

B. Sc. Examination by course unit 2009

MAS309 Coding Theory

Duration: 2 hours

Date and time: 5 June 2009, 10:00 a.m.

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

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 answered will be counted.

Calculators are NOT permitted in this examination. The unauthorized use of a calculator constitutes an examination offence.

Complete all rough workings in the answer book and cross through any work which is not to be assessed.

Candidates should note that the Examination and Assessment Regulations state that possession of unauthorized materials by any candidate who is under examination conditions is an assessment offence. Please check your pockets now for any notes that you may have forgotten that are in your possession. If you have any, then please raise your hand and give them to an invigilator now.

Exam papers must not be removed from the examination room.

Examiner(s): Fayers

Question 1 Suppose \mathbb{A} is an alphabet.

(a) Define what is meant by:

- a *word* of length n over \mathbb{A} ;
- the *Hamming space* \mathbb{A}^n ;
- a *code* of length n over \mathbb{A} ;
- the *distance* between two words of length n over \mathbb{A} ;
- the *minimum distance* of a code.

[[7]]

Solution: [Bookwork] A word of length n is a string of n symbols from \mathbb{A} . The Hamming space \mathbb{A}^n is the set of all words of length n over \mathbb{A} . A code of length n is a subset of \mathbb{A}^n . The distance between two words $v = v_1 \dots v_n$ and $w = w_1 \dots w_n$ is

$$|\{i \mid v_i \neq w_i\}|.$$

The minimum distance of a code C is

$$\min\{d(v, w) \mid v, w \in C, v \neq w\}.$$

[Marking: start with 7, and lose up to two marks for inaccuracy in each definition, down to a minimum of 0.]

(b) Suppose C is a code of length n over \mathbb{A} , and $t > 0$. What does it mean to say that C is *t-error-correcting*?

[[3]]

Solution: [Bookwork] C is *t-error-correcting* if there do not exist $v, w \in C$ and $x \in \mathbb{A}^n$ with $v \neq w$, such that $d(v, x) \leq t$ and $d(w, x) \leq t$.

(c) Prove that if $d(C) > 2t$, then C is *t-error-correcting*. (You may assume the triangle inequality.)

[[4]]

Solution: [Bookwork] We prove the contrapositive: suppose C is not *t-error-correcting*, and take v, w, x as above. Then by the triangle inequality we have

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

with $v, w \in C$ and $v \neq w$, so that $d(C) \leq 2t$.

(d) Suppose x is a word of length n over \mathbb{A} , and $t > 0$. What is meant by the *sphere* $S(x, t)$?

[[2]]

Solution: [Bookwork] $S(x, t)$ is the set of all words $y \in \mathbb{A}^n$ such that $d(x, y) \leq t$.

- (e) If \mathbb{A} is a q -ary alphabet, how many words does $S(x, t)$ contain? (You do not need to justify your answer.) [[2]]

Solution: [Bookwork]

$$|S(x, t)| = \sum_{i=0}^t (q-1)^i \binom{n}{i}.$$

- (f) State the Hamming bound. [[2]]

Solution: [Bookwork] If $|\mathbb{A}| = q$ and C is a t -error-correcting code of length n over \mathbb{A} , then

$$|C| \leq \frac{q^n}{\sum_{i=0}^t (q-1)^i \binom{n}{i}}.$$

- (g) Suppose $\mathbb{A} = \{0, 1, 2\}$, and that C is a code of length 11 over \mathbb{A} which is 2-error-correcting. Prove that C contains at most 3^6 words. [[5]]

Solution: [Unseen] Applying the Hamming bound, we have

$$|C| \leq \frac{3^{11}}{\binom{11}{0} + 2\binom{11}{1} + 2^2\binom{11}{2}}.$$

The denominator equals

$$1 + 2 \times 11 + 4 \times 55 = 243 = 3^5,$$

and so

$$|C| \leq \frac{3^{11}}{3^5} = 3^6.$$

- Question 2** (a) Suppose C is a code of length n over an alphabet \mathbb{A} . Explain what is meant by a *nearest-neighbour decoding process* for C . [[4]]

Solution: [Bookwork] If $C \subseteq \mathbb{A}^n$, a nearest-neighbour decoding process is a function $f : \mathbb{A}^n \rightarrow C$ such that

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

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

[Marking: 2 if they define a d.p., 2 more for the nearest-neighbour property.]

