MAS309 Coding Theory: Sheet 7

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 17th March.

1. Let $\mathcal{C}$ be the $[4, 2]$-code over $\mathbb{F}_3$ with generator matrix

$$G = \begin{pmatrix} 1\,0\,1\,2 \\ 0\,1\,1\,2 \end{pmatrix}.$$

   (a) Using Lemma 5.7, write down a parity-check matrix H for $\mathcal{C}$ in standard form. [1]

   (b) Compute the syndromes $S(u)$ and $S(v)$ of $u = 0211$ and $v = 1220$. What can you deduce from a comparison of $S(u)$ and $S(v)$? [2]

   (c) Compute a syndrome look-up table for $\mathcal{C}$. (Probably the easiest way is to compute syndromes for words of weight 1, and then fill in any gaps in the table "by inspection".) [2]

   (d) Use the syndrome look-up table to decode u and v. [2]

2. Demonstrate that $A_2(32, 4) = 2^{26}$. (I.e., that the maximum number of words in a binary code of length 32 and minimum distance 4 is precisely $67\,108\,864$.) [3]

3. (a) The Hamming code $\mathrm{Ham}(2, 7)$ is a linear $[n, k, d]$-code over $\mathbb{F}_7$. What are n, k and d? [3]

   (b) Write down a parity-check matrix H for the Hamming code $\mathrm{Ham}(2, 7)$. (To ensure we all have the same matrix in mind, adopt the following conventions: (i) the first non-zero entry in each column is `1`; (ii) the columns, viewed as base-7 numbers, appear in increasing order.) [1]

   (c) Construct a partial syndrome look-up table, just for the coset leaders `00000000`, `00000001`, `00000010`, `00000100` up to `10000000` (i.e., all words of weight at most 1 composed of `0`s and `1`s. (There are 49 syndromes in all, so I'm not asking for the whole table!) [2]

   (d) Find the syndrome of $u = 21063435$, and use it to decode u. (If the syndrome is not in your partial look-up table, try doing the calculation again!) [1]

   (e) Find the syndrome of $v = 21064435$. Observe that if coset leader $0 \ldots 010 \ldots 0$ has syndrome y, then coset leader $0 \ldots 0\lambda 0 \ldots 0$ has syndrome λy. Hence decode v. [1]

4. Let $\mathcal{H} = \text{Ham}(r, 3)$ for a positive integer r, and let $n = (3^r - 1)/2$. Recall that $\mathcal{H}$ is a perfect 1-error-correcting code, which means that for every $w \in \mathbb{F}_3^n$, there is a unique $v \in \mathcal{H}$ such that $d(v, w) \leqslant 1$.

   (a) Suppose w is a word in $\mathbb{F}_3^n$ of weight 2. Show that there is a unique codeword $v \in \mathcal{H}$ of weight 3 such that $d(v, w) = 1$. [2]

   (b) If v is a word in $\mathbb{F}_3^n$ of weight 3, show that there are exactly three words $w \in \mathbb{F}_3^n$ of weight 2 such that $d(v, w) = 1$. [2]

   (c) How many words of weight 2 are there in $\mathbb{F}_3^n$? [1]

   (d) How many words of weight 3 are there in $\mathcal{H}$? [2]

Solutions

1. (a) From Lemma 5.7,

$$H = \begin{pmatrix} 2\,2\,1\,0 \\ 1\,1\,0\,1 \end{pmatrix}.$$

is a parity-check matrix for $\mathcal{C}$.

(b)

$$S(u) = uH^T = 20 \quad \text{and} \quad S(v) = vH^T = 20.$$

Since $S(u) = S(v)$, the words u and v are in the same coset.
The syndrome look-up table is:

$$\begin{aligned}
00 &\to 0000 \\
01 &\to 0001 \\
02 &\to 0002 \\
10 &\to 0010 \\
11 &\to 0011 \quad (\text{or } 0120 \text{ or } 0202 \text{ or } 1020 \text{ or } 2002) \\
12 &\to 0200 \quad (\text{or } 2000) \\
20 &\to 0020 \\
21 &\to 0100 \quad (\text{or } 1000) \\
22 &\to 0022 \quad (\text{or } 0210 \text{ or } 0101 \text{ or } 2010 \text{ or } 1001)
\end{aligned}$$

(c) We saw that $S(u) = S(v) = 20$. According to the syndrome look-up table, the corresponding coset leader is 0020 in both cases. So the decoded words are

$$0211 - 0020 = 0221$$

and

$$1220 - 0020 = 1200.$$

(The decoding is unique, since the coset leader is uniquely defined in this instance.)

2. The Hamming code $\mathrm{Ham}(5, 2)$ is a binary $[2^5 - 1, 2^5 - 5 - 1, 3]$-code, i.e., it has length $2^5 - 1 = 31$, size $2^{2^5-5-1} = 2^{26}$, and minimum distance 3. Thus $A(31, 3) \geq 2^{26}$, and, since $\mathrm{Ham}(5, 2)$ attains the Hamming bound, $A(31, 3) = 2^{26}$. Then, by Theorem 2.3, $A(32, 4) = 2^{26}$.

3. (a)

$$\begin{aligned}
&n = (q^r - 1)/(q - 1) = (7^2 - 1)/(7 - 1) = 48/6 = 8, \\
&k = n - r = 8 - 2 = 6, \quad \text{and} \\
&d = 3.
\end{aligned}$$

(b)

$$H = \begin{pmatrix} 01111111 \\ 10123456 \end{pmatrix}$$

(c)

$$\begin{aligned} 00 &\to 00000000 \\ 16 &\to 00000001 \\ 15 &\to 00000010 \\ 14 &\to 00000100 \\ 13 &\to 00001000 \\ 12 &\to 00010000 \\ 11 &\to 00100000 \\ 10 &\to 01000000 \\ 01 &\to 10000000 \end{aligned}$$

(d) Syndrome is $S(u) = uH^T = 10$, so the decoding is $u - 01000000 = 20063435$.

(e) Syndrome is $S(v) = vH^T = 23 = 2 \times 15$, so the decoding is $v - 2 \times 00000020 = 21064415$.

4. (a) There is exactly one word $v \in \mathcal{H}$ such that $d(v, w) \leqslant 1$. This implies that the weight of v is 1, 2 or 3. Hence the weight of v equals 3: $\mathcal{H}$ has minimum dstance 3, so has no codewords of weight 1 or 2. In particular, $v \neq w$, so $d(v, q) = 1$.

(b) We obtain w from v by changing one symbol, and since the weight of w is less than the weight of v, we must change a non-zero symbol into zero. There are three different non-zero symbols in v we could choose to change, so there are three possible ws. For example, if $v = 0121$, then the possible ws are $0021, 0101, 0120$.

(c) There are exactly $4\binom{n}{2}$ words of weight 2: we choose a word of weight 2 by choosing which two positions will contain the non-zero symbols ($\binom{n}{2}$ choices), and then we choose what each of those symbols will be (2 choices for each).

(d) By part (a) we can define a function

$$f : \{\text{words of weight } 2\} \longrightarrow \{\text{codewords of weight } 3\}$$

by sending a word w to the unique codeword v such that $d(v, w) = 1$. By part (b) this is a three-to-one function, i.e. for every codeword v of weight 3, there are exactly three words w such that $f(w) = v$. This means that the number of words of weight 2 is three times the number of codewords of weight 3, so

$$\text{no. of codewords of weight } 3 = \frac{\text{no. of words of weight } 2}{3} = \frac{4\binom{n}{2}}{3}.$$