MAS309 Coding Theory: Sheet 4

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, 18th February.

1. Suppose $\mathcal{C}$ is a linear binary code of length n. Let $\pi = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ be the permutation that transposes `0` and `1`. Denote by $\overline{\mathcal{C}}$ the code $\overline{\mathcal{C}} = \{\pi(x_1)\pi(x_2)\ldots\pi(x_n) : x_1x_2\ldots x_n \in \mathcal{C}\}$ obtained by "complementing" the codewords in $\mathcal{C}$. (Thus if $\mathcal{C}$ contains the codeword `011` then $\overline{\mathcal{C}}$ will contain the codeword `100`, and vice versa.)

   (a) Write down a linear binary $[3, 2]$-code $\mathcal{C}$ such that $\overline{\mathcal{C}}$ is also a linear code. [3]

   (b) Write down a linear binary $[3, 2]$ code $\mathcal{C}$ such that $\overline{\mathcal{C}}$ is not a linear code. [3]

   (c) In general, what is the relationship between the minimum distances of $\mathcal{C}$ and $\overline{\mathcal{C}}$? [2]

   In all three parts, explain your reasoning.

2. Suppose $\mathcal{C}$ is a linear code of length n over $\mathbb{F}_q$. Prove that $\mathcal{C}^2 = \{vv : v \in \mathcal{C}\}$ is a linear code of length $2n$ over $\mathbb{F}_q$. (Juxtaposition here denotes concatenation; so, for example, if $v =$ `1101` then $vv =$ `11011101`.) [5]

3. Let $\mathcal{C}$ be the following linear binary code of length six:

$$\mathcal{C} = \{\texttt{000000}, \texttt{000111}, \texttt{011011}, \texttt{011100}, \texttt{101001}, \texttt{101110}, \texttt{110010}, \texttt{110101}\}.$$

   (a) What is the dimension of $\mathcal{C}$? Briefly explain your answer. [1]

   (b) What is its minimum distance of $\mathcal{C}$? Briefly explain your answer. [1]

   (c) Which of the following are generator matrices for $\mathcal{C}$? Justify your answers.

$$\begin{pmatrix}\texttt{011100}\\ \texttt{101001}\end{pmatrix}, \begin{pmatrix}\texttt{011100}\\ \texttt{101110}\\ \texttt{110011}\end{pmatrix}, \begin{pmatrix}\texttt{011100}\\ \texttt{101110}\\ \texttt{110101}\end{pmatrix}, \begin{pmatrix}\texttt{011100}\\ \texttt{101110}\\ \texttt{110010}\end{pmatrix}, \begin{pmatrix}\texttt{000111}\\ \texttt{011100}\\ \texttt{101001}\\ \texttt{110010}\end{pmatrix}. \quad [5]$$

4. Consider the matrices

$$G_1 = \begin{pmatrix}\texttt{00111}\\ \texttt{11110}\end{pmatrix} \quad \text{and} \quad G_2 = \begin{pmatrix}\texttt{11100}\\ \texttt{00111}\end{pmatrix}$$

   (a) Do G_1 and G_2 generate the same binary code over $\mathbb{F}_2$? [2]

   (b) Do G_1 and G_2 generate equivalent binary codes over $\mathbb{F}_2$? [3]

   Justify your answer in both cases.

Solutions

1. (a) If $\overline{\mathcal{C}}$ is to be a linear code it must contain the codeword 000, and hence $\mathcal{C}$ must contain the codeword 111; let this be one element in our basis for $\mathcal{C}$. For the other, choose any vector other than 000 and 111, say 001. Then

$$\mathcal{C} = \langle 001, 111 \rangle = \{000, 001, 110, 111\}$$

and

$$\overline{\mathcal{C}} = \{111, 110, 001, 000\} = \mathcal{C},$$

which we know is linear. (The answer is unique up to equivalence.)

(b) By the observation of the previous part, we just need to find a code of dimension 2 not containing the codeword 111. The first example that comes to mind is the parity-check code:

$$\mathcal{C} = \{000, 011, 101, 110\},$$

but

$$\mathcal{C}' = \{000, 001, 010, 011\}$$

will also do. These two are the only possibilities, up to equivalence.

(c) The minimum distances of the two codes are equal, since the operation of permuting alphabet symbols at any position preserves minimum distance (Corollary 1.9), even though it does not preserve linearity.

2. Suppose $uu, vv \in \mathcal{C}^2$ are any two codewords in $\mathcal{C}^2$ and $\lambda \in \mathbb{F}_q$ any scalar.

We need to verify that the vector subspace axioms hold.

- (Zero vector exists.) Since $0^n \in \mathcal{C}$, so $0^n 0^n = 0^{2n} \in \mathcal{C}^n$.
- (Closure under vector addition.) We have $uu + vv = (u + v)(u + v) = ww$ where $w = u + v \in \mathcal{C}$. Hence $uu + vv = ww \in \mathcal{C}^2$.
- (Closure under scalar multiplication.) We have $\lambda(uu) = (\lambda u)(\lambda u) = ww$, where $w = \lambda u \in \mathcal{C}$. Hence $\lambda(uu) = ww \in \mathcal{C}^2$.

As we touched on in the lectures: the third test is actually redundant, since the underlying field is finite.

3. (a) If $\mathcal{C}$ has dimsension d, then the number of words in $\mathcal{C}$ is 2^d, by Lemma 4.5. There are 8 words in $\mathcal{C}$, so $d = 3$.

(b) The minimum distance is 3, since that is the minimum weight of a non-zero codeword, e.g., 000111.

(c) A matrix is a generator matrix for $\mathcal{C}$ if and only if its rows form a basis for $\mathcal{C}$. Since $\mathcal{C}$ has dimension 3, any basis must contain 3 vectors, and so a generator matrix must have 3 rows. So the first and last matrices are not generator matrices. The second

matrix is not a generator matrix, since one of its rows, namely 110011 is not a codeword in $\mathcal{C}$. The fourth matrix is not a generator matrix since its rows are not linearly independent: $011100 + 101110 + 110010 = 000000$.

The third matrix is a generator matrix, since its three rows are all codewords and are linearly independent. (There are no duplicate rows and the three rows sum to a non-zero vector.)

4. (a) No, the codes are not the same. E.g., the word 11110 is a row of G_1, but clearly not in the row space of G_2. So the row spaces of G_1 and G_2 are different, and so are the codes they generate.

   (b) Yes, they do indeed generate equivalent codes. E.g., First add row 1 of G_1 to row 2 (MO2) to obtain

$$G_1' = \begin{pmatrix} 00111 \\ 11001 \end{pmatrix}.$$

   Then apply apply a column permutation σ (MO4) to map G_1' to G_2. A possible choice is

$$\sigma = \begin{pmatrix} 12345 \\ 34512 \end{pmatrix}.$$

   But inevitably there are other solutions.