(b) Suppose \mathbb{A} is the binary alphabet $\{0, 1\}$, and C is the code

$\{0000, 0110, 1011, 1101\}$.

Construct a nearest-neighbour decoding process for C .

[[6]]

Solution: [Similar to coursework]

0000 \mapsto 0000
 0001 \mapsto 0000
 0010 \mapsto 0110 (could instead be 0000)
 0011 \mapsto 1011
 0100 \mapsto 0110 (could instead be 0000)
 0101 \mapsto 1101
 0110 \mapsto 0110
 0111 \mapsto 0110
 1000 \mapsto 0000
 1001 \mapsto 1011 (could instead be 1101)
 1010 \mapsto 1011
 1011 \mapsto 1011
 1100 \mapsto 1101
 1101 \mapsto 1101
 1110 \mapsto 0110
 1111 \mapsto 1011 (could instead be 1101).

(c) Suppose we send the word 1101 along a binary symmetric channel with symbol error probability $\frac{1}{10}$. For your chosen decoding process for C , calculate the word error probability for this word.

[[5]]

Solution: [Similar to coursework] Let's calculate the probability that 1101

is decoded correctly. This is the probability that it maps to one of 0101, 1100 or 1101, which is

$$\frac{1}{10} \times \frac{9}{10} \times \frac{9}{10} \times \frac{9}{10} + \frac{9}{10} \times \frac{9}{10} \times \frac{9}{10} \times \frac{1}{10} + \frac{9}{10} \times \frac{9}{10} \times \frac{9}{10} \times \frac{9}{10} = 0.8019.$$

So the w.e.p. is $1 - 0.8019 = 0.1981$.

(Of course, cunning candidates will shorten the calculation by choosing their d.p. to map as few words to 1101 as possible.)

Now suppose C is a 1-error-correcting code of length 10 over the alphabet $\mathbb{A} = \{0, 1\}$, and f is a nearest-neighbour decoding process for C .

- (d) Prove that for every $v \in C$ and $w \in \mathbb{A}^{10}$ such that $d(v, w) = 1$, we must have $f(w) = v$. [[3]]

Solution: [Unseen] By the error-correcting property, there is no $x \in C$ other than v such that $d(x, w) \leq 1$. So v is the (unique) nearest neighbour to w , and hence $f(w) = v$.

- (e) Given $v \in C$, how many words $w \in \mathbb{A}^{10}$ are there such that $d(v, w) = 1$? [[1]]

Solution: [Unseen] 10. (I'm happy with just the answer.)

- (f) Now suppose words are transmitted along a channel with symbol error probability $\frac{1}{10}$ and decoded using f . Prove that the word error probability for any word in C is less than

$$1 - \left(\frac{9}{10}\right)^9.$$

Solution: [Unseen] By part (d), the probability that a word v gets decoded correctly is at least the probability when it gets transmitted, no more than one symbol is changed. This is

$$\left(\frac{9}{10}\right)^{10} + 10 \times \frac{1}{10} \left(\frac{9}{10}\right)^9$$

(the first term for the probability that v is transmitted faithfully, and the second term for each of the ten words at distance 1). So the w.e.p. is at most 1 minus this, i.e.

$$1 - \left(\frac{9}{10}\right)^{10} - \left(\frac{9}{10}\right)^9 < 1 - \left(\frac{9}{10}\right)^9.$$

Question 3 [In this question, you may assume standard terminology and results from linear algebra.]

Suppose \mathbb{A} is a finite field, and C is a linear $[n, k]$ -code over \mathbb{A} .

