot product is symmetric and bilinear.) [5]

Solution: Let $e_1, \dots, e_k$ denote the rows of G. Then $e_1, \dots, e_k$ form a basis for $\mathcal{C}$. The ith symbol of wG^{T} is $w.e_i$, and so we have $wG^{\mathrm{T}} = 0$ if and only if $w.e_i = 0$ for all i. If $w \in \mathcal{C}^\perp$, then $w.v = 0$ for all $v \in \mathcal{C}$, and in particular $w.e_i = 0$ for each i, so $wG^{\mathrm{T}} = 0$. Conversely, suppose $w.e_i = 0$ for all i. A codeword v can be written as $\lambda_1 e_1 + \cdots + \lambda_k e_k$ for some $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$, and we have

$$w.v = w.(\lambda_1 e_1 + \cdots + \lambda_k e_k) = \lambda_1(w.e_1) + \cdots + \lambda_k(w.e_k) = 0,$$

so $w \in \mathcal{C}^\perp$.

(c) [Bookwork] Prove that $\mathcal{C}^\perp$ is a linear code of length n over $\mathbb{F}_q$. What is the dimension of $\mathcal{C}^\perp$? Justify your answer. [5]

Solution: Fact (The Rank–Nullity Theorem): If G is a $k \times n$ matrix over $\mathbb{F}_q$, then the kernel of G is a vector subspace of $\mathbb{F}_q^n$, of dimension n minus the rank of G.

The previos part of the question shows that $\mathcal{C}^\perp$ is the kernel of G, which is a subspace of $\mathbb{F}_q^n$, i.e. a linear code. Since the rows of G are linearly independent, the rank of G is the number of rows, i.e. k, and so the dimension of $\mathcal{C}^\perp$ is $n - k$.

Now suppose $\mathcal{C}$ is a linear $[4, 2]$-code over $\mathbb{F}_2$ such that $\mathcal{C}^\perp = \mathcal{C}$.

(d) [Bookwork] How many words does $\mathcal{C}$ contain? (You do not need to justify your answer.) [1]

Solution: 4.

(e) [Similar to coursework] Prove that $\mathcal{C}$ contains at least two words of weight 2. [3]

Solution: The If $v = v_1v_2v_3v_4$ is a word in $\mathcal{C}$, then (since $v \in \mathcal{C}^\perp$) we have

$$0 = v.v = v_1^2 + v_2^2 + v_3^2 + v_4^2,$$

and this equals $v_1 + v_2 + v_3 + v_4$, since $0^2 = 0$ and $1^1 = 1$. Hence every word in $\mathcal{C}$ has even weight, i.e. weight 0, 2 or 4. There is only one word of length 4 and weight 0, and only one of length 4 and weight 4, so there must be at least two words in $\mathcal{C}$ of weight 2.

(f) [Similar to coursework] Write down all binary words of length 4 and weight 2. [2]

Solution:

$$0011, 0101, 0110, 1001, 1010, 1100.$$

(g) [Similar to coursework] Deduce that $\mathcal{C}$ is one of the codes

$$\{0000, 0011, 1100, 1111\},$$

$$\{0000, 0101, 1010, 1111\},$$

$$\{0000, 0110, 1001, 1111\}.$$ [3]

Solution: Let v, w be two different words in $\mathcal{C}$ of weight 2. Then (since $w \in \mathcal{C}^\perp$) we have $v.w = 0$. By checking the dot product of each pair of the six words above, we find that $\{v, w\}$ equals $\{0011, 1100\}$, $\{0101, 1010\}$ or $\{0110, 1001\}$. Hence $\mathcal{C}$ is one of the codes listed.

(h) [Unseen] Write down a generator matrix for a linear $[4, 2]$-code $\mathcal{D}$ over $\mathbb{F}_3$ such that $\mathcal{D}^\perp = \mathcal{D}$. [4]

Solution:

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

Note: Parts (e)–(h) are identical to a coursework question.

