TSDT16 Error-correcting codes

Solutions to the exam 2010-10-23

Danyo Danev, danyo@isy.liu.se

1

The length of the code C is the number of columns in $\mathbf{H}$ which is $n = n_1 + n_2$. The dimension of the code C is $n - (n_1 + n_2 - k) = k$.

Since the parity check matrix of C is in systematic form we can obtain the generator matrix $\mathbf{G}$ of the code C as follows.

$$\mathbf{G} = \left[\begin{array}{c|c|c|c} \mathbf{P_1} & \mathbf{I_k} & \mathbf{P_2} & \mathbf{I_k} \end{array} \right].$$

An arbitrary codeword in C can be written as

$$\mathbf{v} = \mathbf{uG} = (\mathbf{p^{(1)}}, \mathbf{u}, \mathbf{p^{(2)}}, \mathbf{u}),$$

where $\mathbf{v^{(1)}} = (\mathbf{p^{(1)}}, \mathbf{u})$ and $\mathbf{v^{(2)}} = (\mathbf{p^{(2)}}, \mathbf{u})$ are codewords in C_1 and C_2, respectively. Thus every non-zero codeword in C (corresponding to a non-zero $\mathbf{u}$) is actually a concatenation of two non-zero codewords in C_1 and C_2 after some rearrangement of the positions. We use the fact that the minimum distance of the code is the minimum Hamming weight of the non-zero codewords in this code. The observation above shows that the minimum Hamming weight of the codewords in C is at least $d_1 + d_2$ and thus for the minimum distance d of C we have $d \geq d_1 + d_2$.

2

For calculations in $\mathbf{GF}(2^4)$ generated by the primitive polynomial $1 + X + X^4$ the following table can be easily created.

Vector repr.	Polynomial repr.	Vector repr.
0	0	(0000)
1	1	(1000)
α	α	(0100)
α^2	α^2	(0010)
α^3	α^3	(0001)
α^4	$1 + \alpha$	(1100)
α^5	$\alpha + \alpha^2$	(0110)
α^6	$\alpha^2 + \alpha^3$	(0011)
α^7	$1 + \alpha + \alpha^3$	(1101)
α^8	$1 + \alpha^2$	(1010)
α^9	$\alpha + \alpha^3$	(0101)
α^{10}	$1 + \alpha + \alpha^2$	(1110)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0111)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1111)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1011)
α^{14}	$1 + \alpha^3$	(1001)

The syndrome components of the received vector $\mathbf{r} = (\alpha^6, \alpha^9, 0, \alpha^4, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, which corresponds to the polynomial $\mathbf{r}(X) = X^6 + \alpha^4 X^3 + \alpha^9 X + \alpha^6$ are

$$\begin{aligned} S_1 = \mathbf{r}(\alpha) &= \alpha^6, \\ S_2 = \mathbf{r}(\alpha^2) &= \alpha^9, \\ S_3 = \mathbf{r}(\alpha^3) &= \alpha^5, \\ S_4 = \mathbf{r}(\alpha^4) &= \alpha^{14}, \\ S_5 = \mathbf{r}(\alpha^5) &= \alpha^{10}, \\ S_6 = \mathbf{r}(\alpha^6) &= \alpha^9. \end{aligned}$$

The iterative procedure for finding the error location polynomial is shown in the following table.

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$	ρ
-1	1	1	0	-1	$-$
0	1	α^6	0	0	$-$
1	$1+\alpha^6 X$	α^8	1	0	-1
2	$1+\alpha^3 X$	α^{14}	1	1	0
3	$1+\alpha^2 X+\alpha^{12}X^2$	α^{11}	2	1	1
4	$1+\alpha^7 X+\alpha^{11}X^2$	α^{14}	2	2	2
5	$1+\alpha^4 X+\alpha^3 X^2+X^3$	1	3	2	3
6	$1+X+\alpha^{13}X^2+\alpha^{11}X^3$	$-$	3	3	4

The error location polynomial is $\sigma(X) = 1+X+\alpha^{13}X^2+\alpha^{11}X^3$. The roots of this polynomial are α^{10}, α^{11} and α^{13}. Hence the error location numbers are $\alpha^{-10} = \alpha^8$, $\alpha^{-11} = \alpha^4$ and $\alpha^{-13} = \alpha^2$.

From the syndrome components of the received polynomial and the coefficients of the error location polynomial, we find the error value evaluator,

$$\begin{aligned}\mathbf{Z}_0(X) &= S_1 + (S_2 + \sigma_1 S_1)X + (S_3 + \sigma_1 S_2 + \sigma_2 S_1)X^2 \\ &= \alpha^6 + \alpha^5 X + \alpha^{12} X^2.\end{aligned}$$

For the derivative $\sigma'(X)$ of the error location polynomial we have

$$\sigma'(X) = 1 + \alpha^{11} X^2.$$

The error values at positions X^2, X^4 and X^5 are

$$\begin{aligned}e_2 &= -\frac{\mathbf{Z}_0(\alpha^{-2})}{\sigma'(\alpha^{-2})} = \alpha^6, \\ e_4 &= -\frac{\mathbf{Z}_0(\alpha^{-4})}{\sigma'(\alpha^{-4})} = \alpha^{14}, \\ e_5 &= -\frac{\mathbf{Z}_0(\alpha^{-5})}{\sigma'(\alpha^{-5})} = \alpha^{10}.\end{aligned}$$