- (a) Suppose G is a generator matrix for C , and $w \in \mathbb{A}^n$. Prove that $w \in C^\perp$ if and only if $Gw^T = 0$. [[7]]

Solution: [Bookwork] Writing g_{ij} for the entry in the i th row and j th column of G , we have

$$\begin{aligned}(Gw)_i &= g_{i1}w_1 + \cdots + g_{in}w_n \\ &= g^i \cdot w,\end{aligned}$$

where g^i denotes the i th row of G . Hence $Gw = 0$ if and only if $g^i \cdot w = 0$ for all i .

If $w \in C^\perp$, then we have $v \cdot w = 0$ for all $v \in C$. In particular, since each g^i lies in C , we have $g^i \cdot w = 0$ for all i , so that $Gw = 0$.

Conversely, suppose that $g^i \cdot w = 0$ for all i . Given any $v \in C$, we can write

$$v = \lambda_1 g^1 + \cdots + \lambda_k g^k$$

where $\lambda_1, \dots, \lambda_k \in \mathbb{A}$, because g^1, \dots, g^k span C . Hence

$$\begin{aligned}v \cdot w &= (\lambda_1 g^1 + \cdots + \lambda_k g^k) \cdot w \\ &= \lambda_1 (g^1 \cdot w) + \cdots + \lambda_k (g^k \cdot w) \\ &= \lambda_1 \cdot 0 + \cdots + \lambda_k \cdot 0 \\ &= 0.\end{aligned}$$

So $w \in C^\perp$.

- (b) Deduce that C^\perp is a linear code, and find its dimension. [[5]]

Solution: [Bookwork] The map $\alpha : w \mapsto Gw$ is a linear map from \mathbb{A}^n to \mathbb{A}^k , and by part (a) C^\perp is its kernel. The kernel of a linear map is a subspace of its domain, so C^\perp is a subspace of \mathbb{A}^n , i.e. a linear code. The rank of α is the rank of G ; the rows of G are linearly independent, so the rank is the number of rows, i.e. k . The dimension of \mathbb{A}^n is n . Hence by the Rank–Nullity Theorem, the dimension of C^\perp is the nullity of α , which is n minus the rank of α , i.e. $n - k$.

Now suppose $n \geq 2$ and $\mathbb{A} = \mathbb{F}_2 = \{0, 1\}$, and define the *parity-check code*

$$C = \{v \in \mathbb{F}_2^n \mid v_1 + \dots + v_n = 0\}.$$

(c) What is the dimension of C ? Justify your answer. [[4]]

Solution: [Similar to coursework]

The dimension is $n - 1$. To see this, we find a basis. Let e_1, \dots, e_n be the standard basis of \mathbb{A}^n , and let $v^i = e_i + e_n$, for $i = 1, \dots, n - 1$.

v^1, \dots, v^{n-1} **are linearly independent** Suppose $a_1, \dots, a_{n-1} \in \mathbb{A}$ are such that

$$a_1 v^1 + \dots + a_{n-1} v^{n-1} = 0.$$

Then

$$a_1 e_1 + \dots + a_{n-1} e_{n-1} + (a_1 + \dots + a_{n-1}) e_n = 0.$$

The linear independence of e_1, \dots, e_n then guarantees that $a_1 = \dots = a_{n-1} = 0$.

v^1, \dots, v^{n-1} **span C** Given $v \in C$, we claim that

$$v = v_1 v^1 + \dots + v_{n-1} v^{n-1}.$$

The left-hand side equals

$$v_1 e_1 + \dots + v_n e_n,$$

while the right-hand side equals

$$v_1 e_1 + \dots + v_{n-1} e_{n-1} + (v_1 + \dots + v_{n-1}) e_n.$$

But $v_1 + \dots + v_n = 0$, and so $v_1 + \dots + v_{n-1} = -v_n = v_n$, and so the two sides are equal. So we can express any $v \in C$ as a linear combination of v^1, \dots, v^{n-1} .

So v^1, \dots, v^{n-1} form a basis, so the dimension is $n - 1$.

(d) What is the minimum distance of C ? Justify your answer. [[3]]

Solution: [Similar to coursework] The minimum distance is 2:

C **contains two words** v, w **with** $d(v, w) = 2$ For example, $000 \dots 0$ and $110 \dots 0$.

