TSDT16 Error-correcting codes

Solutions to the exam 2014-10-31

Danyo Danev, danyo@isy.liu.se

1

For calculations in $\mathbf{GF}(2^4)$ generated by the primitive polynomial $1+X^3+X^4$ 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	$1+\alpha^3$	(1001)
α^5	$1+\alpha+\alpha^3$	(1101)
α^6	$1+\alpha+\alpha^2+\alpha^3$	(1111)
α^7	$1+\alpha+\alpha^2$	(1110)
α^8	$\alpha+\alpha^2+\alpha^3$	(0111)
α^9	$1+\alpha^2$	(1010)
α^{10}	$\alpha+\alpha^3$	(0101)
α^{11}	$1+\alpha^2+\alpha^3$	(1011)
α^{12}	$1+\alpha$	(1100)
α^{13}	$\alpha+\alpha^2$	(0110)
α^{14}	$\alpha^2+\alpha^3$	(0011)

The syndrome components of the received vector $\mathbf{r} = (0,0,0,0,0,0,\alpha^{10},0,\alpha^4,0,1,0,0,0,0)$, which corresponds to the polynomial $\mathbf{r}(X) = \alpha^{10}X^6 + \alpha^4X^8 + X^{10}$ are

$$\begin{aligned}
S_1 = \mathbf{r}(\alpha) &= \alpha^{16}+\alpha^{12}+\alpha^{10} = \alpha+\alpha^{12}+\alpha^{10} = \alpha^5,\\
S_2 = \mathbf{r}(\alpha^2) &= \alpha^{22}+\alpha^{20}+\alpha^{20} = \alpha^7,\\
S_3 = \mathbf{r}(\alpha^3) &= \alpha^{28}+\alpha^{28}+\alpha^{30} = 1,\\
S_4 = \mathbf{r}(\alpha^4) &= \alpha^{34}+\alpha^{36}+\alpha^{40} = \alpha^4+\alpha^6+\alpha^{10} = \alpha^{14}.
\end{aligned}$$

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^5	0	0	–
1	$1+\alpha^5X$	α^{11}	1	0	-1
2	$1+\alpha^2X$	α^2	1	1	0
3	$1+\alpha^2X+\alpha^{12}X^2$	1	2	1	0
4	$1+\alpha X+\alpha X^2$	–	2	2	2

The error location polynomial is $\sigma(X) = 1+\alpha X+\alpha X^2$. The roots of this polynomial are α^6 and α^8. Hence the error location numbers are $\alpha^{-6}=\alpha^9$ and $\alpha^{-8}=\alpha^7$.

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

$$\begin{aligned}
\mathbf{Z}_0(X) &= S_1 + (S_2+\sigma_1S_1)X\\
&= \alpha^5 + (\alpha^7+\alpha\alpha^5)X\\
&= \alpha^5+\alpha^3X.
\end{aligned}$$

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

$$\sigma'(X) = \alpha.$$

The error values at positions X^7 and X^9 are

$$\begin{aligned}
e_7 &= -\frac{\mathbf{Z}_0(\alpha^{-7})}{\sigma'(\alpha^{-7})} = -\frac{\alpha^5+\alpha^{11}}{\alpha} = \alpha^{12},\\
e_9 &= -\frac{\mathbf{Z}_0(\alpha^{-9})}{\sigma'(\alpha^{-9})} = -\frac{\alpha^5+\alpha^9}{\alpha} = \alpha^7.
\end{aligned}$$

Consequently, the error pattern is

$$\mathbf{e}(X) = \alpha^7X^9 + \alpha^{12}X^7$$

and the decoded codeword polynomial is

$$\begin{aligned}\mathbf{c}(X) &= \mathbf{r}(X) - \mathbf{e}(X)\\ &= X^{10} + \alpha^7 X^9 + \alpha^4 X^8 + \alpha^{12} X^7 + \alpha^{10} X^6,\end{aligned}$$

which corresponds to the codeword

$$\mathbf{c} = (0,0,0,0,0,0,\alpha^{10},\alpha^{12},\alpha^4,\alpha^7,1,0,0,0,0).$$

2

Every codeword $\mathbf{c}(X)$ in the code C_i is a multiple of the generator polynomial $\mathbf{g_i}(X)$ for $i = 1, 2$. Thus the elements of $C = C_1 \cap C_2$ are those $\mathbf{c}(X)$ that are multiples of $\mathbf{g_1}(X)$ and $\mathbf{g_2}(X)$. These are only the polynomials $\mathbf{c}(X)$ that are multiples of $\mathbf{g}(X) = \mathrm{GCD}(\mathbf{g_1}(X), \mathbf{g_2}(X))$. Thus C is a binary linear cyclic code with generator polynomial $\mathbf{g}(X) = \mathrm{GCD}(\mathbf{g_1}(X), \mathbf{g_2}(X)) = X + 1$. The dimension of this code is $k = n - \deg \mathbf{g}(X) = 15 - 1 = 14$ and the minimum distance is $d = 2$.