Consequently, the error pattern is

$$\mathbf{e}(X) = \alpha^6 X^2 + \alpha^{14} X^4 + \alpha^{10} X^5$$

and the decoded codeword polynomial is

$$\begin{aligned}&\mathbf{c}(X) = \mathbf{r}(X) - \mathbf{e}(X) = \\ &\quad X^6 + \alpha^{10}X^5 + \alpha^{14}X^4 + \alpha^4 X^3 + \alpha^6 X^2 + \alpha^9 X + \alpha^6,\end{aligned}$$

which corresponds to the codeword

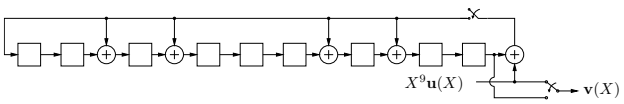
$$\mathbf{c} = (\alpha^6, \alpha^9, \alpha^6, \alpha^4, \alpha^{14}, \alpha^{10}, 1, 0, 0, 0, 0, 0, 0, 0, 0).$$

3

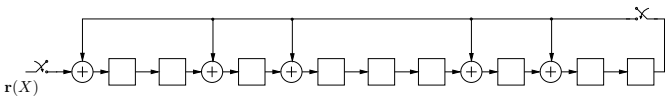
First we have to calculate the generator polynomial $\mathbf{g}(X)$. Since the code is binary and its length is 15 this polynomialis obtained as

$$\mathbf{g}(X) = \frac{X^{15}+1}{\mathbf{h}(X)} = X^9 + X^7 + X^6 + X^3 + X^2 + 1.$$

The encoding circuit as given in Figure 5.1 (page 147 in Lin-Costello) is in this case as follows.



The syndrom computation circuit as given in Figure 5.5 (page 150 in Lin-Costello) is in this case as follows.



The received vector $\mathbf{r}$ corresponding to the received polynomial $\mathbf{r}(X) = 1 + X^6 + X^{10}$ is

$$\mathbf{r} = (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0).$$

The contents of the syndrom calculation shift register af-

ter each step are as follows

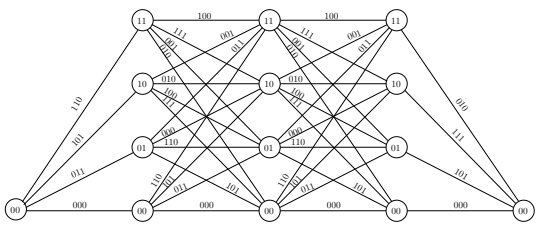
i	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	1	0	0	0	0	0	0	0	0
6	0	1	0	0	0	0	0	0	0
7	0	0	1	0	0	0	0	0	0
8	0	0	0	1	0	0	0	0	0
9	1	0	0	0	1	0	0	0	0
10	0	1	0	0	0	1	0	0	0
11	0	0	1	0	0	0	1	0	0
12	0	0	0	1	0	0	0	1	0
13	0	0	0	0	1	0	0	0	1
14	1	0	1	1	0	1	1	1	0
15	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**1**

This shows that the syndrom polynomial $\mathbf{s}(X)$ of the received polynomial $\mathbf{r}(X)$ is

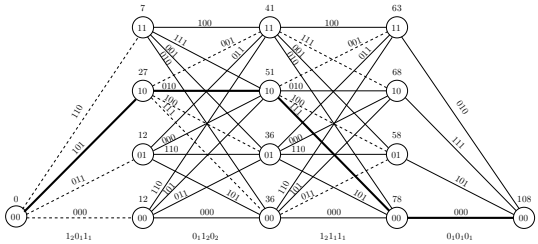
$$\mathbf{s}(X) = X^8 + X^7 + X^6 + X^4 + X^3 + X + 1.$$

4

The trellis for the rate 2/3 convolutional code used is given in the following figure.



The path that maximizes the path-metric is given in the figure below. The metric value and the surviving path for the corresponding node are also given. The received vector is given at the bottom of the figure.



Thus the maximum-likelihood message is $\mathbf{m} = (10, 10, 00)$.

5

a) We know that the dual $C^\perp$ of the Hamming code C is the simplex code of length 15. Thus the weight enumerator of $C^\perp$ is

$$B(z) = 1 + 15z^8.$$

Using the MacWilliams identity (3.32) we obtain the weight enumerator of C as

$$\begin{aligned} A(z) &= 2^{-(n-k)}(1+z)^n B\left(\frac{1-z}{1+z}\right) \\ &= 2^{-4}(1+z)^{15}\left(1 + 15\frac{(1-z)^8}{(1+z)^8}\right) \\ &= 2^{-4}((1+z)^{15} + 15(1-z)^8(1+z)^7) \\ &= z^{15} + 35z^{12} + 105z^{11} + 168z^{10} \\ &+ 280z^9 + 435z^8 + 435z^7 + 280z^6 \\ &+ 168z^5 + 105z^4 + 35z^3 + 1. \end{aligned}$$

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

$$\begin{aligned} P_u(E) &= 2^{-m}\left\{1 + (2^m - 1)(1-2p)^{2^{m-1}}\right\} - (1-p)^{2^m - 1} \\ &= 2^{-4}\left\{1 + (2^4 - 1)(1-2p)^8\right\} - (1-p)^{15} \\ &= 2^{-4}\left\{1 + 15 \cdot 0.8^8\right\} - 0.9^{15} \\ &\approx 0.013895. \end{aligned}$$