C **does not contain two words** v, w **with** $d(v, w) = 1$ Suppose it does. Then there is some i such that $v_j = w_j$ for all $j \neq i$, while $v_i = w_i + 1$. But then

$$\begin{aligned} 0 &= v_1 + \dots + v_n \\ &= w_1 + \dots + w_{i-1} + (w_i + 1) + w_{i+1} + \dots + w_n \\ &= (w_1 + \dots + w_n) + 1 \\ &= 1, \end{aligned}$$

a contradiction.

- (e) For which values of n is it true that $C \supseteq C^\perp$? Justify your answer. [[6]]

Solution: [Unseen] Answer: even values of n . We claim that

$$C^\perp = \{00 \dots 0, 11 \dots 1\}.$$

If we have a word w with $w_i = 0$ and $w_j = 1$ for some i, j , then $w \cdot (e_i + e_j) \neq 0$; since $e_i + e_j \in C$, this means that $w \notin C^\perp$. On the other hand $00 \dots 0 \in C^\perp$ since $v \cdot 00 \dots 0 = 0$ for any v , and $11 \dots 1 \in C^\perp$, since

$$v \cdot 11 \dots 1 = v_1 + \dots + v_n = 0$$

for $v \in C$.

So $C \supseteq C^\perp$ if and only if both $00 \dots 0$ and $11 \dots 1$ lie in C . $00 \dots 0$ clearly lies in C , while $11 \dots 1$ lies in C if and only if

$$0 = 1 + 1 + \dots + 1 = n \pmod{2};$$

this is true if and only if n is even.

Question 4 Suppose \mathbb{A} is a finite field, C is a linear code of length n over \mathbb{A} , and H is a parity-check matrix for C .

- (a) Given a word $w \in \mathbb{A}^n$, how can you use H to test whether $w \in C$? [[2]]

Solution: [Bookwork] $w \in C$ if and only if $Hw = 0$. (n.b. I'm quite casual about whether elements of \mathbb{A}^n are considered as row vectors or column vectors. The candidates may write $wH^T = 0$ here.)

- (b) Suppose C is the linear code over \mathbb{F}_3 with parity-check matrix

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

Write down a non-zero word in C . [[2]]

Solution: [Unseen] 0012. (Use test in part (a).)

- (c) Suppose $0 < d \leq n$. Give (with proof) a condition on the columns of H that guarantees that C has minimum distance at least d . (You may assume a relationship between the minimum distance of a linear code and the weights of its words.) [[7]]

Solution: [Bookwork] The condition is that any $d-1$ columns of H should be linearly independent over \mathbb{A} . To prove this, we prove the contrapositive, supposing that C has minimum distance less than d . Since the minimum distance of C equals the smallest weight of any non-zero word in C , we can find a non-zero word $w \in C$ such that w has weight less than d . By the previous part we have $Hw = 0$. Since w has weight less than d , we can find $1 \leq i_1 < \dots < i_{d-1} \leq n$ such that $w_i = 0$ for $i \notin \{i_1, \dots, i_{d-1}\}$. Now the condition $Hw = 0$ means that

$$w_{i_1}c_{i_1} + \dots + w_{i_{d-1}}c_{i_{d-1}} = 0,$$

where c_i denotes the i th column of H . Since w is non-zero, the coefficients $w_{i_1}, \dots, w_{i_{d-1}}$ are not all zero, and so we have a linear dependence between $d-1$ columns of H .

Now suppose q is a prime power, and $r > 0$.

- (d) Explain how to construct a parity-check matrix for an $[n, n-r, 3]$ -code over \mathbb{F}_q , where

$$n = \frac{q^r - 1}{q - 1}.$$

Illustrate by giving a parity-check matrix for a $[6, 4, 3]$ -code over \mathbb{F}_5 . [[7]]

Solution: We define an equivalence relation on the set of non-zero words in \mathbb{A}^r by saying that $x \equiv y$ if $x = \lambda y$ for some non-zero $\lambda \in \mathbb{A}$. We construct a parity-check matrix by taking one vector from each equivalence class, and using these as the columns. For the given example, we want $r = 2$, and we take equivalence class representatives

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

giving a parity-check matrix

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

[Marking: 4 for construction, 3 for example.]

