S-72.341 CODING METHODS

Tutorial 7, Solutions

1. The rows of the generator matrix are given in Example 7-3 (Figure 7-1). The parity-check matrix is the generator matrix of the dual code of $\Re(2,4)$, i.e. $\Re(1,4)$. This is a subcode of $\Re(2,4)$ (see problem 4.2). The generator matrix of $\Re(1,4)$ consists of the first five rows of Figure 7-1, that is

$$\mathbf{H}_{\Re(2,4)} = \mathbf{G}_{\Re(1,4)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

2. This problem is about basic properties of RM codes.

   a) Dimension $k = 1 + \binom{5}{1} + \binom{5}{2} = 16$. See equation (7-2).

   b) Rate of the code is $\frac{16}{32} = \frac{1}{2}$.

   c) $d_{\min} = 2^3 = 8$. $t = \left\lfloor \frac{8-1}{2} \right\rfloor = 3$. See Theorem 7-2.

   d) This part has nothing to do with RM codes, but it reminds us of the basic principles of decoding of block codes (chapter 4 in the book).

   Since probability of a bit error is 0.5, all 32-tuples are equally probable at the receiver. Thus, we need to calculate the probability of the received vector being within a Hamming sphere of a wrong code word. There are $2^{16} - 1$ wrong code words. Hamming spheres of radius 3 have volume

$$V_2(32,3) = \sum_{j=0}^{3} \binom{32}{j} = 5489.$$

   Probability of *decoding error* is

$$P_{dc} = \frac{\left(2^{16} - 1\right) \cdot 5489}{2^{32}} \approx 0.084.$$

The probability of *decoding failure* is

$$P_{df} = \frac{2^{32} - 2^{16} \cdot 5489}{2^{32}} \approx 0.916 .$$

Note: For a bounded-distance decoder there is a difference between decoder error and decoder failure, see page 74 of the book.

The probability that a code word is decoded correctly is only $5489/2^{32} \approx 1.3 \cdot 10^{-6}$. In this case "decoding" is perhaps not a very meaningful term, since all 32-tuples are equally probably.

3. A $\Re(m-1,m)$ code has a dual code $\Re(0,m)$. Generator matrix of the $\Re(0,m)$ code (a row vector of ones) is the parity-check matrix $\mathbf{H}$ of the $\Re(m-1,m)$ code. The condition

$$\mathbf{c}^T\mathbf{H} = \mathbf{c}^T \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}^T}_{\text{even \# of ones}} = 0$$

must be satisfied all code words $\mathbf{c}$. This means that all 2^{2^m-1} code words must have even weight. Thus, the code constitutes all even-weight 2^m-tuples.

4. We need to compute the checksums for message bit estimates m_1, m_2, m_3, and m_4. The algorithm for doing this is described on pp. 160-161 of the course book. Here computation for obtaining the checksums for m_1 is shown. Others follow similarly.

   i. The incidence vector is $\mathbf{v}_1 = 0101010101010101$, see Example 7-3. The subspace associated with $\mathbf{v}_1$ is

   $$\begin{aligned} S &= \{P_1, P_3, P_5, P_7, P_9, P_{11}, P_{13}, P_{15}\} \\ &= \{(1110),(1100),(1010),(1000),(0110),(0100),(0010),(0000)\}. \end{aligned}$$

   Table 7-2 on page 161 can be used to obtain the 4-tuples.

   ii. The complementary subspace of S can be found by examining the incidence vector $\mathbf{v}_2\mathbf{v}_3\mathbf{v}_4 = 0000000000000011$. This results in

   $$T = \{P_{14}, P_{15}\} = \{(0001),(0000)\}.$$

   iii. The first checksum is $m_1^1 = c_{14} + c_{15}$.

iv. The translation of T wrt $P_1 = (1110)$ is $\{(1111),(1110)\} = \{P_0, P_1\}$. Notice that all translations result in the original point in the subspace S and a point whose index is lowered by 1. Thus, the remaining translations are $\{P_3, P_2\}$, $\{P_5, P_4\}$, $\{P_7, P_6\}$, $\{P_9, P_8\}$, $\{P_{11}, P_{10}\}$, $\{P_{13}, P_{12}\}$, and $\{P_{15}, P_{14}\}$. For message bit m_1 the orthogonal checksums m_1^i, $i = 1,2,...,8$, are

$$
\begin{aligned}
m_1^1 &= c_{14} + c_{15} \\
m_1^2 &= c_{12} + c_{13} \\
m_1^3 &= c_{10} + c_{11} \\
m_1^4 &= c_8 + c_9 \\
m_1^5 &= c_6 + c_7 \\
m_1^6 &= c_4 + c_5 \\
m_1^7 &= c_2 + c_3 \\
m_1^8 &= c_0 + c_1
\end{aligned}
$$

