MAS309 Coding Theory: Sheet 6

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 10th March.

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

   (a) Show that $k = 2$. [1]

   (b) Show that every word in $\mathcal{C}$ has even weight. [2]

   (c) Show that $\mathcal{C}$ contains at least two words of weight 2. [1]

   (d) Show that $\mathcal{C}$ is one of the codes

   $$\{\mathtt{0000}, \mathtt{0011}, \mathtt{1100}, \mathtt{1111}\},$$
   $$\{\mathtt{0000}, \mathtt{0101}, \mathtt{1010}, \mathtt{1111}\}, \quad \text{or}$$
   $$\{\mathtt{0000}, \mathtt{0110}, \mathtt{1001}, \mathtt{1111}\}.$$ [2]

2. Let $\mathcal{C}$ be the binary $[5, 3]$-code with generator matrix

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

   (a) Write down a generator matrix H for $\mathcal{C}^\perp$, the code dual to $\mathcal{C}$. (Note that G *cannot* be reduced to standard form using just row operations, so Lemma 5.7 is not applicable here.) Verify that H is a parity-check matrix for $\mathcal{C}$ by appealing to Lemma 5.6. [3]

   (b) Consider $\mathcal{D} = \mathcal{C} \cap \mathcal{C}^\perp$. Since $\mathcal{D}$ is the intersection of linear subspaces of $\mathbb{F}_2^5$, it is itself a linear $[5, k]$-code for some k. What is k? Write down a generator matrix for $\mathcal{D}$. Briefly justify your answer. [2]

   (c) Is $\mathcal{C} \cup \mathcal{C}^\perp$ a linear code? Briefly justify your answer. [2]

3. Suppose $\mathcal{C}$ is a binary $[n, k]$-code with generator matrix G, and that H is a generator matrix for the dual code $\mathcal{C}^\perp$. Let $H_{*1}, \ldots, H_{*n}$ be an enumeration of the columns of H.

   (a) Prove that if $\mathcal{C}$ has minimum distance 1 then there exists i such that H_{*i} is the zero vector. [3]

   (b) Prove that if $\mathcal{C}$ has minimum distance 2 then there exist distinct i, j such that $H_{*i} = H_{*j}$. [2]

   Remark. (a) and (b) tell us that if we have a matrix H with no zero columns and no repeated columns, then H is a parity-check matrix of a code with minimum distance at least 3.

[Continued overleaf.]

4. Let $\mathcal{C}$ be the linear $[6, 3]$-code over $\mathbb{F}_5$ with generator matrix

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

(a) By applying the matrix row-operations MO1–3, put this matrix in standard form, i.e., find a standard-form generator matrix G for the code $\mathcal{C}$. (Note that it is not necessary to use the column operations MO4,5, so the resulting standard-form matrix is for $\mathcal{C}$ itself, not merely a code equivalent to $\mathcal{C}$.) [3]

(b) Write down a parity-check matrix for $\mathcal{C}$. [2]

(c) Find the syndromes of the words `220121` and `020241`. [2]

Solutions

1. (a) $\mathcal{C}$ is a $[4, 4-k]$-code, so if $\mathcal{C}^\perp = \mathcal{C}$ then $4-k = k$, i.e. $k = 2$.

   (b) If $v \in \mathcal{C}$ then $v \in \mathcal{C}^\perp$, and so we must have $v.v = \mathtt{0}$. Now $v.v = v_1^2 + v_2^2 + v_3^2 + v_4^2$, and this equals $v_1 + v_2 + v_3 + v_4$, since $\mathtt{0}^2 = \mathtt{0}$ and $\mathtt{1}^2 = \mathtt{1}$. So $v.v = \mathtt{0}$ implies that v contains an even number of 1s.

   (c) $\mathcal{C}$ contains 4 words, by Lemma 4.5, and each of these has weight 0, 2 or 4. There is only one word in $\mathbb{F}_2^4$ of weight 0, and only one of weight 4, so there are at least two words in $\mathcal{C}$ of weight 2.