Question 7. (a) [Bookwork] Write down parity-check matrices in standard form for the Hamming codes $\mathrm{Ham}(3,2)$ and $\mathrm{Ham}(2,3)$. Hence write down generator matrices for $\mathrm{Ham}(3,2)$ and $\mathrm{Ham}(2,3)$. (You do not have to explain your method, but doing so may help you to gain marks if you make arithmetic errors.) [7]

Solution: For $\mathrm{Ham}(3,2)$: construct a $3 \times 2^3 - 1$ matrix whose columns are all the different non-zero vectors in $\mathbb{F}_2^3$:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

For $\mathrm{Ham}(2,3)$: for $v, w \in \mathbb{F}_3^2$, define $v \equiv w$ if $v = \lambda w$ for a non-zero $\lambda \in \mathbb{F}_3$. Now construct a $2 \times \frac{3^2-1}{3-1}$ matrix whose columns consist of one vector from each equivalence class:

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

If $(B|I)$ is a standard-form parity-check matrix, then $(I|-B^{\mathrm{T}})$ is a generator matrix. So we get generator matrices

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

and

$$\begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}$$

respectively.

[Marks: 4 for the parity-check matrices, 3 for the generator matrices.]

(b) [Bookwork] How many words are there in $\mathrm{Ham}(3,2)$? What is the minimum distance of $\mathrm{Ham}(3,2)$? How many words are there in $\mathrm{Ham}(2,3)$? What is the minimum distance of $\mathrm{Ham}(2,3)$? (You do not need to justify your answers.) [4]

Solution: $\mathrm{Ham}(3,2)$ contains 16 words, and has minimum distance 3. $\mathrm{Ham}(2,3)$ contains 9 words, and has minimum distance 3.

[Marks: 1 for each question.]

Given binary words v, w of length m, define the product $v * w$ by

$$v * w = (v_1 w_1)(v_2 w_2) \dots (v_m w_m).$$

(c) [Bookwork] Using the product $*$ described above, describe how the binary Reed–Muller code $\mathcal{R}(r,n)$ is constructed. Write down generator matrices for $\mathcal{R}(1,3)$ and $\mathcal{R}(2,3)$. [8]

Solution: Let $x_i(n)$ be the word of length 2^n consisting of alternate chunks of 0s and 1s, the chunks being of length 2^i, and the first chunk being a chunk of 0s. Let $1(n)$ denote the word of length 2^n consisting entirely of 1s. Now let $\mathcal{S}(r,n)$ denote the set of all products of at most r of the words $x_0(n), x_1(n), \dots, x_{n-1}(n)$, including the 'empty product' $1(n)$. Then $\mathcal{R}(r,n)$ is the binary linear code spanned by all the words in $\mathcal{S}(r,n)$.

For example, $\mathcal{R}(1,3)$ has generator matrix

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

and $\mathcal{R}(2,3)$ has generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

[Marks: 4 for construction, 4 for the matrices.]

(d) [Bookwork] What is the dimension of $\mathcal{R}(r,n)$? What is its minimum distance? (You do not need to justify your answers.) [2]

Solution: $\mathcal{R}(r,n)$ has dimension $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}$, and minimum distance 2^{n-r}.

(e) [Unseen] Let $\mathcal{C}$ be the code obtained from $\mathcal{R}(1,3)$ by deleting the last symbol from each codeword. Prove that $\mathcal{C}$ is a linear code, and write down a generator matrix for $\mathcal{C}$. [4]

Solution: Given $v \in \mathcal{R}(1,3)$, let $\overline{v}$ denote v with the last symbol removed. $\mathcal{R}(1,3)$ contains the word 00000000, so $\mathcal{C}$ contains the word 0000000. If $x, y \in \mathcal{C}$, then $x = \overline{v}$, $y = \overline{w}$ for some $v, w \in \mathcal{R}(1,3)$. $\mathcal{R}(1,3)$ contains the word $v+w$, and so $\mathcal{C}$ contains the word $\overline{v+w}$. And in fact

$$\overline{v+w} = (v+w)_1 \dots (v+w)_7 = (v_1+w_1)\dots(v_7+w_7) = \overline{v}+\overline{w}.$$

So $\mathcal{C}$ is colsed under addition. $\mathcal{C}$ is closed under scalar multiplication, since $0x = 0000000 \in \mathcal{C}$ for any $x \in \mathcal{C}$ and $1x = x$.

To find a generator matrix, we delete the last column from the generator matrix for $\mathcal{R}(1,3)$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

[Marks: 3 for the proof, 1 for the matrix.]