3

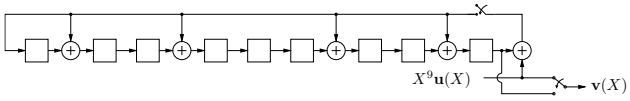
a) We calculate the parity-check polynomial $\mathbf{h}(X)$ to be

$$\mathbf{h}(X) = \frac{X^{17}+1}{\mathbf{g}(X)} = X^8 + X^7 + X^6 + X^4 + X^2 + X + 1,$$

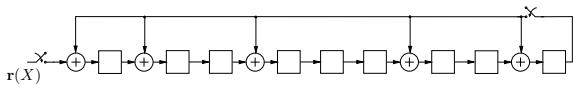
since the code is binary and its length is 17.

obtained as

b) 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.



c) We can use the encoding circuit from b) to obtain the generator matrix G of the code C in systematic form. This generator matrix is

$$G = \begin{bmatrix}
1&1&0&1&0&0&1&0&1&1&0&0&0&0&0&0&0\\
1&0&1&1&1&0&1&1&1&0&1&0&0&0&0&0&0\\
1&0&0&0&1&1&1&1&0&0&0&1&0&0&0&0&0\\
0&1&0&0&0&1&1&1&1&0&0&0&1&0&0&0&0\\
1&1&1&1&0&0&0&1&0&0&0&0&0&1&0&0&0\\
0&1&1&1&1&0&0&0&1&0&0&0&0&0&1&0&0\\
1&1&1&0&1&1&1&0&1&0&0&0&0&0&0&1&0\\
1&0&1&0&0&1&0&1&1&0&0&0&0&0&0&0&1
\end{bmatrix}.$$

The parity-check matrix H is directly obtained from the generator matrix above as

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

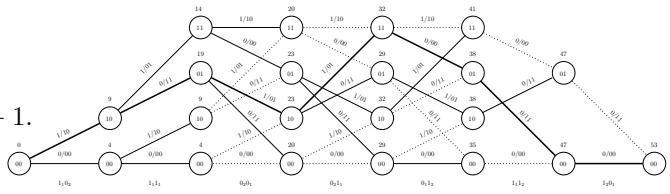
4

$n = 26 = 3^3 - 1$. The roots of the generator polynomial lie in the extension field $\mathbf{GF}(27)$, which can be generated with the help of the primitive polynomial $\mathbf{p}(X) = X^3 + 2X + 1 \in \mathbf{GF}(3)[X]$. The cyclotomic cosets are:

$$\begin{aligned}
C_0 &= \{0\}, && \leftrightarrow \quad \mathbf{m_0}(X) = X - 1 = X + 2,\\
C_1 &= \{1,3,9\}, && \leftrightarrow \quad \mathbf{m_1}(X) = X^3 + 2X + 1,\\
C_2 &= \{2,6,18\}, && \leftrightarrow \quad \mathbf{m_2}(X) = (X - \theta^2)(X - \theta^6)(X - \theta^{18}).
\end{aligned}$$

With $A = C_0 \cup C_1 \cup C_2$ we get $\{0,1,2,3\} \subseteq A$. The BCH-bound ensures that the double error correction is achieved with $\mathbf{g}(X) = \mathbf{m_0}(X)\mathbf{m_1}(X)\mathbf{m_2}(X)$. We have:

$$\begin{aligned}\mathbf{m_2}(X) &= (X-\theta^2)(X-\theta^6)(X-\theta^{18}) \\ &= X^3-(\theta^2+\theta^6+\theta^{18})X^2+(\theta^8+\theta^{20}+\theta^{24})X-1.\end{aligned}$$



With $\mathbf{p}(\theta)=0$ we obtain $\theta^3=2+\theta$, $\theta^{26}=1$, $\theta^{13}=-1=2$, as well as

$$\begin{aligned}\theta^6 &= (2+\theta)^2=4+4\theta+\theta^2=1+\theta+\theta^2, \\ \theta^{18} &= 2\theta^5=2\theta^2(2+\theta)=1+2\theta+\theta^2.\end{aligned}$$

Thus

$$\theta^2+\theta^6+\theta^{18}=\theta^2+1+\theta+\theta^2+1+2\theta+\theta^2=2.$$

Moreover:

$\theta^8=\theta^2\cdot\theta^6=\theta^2+\theta^3+\theta^4=\theta^2+2+\theta+2\theta+\theta^2=2+2\theta^2$,

$\theta^{20}=\theta^2\cdot\theta^{18}=\theta^2+2\theta^3+\theta^4=1+\theta+2\theta^2$,

$\theta^{24}=\theta^4\cdot\theta^{20}=(2\theta+\theta^2)(1+\theta+2\theta^2)=1+2\theta+2\theta^2$,

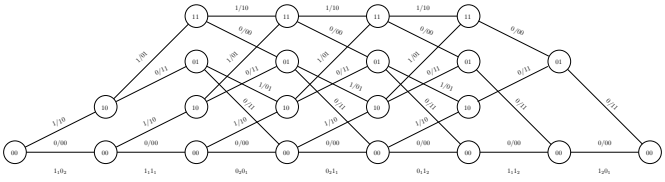
thus $\theta^8+\theta^{20}+\theta^{24}=1$ and $\mathbf{m_2}(X)=X^3-2X^2+X-1=X^3+X^2+X+2$. This leads to

$$\begin{aligned}\mathbf{g}(X) &= \mathbf{m_0}(X)\mathbf{m_1}(X)\mathbf{m_2}(X) \\ &= (X+2)(X^3+2X+1)(X^3+X^2+X+2) \\ &= X^7+2X^5+2X^4+X^3+1.\end{aligned}$$

Thus the maximum-likelihood message is $\mathbf{m}=(1,0,1,1,0)$.

5

The trellis for the rate $1/2$ 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.