- (e) Explain how to construct a parity-check matrix for a $[q+1, q+1-r, r+1]$ -code over \mathbb{F}_q . Illustrate by giving a parity-check matrix for a $[6, 3, 4]$ -code over \mathbb{F}_5 . [[7]]

Solution: Write the elements of \mathbb{F}_q as a_1, \dots, a_q . Now construct the parity-check matrix

$$\begin{pmatrix} 1 & \dots & 1 & 0 \\ a_1 & \dots & a_q & 0 \\ a_1^2 & \dots & a_q^2 & 0 \\ \vdots & & \vdots & \vdots \\ a_1^{r-1} & \dots & a_q^{r-1} & 1 \end{pmatrix}.$$

For the given example, we get

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

[Marking: 4 for construction, 3 for example.]

Question 5 In this question, we work with the binary alphabet $\mathbb{A} = \{0, 1\}$.

- (a) Suppose $n > 0$. Give (with proof) the value of $A_2(n, n)$.

[[5]]

Solution: [Bookwork] $A_2(n, n) = 2$. First consider the repetition code

$$\{00 \dots 0, 11 \dots 1\}.$$

This has two words at distance n , so is a binary $(n, 2, n)$ -code, so $A_2(n, n) \geq n$. To show that $A_2(n, n) \leq 2$, suppose for a contradiction that we can find an (n, M, n) -code C with $M \geq 3$. Take three distinct words $v, w, x \in C$. Then two of them, say v, w , must have the same last symbol (because there are only two symbols in the alphabet). But then $d(v, w) \leq n - 1$: $d(v, w)$ is the number of values of i such that $v_i \neq w_i$, and since $v_n = w_n$, there are at most $n - 1$ values of i such that $v_i \neq w_i$. This contradicts the fact that C has minimum distance at least n , so no such C exists. So $A_2(n, n) \leq 2$, and hence $A_2(n, n) = 2$.

[Marking: 3 for each part.]

- (b) Suppose $n, d > 1$, and C is a binary (n, M, d) -code. Explain how to construct a binary $(n - 1, M, d - 1)$ -code. (You do not need to prove that your construction works.)

[[3]]

Solution: [Bookwork] Delete the last symbol from each word in the code, and take the resulting set of words of length $n - 1$.

(c) Deduce that for $n, d > 1$,

$$A_2(n-1, d-1) \geq A_2(n, d).$$

Solution: [Bookwork] Taking an (n, M, d) -code C with $M = A_2(n, d)$, we obtain an $(n-1, M, d-1)$ -code. Hence [[3]]

$$A_2(n-1, d-1) \geq M = A_2(n, d).$$

(d) Find (with proof) two integers $n, d > 0$ such that $A_2(n, d) < 2^{n-d+1}$. (You may use a theorem from lectures, as long as you state it accurately.) [[6]]

Solution: [Unseen] We quote half of the Plotkin bound: if $n, d > 0$ with d even and $2d > n$, then

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

Putting $n = 5, d = 4$, we obtain

$$A_2(5, 4) \leq 2 \left\lfloor \frac{4}{3} \right\rfloor = 2 < 2^{5-4+1}.$$

Now suppose C is a binary code containing M words of length n , with minimum distance d . Let C^2 be the code of length $2n$ obtained by joining together all pairs of words in C .

(For example, if

$$C = \{000, 001, 110\},$$

then

$$C^2 = \{000000, 000001, 000110, 001000, 001001, 001110, 110000, 110001, 110110\}.$$

(e) What is the minimum distance of C^2 ? [[2]]

Solution: [Unseen] d : two different words in C^2 have either the first half or the second half different, so have either at least d differences among the first n places, or at least d differences among the last n places. So the minimum distance is at least d . To show that the minimum distance is at most d , we take two words $v, w \in C$ at distance d ; then the words vv and vw in C^2 are at distance d .

