MAS309 Coding Theory: Sheet 3

Please send comments and corrections to M.Jerrum@qmul.ac.uk.
Put solutions in the orange box on the ground floor by 17:00 on Monday, 11th February.

1. Show that for any positive integers n, m, d, q we have:

   (a) $A_q(nm, dm) \geqslant A_q(n, d)$, and [3]
   (HintHintHintHint)

   (b) $A_q(nm, d) \geqslant A_q(n, d)^m$. [3]
   (HintClueTipHint)

2. Prove that, for all $m \geq 1$:

   (a) $A_2(3m, 2m) = 4$, and [4]

   (b) $A_2(3m, 2m + 1) = 2$. [3]

   (Hint: Notice that d is rather large in relation to n here. Which bound from the notes is particularly appropriate in this situation? Also, don't forget your answer to Question 1!)

3. (a) What is the capacity of a binary symmetric channel with error probability $\frac{1}{4}$? Express your answer in terms of $\log_2 3$.) [1]

   (b) Let $\mathcal{C}$ be the binary code $\{\mathtt{000}, \mathtt{001}, \mathtt{011}, \mathtt{111}\}$. What is the rate of code $\mathcal{C}$? [1]

   (c) Design a nearest-neighbour decoding process $f : \{\mathtt{0}, \mathtt{1}\}^3 \to \mathcal{C}$ for $\mathcal{C}$ that has the property that $|f^{-1}(v)| = 2$ for all codewords $v \in \mathcal{C}$. (Note: the solution is unique.) [2]

   (d) Given your decoding process of part (c), what is the error probability for the word 000 transmitted through the channel of part (a)? [2]

Please turn over.

4. This question is an exercise in linear algebra, just to make sure that your skills in this area are up to scratch, and to give you an idea of the kind of counting arguments that can be used when doing linear algebra with a finite field. There will not be questions like this in the exam.

   Suppose V is a vector space of dimension 2 over $\mathbb{F}_q$.

   (a) How many vectors are there in V? [1]

   (b) Show that $\{v, w\}$ is a basis of V if and only if

   - $v \neq 0$, and
   - $w \notin \langle v \rangle$. [2]

   (You may assume that a set of d vectors in a vector space of dimension d is a basis if and only if the vectors are linearly independent.)

   (c) If $v \neq 0$, what is the dimension of $\langle v \rangle$? So how many vectors are there in $\langle v \rangle$? [1]

   (d) Show that the number of different bases of V is

   $$\frac{(q^2-1)(q^2-q)}{2}.$$ [2]

   (N.B. We don't count $\{v, w\}$ as a different basis from $\{w, v\}$.)

Solutions

1. (a) Suppose we have a q-ary (n, M, d)-code $\mathcal{C}$, where $M = A_q(n, d)$. We form a code $\mathcal{D}$ of length mn by writing each codeword m times, e.g. if $\mathcal{C} = \{\mathtt{001}, \mathtt{110}, \mathtt{101}\}$ and $m = 3$, then $\mathcal{D} = \{\mathtt{001001001}, \mathtt{110110110}, \mathtt{101101101}\}$. $\mathcal{D}$ has M codewords, so to prove that $\mathcal{D}$ is an (mn, M, md)-code we need to prove that $d(x, y) \geqslant md$ for all $x, y \in \mathcal{D}$ with $x \neq y$.

   Codewords x and y are obtained by repeating codewords from $\mathcal{C}$ m times; suppose x is obtained from $v \in \mathcal{C}$ and y is obtained from $w \in \mathcal{C}$. Now, $v \neq w$, so we have $d(v, w) \geqslant d$. So v and w differ in at least d positions. Now if x and y differ in position i, then v and w differ in positions $i, n + i, 2n + i, 3n + i, \ldots, (m - 1)n + i$. So for each position where v and w differ there are m positions where x and y differ, so there are alogether at least dm positions where x and y differ.

   So $\mathcal{D}$ is an (mn, M, md)-code and $A_q(mn, md) \geqslant M$.

   (b) Suppose we have a q-ary (n, M, d)-code $\mathcal{C}$, where $M = A_q(n, d)$. We form a code $\mathcal{D}$ of length mn by writing all possible strings of m codewords from $\mathcal{C}$, e.g. if $\mathcal{C} = \{\mathtt{001}, \mathtt{110}, \mathtt{101}\}$ and $m = 2$, then

   $$\mathcal{D} = \{\mathtt{001001}, \mathtt{001110}, \mathtt{001101}, \mathtt{110001}, \mathtt{110110}, \mathtt{110101}, \mathtt{101001}, \mathtt{101110}, \mathtt{101101}\}.$$

   The number of codewords in $\mathcal{D}$ is M^m, since we can choose the first word in the string in M different ways, and we can choose the second in M different ways, and so on. And the minimu distance of $\mathcal{D}$ is at least d: given $v, w \in \mathcal{D}$, suppose that v is obtained by joining together the words $v^1, v^2, \ldots, v^m$ and w is obtained by joining together the words $w^1, w^2, \ldots, w^m$. If $v \neq w$, then $v^i \neq w^i$ for some i; since $\mathcal{C}$ has minimum distance at least d, the words v^i and w^i differe in at least d positions, and so v and w differ in at least d positions. So $\mathcal{D}$ is an (mn, M^m, d)-code and $A_q(mn, d) \geqslant M^m$.