Similarly for the other message bits we obtain

$$
\begin{aligned}
m_2^1 &= c_{13} + c_{15} & m_3^1 &= c_{11} + c_{15} & m_4^1 &= c_7 + c_{15} \\
m_2^2 &= c_{12} + c_{14} & m_3^2 &= c_{10} + c_{14} & m_4^2 &= c_6 + c_{14} \\
m_2^3 &= c_9 + c_{11} & m_3^3 &= c_9 + c_{13} & m_4^3 &= c_5 + c_{13} \\
m_2^4 &= c_8 + c_{10} & m_3^4 &= c_8 + c_{12} & m_4^4 &= c_4 + c_{12} \\
m_2^5 &= c_5 + c_7 & m_3^5 &= c_3 + c_7 & m_4^5 &= c_3 + c_{11} \\
m_2^6 &= c_4 + c_6 & m_3^6 &= c_2 + c_6 & m_4^6 &= c_2 + c_{10} \\
m_2^7 &= c_1 + c_3 & m_3^7 &= c_1 + c_5 & m_4^7 &= c_1 + c_9 \\
m_2^8 &= c_0 + c_2 & m_3^8 &= c_0 + c_4 & m_4^8 &= c_0 + c_8.
\end{aligned}
$$

5. The Reed decoding algorithm is explained in the course book, starting from page 155. In the following we decode the first 16-tuple, and give only answer to the remaining three.

   Before the actual decoding we must find the checksums for each message bit. Checksums for 2nd order message bits m_{12}, m_{13}, m_{34} are given in equations (7-8) and (7-9) of the book. To obtain checksums for m_{14}, m_{24}, and m_{34} we examine the tesseracts in Figures 7-3a and 7-3b.

Checksums for m_{14}: Using the lower left tesseract in Figure 7-3a we identify the following complementary subspaces:

$$\begin{aligned}
T_{14}^1 &= \{(0000),(0001),(1001),(1000)\} = \{P_0, P_1, P_9, P_8\} \\
T_{14}^2 &= \{(0010),(1010),(1011),(0011)\} = \{P_2, P_{10}, P_{11}, P_3\} \\
T_{14}^3 &= \{(0100),(0101),(1101),(1100)\} = \{P_4, P_5, P_{13}, P_{12}\} \\
T_{14}^4 &= \{(0110),(1110),(0111),(1111)\} = \{P_6, P_{14}, P_7, P_{15}\}.
\end{aligned}$$

The checksums are:

$$\begin{aligned}
m_{14}^1 &= c_0 + c_1 + c_8 + c_9 \\
m_{14}^2 &= c_2 + c_3 + c_{10} + c_{11} \\
m_{14}^3 &= c_4 + c_5 + c_{12} + c_{13} \\
m_{14}^4 &= c_6 + c_7 + c_{14} + c_{15}.
\end{aligned}$$

Checksums for m_{24}: Using the middle tesseract in Figure 7-3a we identify the following complementary subspaces:

$$\begin{aligned}
T_{24}^1 &= \{(0000),(1000),(1010),(0010)\} = \{P_0, P_8, P_{10}, P_2\} \\
T_{24}^2 &= \{(0001),(1001),(1011),(0011)\} = \{P_1, P_9, P_{11}, P_3\} \\
T_{24}^3 &= \{(0101),(0111),(1111),(1101)\} = \{P_5, P_7, P_{15}, P_{13}\} \\
T_{24}^4 &= \{(0110),(1110),(1100),(0100)\} = \{P_6, P_{14}, P_{12}, P_4\}.
\end{aligned}$$

The checksums are:

$$\begin{aligned}
m_{24}^1 &= c_0 + c_2 + c_8 + c_{10} \\
m_{24}^2 &= c_1 + c_3 + c_9 + c_{11} \\
m_{24}^3 &= c_5 + c_7 + c_{13} + c_{15} \\
m_{24}^4 &= c_4 + c_6 + c_{12} + c_{14}.
\end{aligned}$$

