Chapter 4

4.1 A parity-check matrix for the $(15, 11)$ Hamming code is

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Let $\boldsymbol{r} = (r_0, r_1, \ldots, r_{14})$ be the received vector. The syndrome of $\boldsymbol{r}$ is (s_0, s_1, s_2, s_3) with

$$\begin{aligned} s_0 &= r_0 + r_4 + r_7 + r_8 + r_{10} + r_{12} + r_{13} + r_{14}, \\ s_1 &= r_1 + r_4 + r_5 + r_9 + r_{10} + r_{11} + r_{13} + r_{14}, \\ s_2 &= r_2 + r_5 + r_6 + r_8 + r_{10} + r_{11} + r_{12} + r_{14}, \\ s_3 &= r_3 + r_6 + r_7 + r_9 + r_{11} + r_{12} + r_{13} + r_{14}. \end{aligned}$$

Set up the decoding table as Table 4.1. From the decoding table, we find that

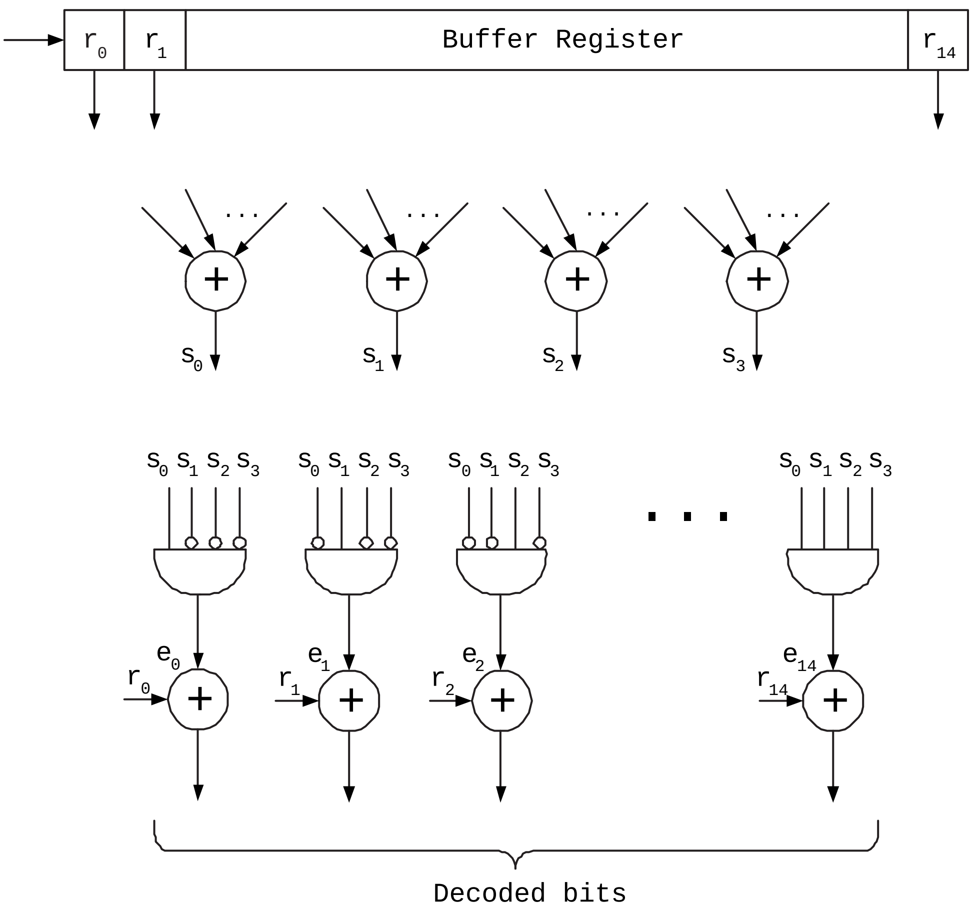
$$e_0 = s_0\bar{s}_1\bar{s}_2\bar{s}_3,\ e_1 = \bar{s}_0 s_1\bar{s}_2\bar{s}_3,\ e_2 = \bar{s}_0\bar{s}_1 s_2\bar{s}_3,$$