2. (a) Apply the Plotkin bound with $n = 3m$ and $d = 2m$:

   $$A_2(3m, 2m) \leq 2 \left\lfloor \frac{2m}{2 \times 2m - 3m} \right\rfloor = 2 \left\lfloor \frac{2m}{m} \right\rfloor = 4.$$

   On the other hand, by Question 1(a), $A_2(3m, 2m) \geq A_2(3, 2) \geq 4$. (The latter inequality comes from considering the binary parity-check code of length 3.)

   (b) Apply the Plotkin bound with $n = 3m$ and $d = 2m + 1$:

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

   On the other hand, $A_2(3m, 2m + 1) \geq 2$ by considering the binary repetition code of length $3m \geq 2m + 1$.

3. (a)

$$\begin{aligned} C(\tfrac{1}{4}) &= 1 + \tfrac{1}{4}\log_2(\tfrac{1}{4}) + \tfrac{3}{4}\log_2(\tfrac{3}{4}) \\ &= 1 - \tfrac{1}{2} + \tfrac{3}{4}(\log_2 3 - 2) \\ &= \tfrac{3}{4}\log_2 3 - 1. \end{aligned}$$

(b) The rate of $\mathcal{C}$ is $(\log_2 4)/3 = \frac{2}{3}$.

(c) The decoding function must map the codewords `000`, `001`, `011` and `111` to themselves. The non-codewords `100` and `110` both have unique nearest neighbours, namely `000` and `111`, respectively. The remaining non-codewords have two nearest neighbours each, but the additional condition on f (preimages of codewords have size 2) forces us to assign `101` to `001` and `010` to `011`. Summarising:

$$\begin{aligned} f(\texttt{000}) &= \texttt{000} \\ f(\texttt{001}) &= \texttt{001} \\ f(\texttt{010}) &= \texttt{011} \\ f(\texttt{011}) &= \texttt{011} \\ f(\texttt{100}) &= \texttt{000} \\ f(\texttt{101}) &= \texttt{001} \\ f(\texttt{110}) &= \texttt{111} \\ f(\texttt{111}) &= \texttt{111}. \end{aligned}$$

(d) In order to correctly recover `000` the word received must be either `000` or `100`. The first case occurs with probability $(1-p)^3$ and the second with probabilty $p(1-p)^2$. The probability of *correct* decoding is thus $(\frac{3}{4})^3 + (\frac{1}{4})(\frac{3}{4})^2 = \frac{27+9}{64} = \frac{36}{64} = \frac{9}{16}$. The word error probability for `000` is thus $1 - \frac{9}{16} = \frac{7}{16}$.

4. (a) q^2, from Lemma 4.5 in lectures.

(b) We need to show that v, w are linearly independent if and only if they satisfy the two given conditions. Suppose first that v, w are not linearly independent, so we have

$$\lambda v + \mu w = 0,$$

with λ, μ not both zero.

- If $\mu \neq 0$, then we have
$$w = -\frac{\lambda}{\mu} v,$$
so $w \in \langle v \rangle$.
- If $\mu = 0$, then $\lambda \neq 0$ and
$$\lambda v = 0,$$
and we can divide by λ to get $v = 0$.

Conversely, suppose one of the given conditions is not true. If $v = 0$, then we have $1.v + 0.w$ so that v and w are not linearly independent. If $w \in \langle v \rangle$, then $w = \lambda v$ for some $\lambda \in \mathbb{F}_q$, so we have $-\lambda.v + 1.w$ so that again v, w are not linearly independent.

(c) If $v \neq 0$, then $\{v\}$ is a linearly independent set and hence $\{v\}$ is a basis for $\langle v \rangle$. Thus $\dim\langle v \rangle = 1$, and $\langle v \rangle$ contains q vectors, by Lemma 4.5.

(d) By (b), the number of ways of choosing a basis for V is the number of ways of choosing two vectors v, w satisfying the conditions of part (b). First we choose v. There are q^2 vectors altogether, but we must have $v \neq 0$, so we have $q^2 - 1$ possibilities for v. Next we choose w. There are q^2 vectors altogether, but we're not allowed to choose any vector in $\langle v \rangle$. There are q vectors in $\langle v \rangle$ by (c), so we have $q^2 - q$ possibilities for w. So the total number of ways of choosing v, w is

$$(q^2 - 1)(q^2 - q).$$

But we could have chosen these vectors in the other order, and we'd still have the same basis. So we've counted each basis twice, so we must divide by 2 to get the number of different bases.