(f) How many words does C^2 contain? [[2]]

Solution: [Unseen] M^2 . Can choose the first half of a word in M ways, and the second half in M ways.

- (g) What inequality can you deduce involving $A_2(2n, d)$? [[4]]

Solution: [Unseen]

$$A_2(2n, d) \geq A_2(n, d)^2.$$

(For parts (e,f,g) you are not required to explain your answers.)

Question 6 Suppose \mathbb{A} is a finite field.

- (a) Suppose C and \mathcal{D} are linear codes of length n over \mathbb{A} . Explain what it means to say that C and \mathcal{D} are *equivalent* as linear codes. [[5]]

Solution: [Bookwork] C and \mathcal{D} are equivalent if we can get from C to \mathcal{D} by a sequence of the following operations:

Operation 1 Choose a permutation σ of $\{1, \dots, n\}$, and for each $w = w_1 \dots w_n \in \mathbb{A}^n$ define

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

Now replace C with

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

Operation 2' Choose $i \in \{1, \dots, n\}$ and $a \in \mathbb{A} \setminus \{0\}$, and for each $w = w_1 \dots w_n \in \mathbb{A}^n$ define

$$w_{a,i} = w_1 \dots w_{i-1}(aw_i)w_{i+1} \dots w_n.$$

Now replace C with

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

- (b) What is meant by the *weight* of a word in \mathbb{A}^n ? [[2]]

Solution: [Bookwork] The weight of a word is the number of non-zero symbols in that word.

- (c) Prove that if two linear codes are equivalent, then they have the same number of words of weight w , for each w . [[8]]

Solution: [Similar to coursework] Let $v \in \mathbb{A}^n$, and let σ be a permutation of $\{1, \dots, n\}$. Then v_σ has the same weight as v , because v_σ contains the same symbols as v (in a different order), and hence has the same number of non-zero symbols. So if C is a linear code of length n over \mathbb{A} , then for each w the map $v \mapsto v_\sigma$ is a bijection between the set of words in C with weight w and the set of words in C_σ with weight w . So if we can get from one code to another using Operation 1, then the two codes have the same number of words of weight w , for each w .

Now let $v \in \mathbb{A}^n$, $i \in \{1, \dots, n\}$ and $a \in \mathbb{A} \setminus \{0\}$, and let $u = v_{a,i}$. Then we claim that for each j we claim that $u_j \neq 0$ iff $v_j \neq 0$. For $j \neq i$ this is clear, since $v_j = u_j$. For $j = i$ we have $u_j = av_j$, so if $v_j = 0$ then $u_j = a \cdot 0 = 0$, while if $u_j = 0$ then $v_j = a^{-1} \cdot 0 = 0$.

Hence the number of non-zero symbols in u is the same in v as in u . So for a linear code C , the map $v \mapsto v_{a,i}$ gives a bijection between the set of words in C with weight w and the set of words in $C_{a,i}$ with weight w . So if we can get from one linear code to another using Operation 2', then the two codes have the same number of words of weight w , for each w .

So if we can get from one linear code to another using Operations 1 and 2', then the two codes have the same number of words of weight w , for each w .

Suppose $\mathbb{A} = \mathbb{F}_3$, and let C be the linear code

$$\{0000, 0111, 0222, 2100, 2211, 2022, 1200, 1011, 1122\}.$$

- (d) Find a linear code which is equivalent to C and contains the word 1120. (You do not have to show your working, but doing so may help you to gain marks if you make arithmetical errors.) [[4]]

Solution: [Unseen] Apply Operation 1, with σ being the transposition (2 4), to get

$$\{0000, 0111, 0222, 2001, 2112, 2220, 1002, 1110, 1221\}.$$

Now apply Operation 2', with $i = 3$ and $a = 2$, to get

$$\{0000, 0121, 0212, 2001, 2122, 2210, 1002, 1120, 1211\}.$$

- (e) Find a linear $[4, 2, 2]$ -code \mathcal{D} which is not equivalent to C . Explain briefly why C and \mathcal{D} are not equivalent. [[6]]

Solution: [Unseen] For example

$$\mathcal{D} = \{0000, 0011, 0022, 1100, 1111, 1122, 2200, 2211, 2222\}.$$

To see inequivalence: C contains words of weight 3 but \mathcal{D} does not, so by part (c) C and \mathcal{D} cannot be equivalent.