   (d) Let v, w be two words of weight 2 in $\mathcal{C}$. This means that v and w are two of the following words:

   $$\mathtt{0011}, \mathtt{0101}, \mathtt{0110}, \mathtt{1001}, \mathtt{1010}, \mathtt{1100}.$$

   Since $w \in \mathcal{C}^\perp$ we must have $v.w = \mathtt{0}$, and by checking the products of all pairs of the above words, we find that $\{v, w\}$ must be $\{\mathtt{0011}, \mathtt{1100}\}$, $\{\mathtt{0101}, \mathtt{1010}\}$ or $\{\mathtt{0110}, \mathtt{1001}\}$. In any of these cases, we find that $v + w = \mathtt{1111}$, and so $\mathcal{C}$ must be one of the codes listed.

2. (a) One possibility is

   $$H = \begin{pmatrix} \mathtt{0}&\mathtt{0}&\mathtt{1}&\mathtt{1}&\mathtt{1} \\ \mathtt{1}&\mathtt{1}&\mathtt{1}&\mathtt{0}&\mathtt{0} \end{pmatrix}.$$

   (I did this "by inspection". As a last resort, one could enumerate all words in the dual code, since there are just four of them.)

   Verification: The rows of H are clearly independent, and

   $$GH^\perp = \begin{pmatrix} \mathtt{0}&\mathtt{0}&\mathtt{0}&\mathtt{1}&\mathtt{1} \\ \mathtt{1}&\mathtt{1}&\mathtt{0}&\mathtt{0}&\mathtt{0} \\ \mathtt{0}&\mathtt{1}&\mathtt{1}&\mathtt{1}&\mathtt{0} \end{pmatrix} \times \begin{pmatrix} \mathtt{0}&\mathtt{1} \\ \mathtt{0}&\mathtt{1} \\ \mathtt{1}&\mathtt{1} \\ \mathtt{1}&\mathtt{0} \\ \mathtt{1}&\mathtt{0} \end{pmatrix} = \begin{pmatrix} \mathtt{0}&\mathtt{0} \\ \mathtt{0}&\mathtt{0} \end{pmatrix}.$$

   Thus the two conditions of lemma 5.6 are satisfied.

   (b) The only non-zero vector that is in the row spaces of both G and H is $\mathtt{11011}$. Thus the dimension of $\mathcal{D}$ is $k = 1$, and

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

   is its (unique) generator matrix.

   (c) $\mathcal{C} \cup \mathcal{C}^\perp$ has

   $$|\mathcal{C} \cup \mathcal{C}^\perp| = |\mathcal{C}| + |\mathcal{C}^\perp| - |\mathcal{C} \cap \mathcal{C}^\perp| = |\mathcal{C}| + |\mathcal{C}^\perp| - |\mathcal{D}| = 8 + 4 - 2 = 10$$

   codewords. But the number of codewords in any binary linear code is a power of 2.

3. (a) Since $\mathcal{C}$ has minimum distance 1, it contains a codeword v of weight 1. Suppose v has its unique 1 in position i. Let $w = w_1 \dots w_n \in \mathcal{C}^\perp$ be any codeword in the dual code. Since $v \cdot w = 0$, we have $w_i = 0$. This is so for any codeword in $\mathcal{C}^\perp$, and in particular for the rows of H. So $H_{*i} = 0$.

   (b) Since $\mathcal{C}$ has minimum distance 2, it contains a codeword v of weight 2. Suppose v has 1s in positions i and j. Let $w = w_1 \dots w_n \in \mathcal{C}^\perp$ be any codeword in the dual code. Since $v \cdot w = 0$, we have $w_i + w_j = 0$; equivalently, $w_i = w_j$ since we are working in $\mathbb{F}_2$. This is so for any codeword in $\mathcal{C}^\perp$, and in particular for the rows of H. So $H_{*i} + H_{*j} = 0$.

4. (a) Subtract row 1 from row 3 (equivalently, add 4 times row 1 to row 3):

$$\begin{pmatrix} 123400 \\ 010224 \\ 001313 \end{pmatrix}.$$

   Now add 3 times row 2 to row 1:

$$\begin{pmatrix} 103012 \\ 010224 \\ 001313 \end{pmatrix}.$$

   Finally add twice row 3 to row 1:

$$\begin{pmatrix} 100133 \\ 010224 \\ 001313 \end{pmatrix}.$$

   The resulting generator matrix for $\mathcal{C}$ is in standard form.

   (b) By Lemma 5.7, the parity-check matrix is

$$H = \begin{pmatrix} 432100 \\ 234010 \\ 212001 \end{pmatrix}.$$

   (c) The syndromes are

$$S(220121) = 220121\, H^T = 022 \qquad S(010241) = 010241\, H^T = 022.$$