$$e_3 = \bar{s}_0\bar{s}_1\bar{s}_2 s_3,\ e_4 = s_0 s_1\bar{s}_2\bar{s}_3,\ e_5 = \bar{s}_0 s_1 s_2\bar{s}_3,$$

$$\ldots,\ e_{13} = s_0 s_1\bar{s}_2 s_3,\ e_{14} = s_0 s_1 s_2 s_3.$$

Table 4.1: Decoding Table

s_0	s_1	s_2	s_3	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1



4.3 From (4.3), the probability of an undetected error for a Hamming code is

$$P_u(E) = 2^{-m}\{1 + (2^m - 1)(1-2p)^{2^{m-1}}\} - (1-p)^{2^m-1}$$

$$= 2^{-m} + (1-2^{-m})(1-2p)^{2^{m-1}} - (1-p)^{2^m-1}. \qquad (1)$$

Note that

$$(1-p)^2 \geq 1-2p, \qquad (2)$$

and

$$(1-2^{-m}) \geq 0. \qquad (3)$$

Using (2) and (3) in (1), we obtain the following inequality:

$$P_u(E) \leq 2^{-m} + (1-2^{-m})\left[(1-p)^2\right]^{2^{m-1}} - (1-p)^{2^m-1}$$

$$= 2^{-m} + (1-p)^{2^m-1}\{(1-2^{-m})(1-p) - 1\}$$

$$= 2^{-m} - (1-p)^{2^m-1}\{(1-(1-p)(1-2^{-m})\}. \qquad (4)$$

Note that $0 \leq 1-p \leq 1$ and $0 \leq 1-2^{-m} < 1$. Clearly $0 \leq (1-p)\cdot(1-2^{-m}) < 1$, and

$$1-(1-p)\cdot(1-2^{-m}) \geq 0. \qquad (5)$$

Since $(1-p)^{2^m-1} \geq 0$, it follows from (4) and (5) that $P_u(E) \leq 2^{-m}$.

4.6 The generator matrix for the 1st-order RM code RM(1,3) is

$$\mathbf{G} = \begin{bmatrix} \mathbf{v}_0 \\ \mathbf{v}_3 \\ \mathbf{v}_2 \\ \mathbf{v}_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \qquad (1)$$

The code generated by this matrix is a $(8,4)$ code with minimum distance 4. Let (a_0, a_3, a_2, a_1)

be the message to be encoded. Then its corresponding codeword is

$$\mathbf{b} = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)$$

$$= a_0\mathbf{v}_0 + a_3\mathbf{v}_3 + a_2\mathbf{v}_2 + a_1\mathbf{v}_1. \quad (2)$$

From (1) and (2), we find that

$$b_0 = a_0, b_1 = a_0 + a_1, b_2 = a_0 + a_2, b_3 = a_0 + a_2 + a_1,$$

$$b_4 = a_0 + a_3, b_5 = a_0 + a_3 + a_1, b_6 = a_0 + a_3 + a_2,$$

$$b_7 = a_0 + a_3 + a_2 + a_1. \quad (3)$$

From (3), we find that

$$a_1 = b_0 + b_1 = b_2 + b_3 = b_4 + b_5 = b_6 + b_7,$$

$$a_2 = b_0 + b_2 = b_1 + b_3 = b_4 + b_6 = b_5 + b_7,$$

$$a_3 = b_0 + b_4 = b_1 + b_5 = b_2 + b_6 = b_3 + b_7,$$

$$a_0 = b_0 = b_1 + a_1 = b_2 + a_2 = b_3 + a_2 + a_1 = b_4 + a_3$$

$$= b_5 + a_3 + a_1 = b_6 + a_3 + a_2 = b_7 + a_3 + a_2 + a_1.$$

Let $\mathbf{r} = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7)$ be the received vector. The check-sum for decoding a_1, a_2 and a_3 are:

