Coding Theory

Sheet 6 Solutions

Spring 2014

1. For $\text{Ham}(r,q)$,
$$n = \frac{q^r - 1}{q-1}, \quad k = n - r, \quad d = 3.$$
A code C is MDS if $d = n - k + 1$. Hence $\text{Ham}(r,q)$ is MDS when $3 = r + 1$; that is, $r = 2$. So, only $\text{Ham}(2,q)$ is MDS.

2. (a) $\text{Ham}(2,3)$ is a $[4,2]$ code.
$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix} = H.$$
Hence
$$G = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{bmatrix}.$$
(b) $\text{Ham}(2,4)$ is a $[5,3]$ code; $\mathbf{F}_4 = \{0, 1, \omega, \bar{\omega} \mid \bar{\omega} = \omega + 1 = \omega^2\}$.
$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \bar{\omega} \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & \omega & \bar{\omega} & 0 & 1 \end{bmatrix} = H.$$
Hence
$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega \\ 0 & 0 & 1 & 1 & \bar{\omega} \end{bmatrix}.$$
(c) $\text{Ham}(3,3)$ is a $[13,10]$ code. Similarly, to the previous examples, let
$$H = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 1 & 0 \\ 1 & 2 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}.$$

Hence

$$H = \left[\begin{array}{cccccccccc|ccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1
\end{array}\right].$$

(d) Ham$(3, 4)$ is a $[21, 18]$ code. Here,

$$H = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \omega & \omega & \omega & \omega & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\
1 & 0 & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega}
\end{bmatrix},$$

$$\begin{aligned} H' &= \begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \omega & \omega & \omega & \omega & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & 0 & 1 & 0 \\
1 & \omega & \bar{\omega} & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega} & 0 & 1 & \omega & \bar{\omega} & 0 & 0 & 1
\end{bmatrix} \\
&= [B\ I_3]\,. \end{aligned}$$

Then $G' = \left[I_{18}\ B^T\right]$.

(e) Ham$(3, 5)$ is a $[31, 28]$ code. Here, $H = [A_1\ A_2] = [B\ I_3]$, where

$$A_1 = \begin{bmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4
\end{bmatrix}$$

$$A_2 = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 4 & 0 & 1 & 0 \\
0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 0 & 1
\end{bmatrix}.$$

So $G = [I_{28} \quad -B^T]$.

(f) Ham(4, 2) is a [15, 11] code.

$$\begin{aligned}
H &= \begin{bmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix} \\
&\to \begin{bmatrix} 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0 \\ 0&1&1&1&0&0&0&1&1&1&1&0&1&0&0 \\ 1&0&1&1&0&1&1&0&0&1&1&0&0&1&0 \\ 1&1&0&1&1&0&1&0&1&0&1&0&0&0&1 \end{bmatrix} \\
&= H' = [B\ I_4].
\end{aligned}$$

Then $G = [I_{11}\ B^T]$.

3. Use H as in 3(f). A coset leader is 0 or $l_i,\ i = 1, \ldots, 15$. For a received message y_j, let x_j be the corrected message.

   (a) $y_1 = 00000\,00000\,11111 \Rightarrow y_1 H^T = 1011 \Rightarrow$ coset leader is l_{11} $\Rightarrow x_1 = 00000\,00000\,01111$;

   (b) $y_2 = 00000\,11111\,11111 \Rightarrow y_2 H^T = 0001 \Rightarrow$ coset leader is l_1 $\Rightarrow x_2 = 10000\,11111\,11111$;

   (c) $y_3 = 11111\,11111\,11111 \Rightarrow y_3 H^T = 0000 \Rightarrow x_3 = y_3$.

4. Let $\mathbf{F}_4 = \{0, 1, \omega, \bar{\omega} \mid \bar{\omega} = \omega + 1 = \omega^2\}$. Use H as in 3(d).

   (a) $y = 1111111\ 1111111\ 1111111 \Rightarrow yH^T = 001 \Rightarrow x = 0111111\ 1111111\ 1111111$;

   (b) $y' = 1111111\ \omega\omega\omega\omega\omega\omega\omega\ \bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega} \Rightarrow y'H^T = 1\omega\omega$ $\Rightarrow x' = 1111111\ \omega\omega\omega\omega\omega\omega\omega\ \bar{\omega}\omega\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}$.

5. Since $x \cap y = (x_1 y_1, \ldots, x_n y_n)$, so

$$x \cap y = (z_1, \ldots, z_n), \text{ where } z_i = 1 \Leftrightarrow x_i = y_i = 1.$$

Also

$$x + y = (t_1, \ldots, t_n), \text{ with } t_i = 1 \Leftrightarrow (x_i, y_i) = (1, 0) \text{ or } (0, 1).$$

So

$$\begin{aligned}
w(x + y) &= \text{number of 1's in } x \\
&\quad + \text{number of 1's in } y \\
&\quad -2 \times \text{ number of } i \text{ where } x_i = y_i = 1 \\
&= w(x) + w(y) - 2w(x \cap y).
\end{aligned}$$

6. Let $H = [c_1 \cdots c_n]$ in columns; also $Hx^T = 0$ for $x \in C$. So $Hx^T = x_1c_1 + \cdots + x_nc_n = 0$. Let $x' = [x\ x_{n+1}]$. Then, if $x \in C$, we have $x' \in C'$ when $x_1 + \cdots + x_n + x_{n+1} = 0$. So

$$\begin{aligned} H'x'^T &= \begin{bmatrix} c_1 & \cdots & c_n & z^T \\ 1 & \cdots & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \\ x_{n+1} \end{bmatrix} \\ &= \begin{bmatrix} x_1c_1+ & \cdots & +x_nc_n+ & 0 \\ x_1+ & \cdots & +x_n+ & x_{n+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \end{aligned}$$

Hence H' is a parity-check matrix for C'.

7. Let $H = [h_1, \ldots, h_r]^{\mathrm{T}}$ be a parity-check matrix of $C = \mathrm{Ham}(r, 2)$ with rows $h_1, \ldots, h_r$, and let $h = \sum \lambda_i h_i$ be an element of $C^{\perp}$. If $(x_1, \ldots, x_r)^{\mathrm{T}}$ is the $j-$th column of H, then the $j-$th coordinate of h is zero if $\sum \lambda_i x_i = 0$. However, the number of non-zero solutions $(x_1, \ldots, x_r)$ of $\sum \lambda_i x_i = 0$ is the number N of elements of $V(r, 2)\backslash\{0\}$ in a subspace of dimension $r - 1$. Hence $N = 2^{r-1} - 1$. So

$$\begin{aligned} w(h) = n - N &= (2^r - 1) - (2^{r-1} - 1) \\ &= 2^r - 2^{r-1} = 2^{r-1}. \end{aligned}$$