Checksums for m_{23}: Using the uppermost tesseract in Figure 7-3b we identify the following complementary subspaces:

$$\begin{aligned}
T_{23}^1 &= \{(0000),(0010),(0100),(0110)\} = \{P_0, P_2, P_4, P_6\} \\
T_{23}^2 &= \{(0001),(0011),(0111),(0101)\} = \{P_1, P_3, P_7, P_5\} \\
T_{23}^3 &= \{(1001),(1101),(1011),(1111)\} = \{P_9, P_{13}, P_{11}, P_{15}\} \\
T_{23}^4 &= \{(1000),(1010),(1100),(1110)\} = \{P_8, P_{10}, P_{12}, P_{14}\}.
\end{aligned}$$

The checksums are:

$$
\begin{aligned}
m_{23}^{1} &= c_0 + c_2 + c_4 + c_6 \\
m_{23}^{2} &= c_1 + c_3 + c_5 + c_7 \\
m_{23}^{3} &= c_9 + c_{11} + c_{13} + c_{15} \\
m_{23}^{4} &= c_8 + c_{10} + c_{12} + c_{14}.
\end{aligned}
$$

The checksums for the 1st order terms were calculated in problem 4.

a) First we compute estimates for second order message bits by substitution $c_i \to r_i$, $i = 0,1,2,...,15$ in the checksums. The received word is

$$
\mathbf{r} = \underset{r_0}{0}\ \underset{r_1}{0}\ \underset{r_2}{1}\ \underset{r_3}{1}\ \underset{r_4}{0}\ \underset{r_5}{1}\ \underset{r_6}{1}\ \underset{r_7}{1}\ \underset{r_8}{0}\ \underset{r_9}{0}\ \underset{r_{10}}{0}\ \underset{r_{11}}{1}\ \underset{r_{12}}{0}\ \underset{r_{13}}{1}\ \underset{r_{14}}{1}\ \underset{r_{15}}{1}
$$

Here we go:

$$
\begin{aligned}
\hat{m}_{12}^{1} &= r_0 + r_1 + r_2 + r_3 = 0 + 0 + 1 + 1 = 0 \\
\hat{m}_{12}^{2} &= r_4 + r_5 + r_6 + r_7 = 0 + 1 + 1 + 1 = 1 \\
\hat{m}_{12}^{3} &= r_8 + r_9 + r_{10} + r_{11} = 0 + 0 + 0 + 1 = 1 \\
\hat{m}_{12}^{4} &= r_{12} + r_{13} + r_{14} + r_{15} = 0 + 1 + 1 + 1 = 1
\end{aligned}
$$

$$
\begin{aligned}
\hat{m}_{13}^{1} &= r_0 + r_1 + r_4 + r_5 = 1 \\
\hat{m}_{13}^{2} &= r_2 + r_3 + r_6 + r_7 = 0 \\
\hat{m}_{13}^{3} &= r_8 + r_9 + r_{12} + r_{13} = 1 \\
\hat{m}_{13}^{4} &= r_{10} + r_{11} + r_{14} + r_{15} = 1
\end{aligned}
$$

$$
\begin{aligned}
\hat{m}_{14}^{1} &= r_0 + r_1 + r_8 + r_9 = 0 \\
\hat{m}_{14}^{2} &= r_2 + r_3 + r_{10} + r_{11} = 1 \\
\hat{m}_{14}^{3} &= r_4 + r_5 + r_{12} + r_{13} = 0 \\
\hat{m}_{14}^{4} &= r_6 + r_7 + r_{14} + r_{15} = 0
\end{aligned}
$$

$$
\begin{aligned}
\hat{m}_{23}^{1} &= r_0 + r_2 + r_4 + r_6 = 0 \\
\hat{m}_{23}^{2} &= r_1 + r_3 + r_5 + r_7 = 1 \\
\hat{m}_{23}^{3} &= r_9 + r_{11} + r_{13} + r_{15} = 1 \\
\hat{m}_{23}^{4} &= r_8 + r_{10} + r_{12} + r_{14} = 1
\end{aligned}
$$

$$\hat{m}_{24}^{1} = r_0 + r_2 + r_8 + r_{10} = 1$$
$$\hat{m}_{24}^{2} = r_1 + r_3 + r_9 + r_{11} = 0$$
$$\hat{m}_{24}^{3} = r_5 + r_7 + r_{13} + r_{15} = 0$$
$$\hat{m}_{24}^{4} = r_4 + r_6 + r_{12} + r_{14} = 0$$

$$\hat{m}_{34}^{1} = r_0 + r_4 + r_8 + r_{12} = 0$$
$$\hat{m}_{34}^{2} = r_1 + r_5 + r_9 + r_{13} = 0$$
$$\hat{m}_{34}^{3} = r_2 + r_6 + r_{10} + r_{14} = 1$$
$$\hat{m}_{34}^{4} = r_3 + r_7 + r_{11} + r_{15} = 0$$