(a_1)	(a_2)	(a_3)
$A_1^{(0)} = r_0 + r_1$	$B_1^{(0)} = r_0 + r_2$	$C_1^{(0)} = r_0 + r_4$
$A_2^{(0)} = r_2 + r_3$	$B_2^{(0)} = r_1 + r_3$	$C_2^{(0)} = r_1 + r_5$
$A_3^{(0)} = r_4 + r_5$	$B_3^{(0)} = r_4 + r_6$	$C_3^{(0)} = r_2 + r_6$
$A_4^{(0)} = r_6 + r_7$	$B_4^{(0)} = r_5 + r_7$	$C_4^{(0)} = r_3 + r_7$

After decoding a_1, a_2 and a_3, we form

$$\begin{aligned}\mathbf{r}^{(1)} &= \mathbf{r} - a_1\mathbf{v}_1 - a_2\mathbf{v}_2 - a_3\mathbf{v}_3 \\ &= (r_0^{(1)}, r_1^{(1)}, r_2^{(1)}, r_3^{(1)}, r_4^{(1)}, r_5^{(1)}, r_6^{(1)}, r_7^{(1)}).\end{aligned}$$

Then a_0 is equal to the value taken by the majority of the bits in $\mathbf{r}^{(1)}$.

For decoding (01000101), the four check-sum for decoding a_1, a_2 and a_3 are:

(1) $A_1^{(0)} = 1$, $A_2^{(0)} = 0$, $A_3^{(0)} = 1$, $A_4^{(0)} = 1$;

(2) $B_1^{(0)} = 0$, $B_2^{(0)} = 1$, $B_3^{(0)} = 0$, $B_4^{(0)} = 0$;

(3) $C_1^{(0)} = 0$, $C_2^{(0)} = 0$, $C_3^{(0)} = 0$, $C_4^{(0)} = 1$.

Based on these check-sums, a_1, a_2 and a_3 are decoded as 1, 0 and 0, respectively.

To decode a_0, we form

$$\begin{aligned}\mathbf{r}^{(1)} &= (01000101) - a_1\mathbf{v}_1 - a_2\mathbf{v}_2 - a_3\mathbf{v}_3 \\ &= (00010000).\end{aligned}$$

From the bits of $\mathbf{r}^{(1)}$, we decode a_0 to 0. Therefore, the decoded message is (0001).

4.14

$$\begin{aligned}RM(1,3) = \{ \; & 0, 1, X_1, X_2, X_3, 1 + X_1, 1 + X_2, \\ & 1 + X_3, X_1 + X_2, X_1 + X_3, X_2 + X_3, \\ & 1 + X_1 + X_2, 1 + X_1 + X_3, 1 + X_2 + X_3, \\ & X_1 + X_2 + X_3, 1 + X_1 + X_2 + X_3\}.\end{aligned}$$

4.15 The RM$(r, m-1)$ and RM$(r-1, m-1)$ codes are given as follows (from (4.38)):

$$\begin{aligned}RM(r, m-1) &= \{\mathbf{v}(f) : f(X_1, X_2, \ldots, X_{m-1}) \in \mathcal{P}(r, m-1)\}, \\ RM(r-1, m-1) &= \{\mathbf{v}(g) : g(X_1, X_2, \ldots, X_{m-1}) \in \mathcal{P}(r-1, m-1)\}.\end{aligned}$$

Then

$$\text{RM}(r,m)=\{\mathbf{v}(h) : h = f(X_1, X_2, \ldots, X_{m-1}) + X_m g(X_1, X_2, \ldots, X_{m-1}) \text{ with } f \in \mathcal{P}(r, m-1) \text{ and } g \in \mathcal{P}(r-1, m-1)\}.$$

4.20 a

$$s = (001110001001)$$

$w(s) > 3$ so, we try to find a row of P, p_i such that $w(s + p_i) \leq 3$. We cannot find such p_i. Therefore we go to step five and find $s.P$.

$$s.P = (100011101110)$$

Again $w(s.P) > 3$. So, we look for a p_i such that $w(s.P + p_i) = 2$. We find that if we choose p_0, we get

$$s.P + p_0 = (100011101110) + (100011101101) = (000000000011)$$

So, $w(s.P + p_0) = 2$ and:

$$e = \left(u^{(0)}, s.P + p_i\right) = (100000000011)$$

Finally,

$$v = r + e = (001101110010000011000000)$$