[Marking: 4 for getting a correct code with no explanation, 2 for explanation.]

Question 7 Suppose \mathbb{A} is a finite field, and C is a linear code of length n over \mathbb{A} .

- (a) Define the terms *coset* and *coset leader*, and describe how to construct a *Slepian array* for C . [[7]]

Solution: [Bookwork] If C is a linear $[n, k]$ -code over \mathbb{A} , a coset of C is a set of the form

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

for $w \in \mathbb{A}^n$. A leader for a coset is an element of minimal weight in that coset. To construct a Slepian array:

- choose a leader in each coset;
- in the first row of the array, write the words in C , with the word $00 \dots 0$ at the left, and the remaining words in any order;
- in the first column write the chosen coset leaders, with $00 \dots 0$ of the coset C at the top, and the remaining coset leaders in any order;
- for the entry in row i and column j , we put the word which equals the coset leader at the start of row i plus the codeword at the top of column j .

[Marking: 2 for defining a coset, 1 for a leader, 4 for a Slepian array.]

- (b) Suppose $\mathbb{A} = \mathbb{F}_3$, and

$$C = \{000, 011, 022, 102, 110, 121, 201, 212, 220\}.$$

Construct a Slepian array for C . (You do not have to explain your working, but doing so may help you to gain marks if you make arithmetical errors.) [[4]]

Solution: [Similar to coursework]

000	011	022	102	110	121	201	212	220
001	012	020	100	111	122	202	210	221
002	010	021	101	112	120	200	211	222

(c) Explain what is meant by:

- the *dual code* C^\perp ;
- a *parity-check matrix* for C ;
- the *syndrome* of a word $w \in \mathbb{A}^n$.

[[4]]

Solution: [Bookwork] Define the scalar product $\cdot : \mathbb{A}^n \times \mathbb{A}^n \rightarrow \mathbb{A}$ by

$$v \cdot w = \sum_{i=1}^n v_i w_i.$$

Define $C^\perp = \{w \in \mathbb{A}^n \mid v \cdot w = 0 \text{ for all } v \in C\}$. A parity-check matrix for C is a generator matrix for C^\perp , that is, a matrix whose rows form a basis of C^\perp . If H is a parity-check matrix for C and w is a word in \mathbb{A}^n , the syndrome of w is the word wH^T .

(d) Define a *syndrome look-up table*, and explain how it is used to construct a nearest-neighbour decoding process for C .

[[5]]

Solution: [Bookwork] A syndrome look-up table has two columns; in the first column there are coset leaders, one from each coset. In the second column, next to the coset leader w we write the syndrome of w . Given a syndrome look-up table, we form a decoding process $f : \mathbb{A}^n \rightarrow C$ as follows. Given a word $w \in \mathbb{A}^n$, calculate its syndrome. Find this syndrome in the look-up table, and let v be the coset leader with the same syndrome. Set $f(w) = w - v$.

[Marking: 3 for a syndrome look-up table, 2 for the decoding process.]

(e) Suppose $\mathbb{A} = \mathbb{F}_3$, and

$$\mathcal{D} = \{0000, 1011, 2022, 0121, 1102, 2110, 0212, 1220, 2201\}.$$

Write down a generator matrix and a parity-check matrix for \mathcal{D} , and construct a syndrome look-up table for \mathcal{D} .

[[5]]

(You do not have to explain your method, but doing so may help you to gain marks if you make arithmetical errors.)

Solution: [Unseen] $\{1011, 0121\}$ is a basis for \mathcal{D} , so \mathcal{D} has a generator matrix

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

Using the standard-form trick, \mathcal{D} has a parity-check matrix

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

\mathcal{D} has a syndrome look-up table

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

[Marking: 2 for the parity-check matrix, 3 for the syndrome table.]

End of Paper