Next we estimate the message bits based on majority vote:

$$\hat{m}_{12} = \text{maj}\{0,1,1,1\} = 1$$
$$\hat{m}_{13} = \text{maj}\{1,0,1,1\} = 1$$
$$\hat{m}_{14} = \text{maj}\{0,1,0,0\} = 0$$
$$\hat{m}_{23} = \text{maj}\{0,1,1,1\} = 1$$
$$\hat{m}_{24} = \text{maj}\{1,0,0,0\} = 0$$
$$\hat{m}_{34} = \text{maj}\{0,0,1,0\} = 0.$$

Estimated second order message bits of the message word $\mathbf{m} = \left[\mathbf{m}_0 \mid \mathbf{m}_1 \mid \mathbf{m}_2\right]$ are

$$\begin{aligned}\hat{\mathbf{m}}_2 &= \left[\hat{m}_{34} \quad \hat{m}_{24} \quad \hat{m}_{14} \quad \hat{m}_{23} \quad \hat{m}_{13} \quad \hat{m}_{12}\right] \\ &= \left[0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1\right].\end{aligned}$$

The effect of the 2nd order terms is removed from the received word:

$$\mathbf{r}' = \mathbf{r} - \hat{\mathbf{m}}_2\mathbf{G}_2\,.$$

The generator matrix is given in Figure 7-1. We get

$$\mathbf{r}' = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} -$$
$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{array}{r} \begin{array}{cccccccccccccccc} 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \\ - \begin{array}{cccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \\ \hline \begin{array}{cccccccccccccccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \end{array}.$$

First order terms are obtained as

$$\begin{aligned} \hat{m}_1^1 &= r'_{14} + r'_{15} = 0 \\ \hat{m}_1^2 &= r'_{12} + r'_{13} = 0 \\ \hat{m}_1^3 &= r'_{10} + r'_{11} = 0 \\ \hat{m}_1^4 &= r'_{8} + r'_{9} = 0 \\ \hat{m}_1^5 &= r'_{6} + r'_{7} = 0 \\ \hat{m}_1^6 &= r'_{4} + r'_{5} = 0 \\ \hat{m}_1^7 &= r'_{2} + r'_{3} = 1 \\ \hat{m}_1^8 &= r'_{0} + r'_{1} = 0 \end{aligned}$$

$$\begin{aligned} \hat{m}_2^1 &= r'_{13} + r'_{15} = 0 \\ \hat{m}_2^2 &= r'_{12} + r'_{14} = 0 \\ \hat{m}_2^3 &= r'_{9} + r'_{11} = 0 \\ \hat{m}_2^4 &= r'_{8} + r'_{10} = 0 \\ \hat{m}_2^5 &= r'_{5} + r'_{7} = 0 \\ \hat{m}_2^6 &= r'_{4} + r'_{6} = 0 \\ \hat{m}_2^7 &= r'_{1} + r'_{3} = 0 \\ \hat{m}_2^8 &= r'_{0} + r'_{2} = 1 \end{aligned}$$

... and so on. Since $\mathbf{r}'$ has weight one and all first order estimates are sums of two distinct received coordinates, all first order message bit estimates become zero under majority-vote decoding i.e. $\hat{m}_i = 0$, $i = 1,2,3,4$. Thus,

$$\mathbf{r}'' = \mathbf{r}' - \underbrace{\hat{\mathbf{m}}_1 \mathbf{G}_1}_{=\mathbf{0}} = \mathbf{r}'.$$

The estimate for the message bit m_0 is

$$\hat{m}_0 = \text{maj}\left\{ r_0'', r_1'', \ldots, r_{15}'' \right\} = 0.$$

The decoded message is

$$\begin{aligned} \hat{\mathbf{m}} &= \begin{bmatrix} \hat{m}_0 & \hat{m}_4 & \hat{m}_3 & \hat{m}_2 & \hat{m}_1 & \hat{m}_{34} & \hat{m}_{24} & \hat{m}_{14} & \hat{m}_{23} & \hat{m}_{13} & \hat{m}_{12} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \end{aligned}$$

b) $\hat{\mathbf{m}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$.

c) Decoder failure: $\hat{\mathbf{m}}_{34} = \text{maj}\{1,0,0,1\}$.

d) $\hat{\mathbf{m}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$.