TSDT16 Error-correcting codes

Solutions to the exam 2011-10-22

Danyo Danev, danyo@isy.liu.se

1

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 field $\mathbf{GF}(4) = \{0, 1, \beta, \beta^2\}$ is a sub-field of $\mathbf{GF}(2^4)$ and the element β can be identified as $\beta = \alpha^5$. The syndrome components of the received vector

$$\begin{aligned}\mathbf{r} &= (\beta^2, 1, 0, 0, 1, 0, \beta^2, 0, 0, 0, 0, \beta, 1, 0, 0)\\ &= (\alpha^{10}, 1, 0, 0, 1, 0, \alpha^{10}, 0, 0, 0, 0, \alpha^5, 1, 0, 0),\end{aligned}$$

which corresponds to the polynomial $\mathbf{r}(X) = X^{12} + a^5X^{11} + a^{10}X^6 + X^4 + X + a^{10}$ are

$$\begin{aligned}S_1 = \mathbf{r}(\alpha) &= \alpha^{14},\\ S_2 = \mathbf{r}(\alpha^2) &= \alpha^3,\\ S_3 = \mathbf{r}(\alpha^3) &= \alpha^2,\\ S_4 = \mathbf{r}(\alpha^4) &= \alpha^{11}.\end{aligned}$$

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^{14}	0	0	$-$
1	$1+\alpha^{14}X$	α^8	1	0	-1
2	$1+\alpha^4X$	α^{12}	1	1	0
3	$1+\alpha^3X^2$	α	2	1	1
4	$1+\alpha^4X+\alpha^{13}X^2$	$-$	2	2	2

The error location polynomial is $\sigma(X) = 1+\alpha^4X+\alpha^{13}X^2$. The roots of this polynomial are α^7 and α^{10}. Hence the error location numbers are $\alpha^{-7} = \alpha^8$ and $\alpha^{-10} = \alpha^5$.

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

$$\begin{aligned}\mathbf{Z}_0(X) &= S_1 + (S_2 + \sigma_1 S_1)X\\ &= \alpha^{14}.\end{aligned}$$

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

$$\sigma'(X) = \alpha^4.$$

The error values at positions X^5 and X^8 are

$$e_5 = -\frac{\mathbf{Z}_0(\alpha^{-5})}{\sigma'(\alpha^{-5})} = \alpha^{10},$$
$$e_8 = -\frac{\mathbf{Z}_0(\alpha^{-8})}{\sigma'(\alpha^{-8})} = \alpha^{10},$$

Consequently, the error pattern is

$$\mathbf{e}(X) = \alpha^{10}X^5 + \alpha^{10}X^8$$

and the decoded codeword polynomial is

$$\mathbf{c}(X) = \mathbf{r}(X) - \mathbf{e}(X) = X^{12} + \alpha^5 X^{11} + \alpha^{10}X^8 + \alpha^{10}X^6 + \alpha^{10}X^5 + X^4 + X + a^{10},$$

which corresponds to the codeword

$$\mathbf{c} = (\beta^2, 1, 0, 0, 1, \beta^2, \beta^2, 0, \beta^2, 0, 0, \beta, 1, 0, 0).$$

2

We can show that the minimum distance of this code is $d_{min} = 6$. First we note that the code has codewords of only even weight. This is due to the fact that the all-one vector of length 20 is a parity-check vector (it is the sum of the first five rows of H). Obviously all the columns of H are different and thus there are no codewords of weight 2. In order to show that d_{min} is at least 6 it remains to show that the sum of no 4 columns of H gives the all-zero vector of length 15. We can divide the columns in 5 groups depending on which of the first five positions they have a one. We note that neither of the sums of all vectors in a certain group is the all-zero vector. Thus if four columns have a zero sum then there should be two columns from two of these five groups in this sum (if there are odd number of columns from group l then there would be one on the l-th position of the sum). All the columns of group 1 have zeros in positions 10 and 15, group $2-9$ and 14, group $3-8$ and 13, group $4-7$ and 11, group $5-6$ and 12. Thus any sum of two vectors from a given group has zero in the corresponding positions. We observe that there are no two vectors from the same group that have ones in a common position (this is the requirement for a LDPC code) and there is a vector in each group that has one in any of the positions from 6 to 15 but the above mentioned. In this way only one possibility for each pair of groups is remaining if the sum of two pairs of vectors from those groups should be identical. For example if we take groups 1 and 2, we have to choose the second and third columns from group 2 since the other two have ones on either position 10 or 15. The columns of group 1 that have ones in positions 7 and 8 are the second and third but obviously their sum is not identical to the sum of the second and third columns of group 3. In a similar way we can show no sum of two columns from a group is identical to a sum of two columns from another group. This shows that there are no codewords of weight 4 and thus $d_{min} \geq 6$. It is easy to check that the vector

$$\mathbf{v} = (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$$

is a codeword which gives $d_{min} = 6$.

3

In order to calculate the generator and parity-check polynomials for the the binary primitive double error-correcting BCH-code of length 15 we can use the table for the field $\mathbf{GF}(16)$ in the solution of problem 1. The minimal polynomials of elements in $\mathbf{GF}(2^4)$ are given in the table below.

Conjugate roots	$\varphi_i(X)$
1	$1+X$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$1+X+X^4$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$1+X+X^2+X^3+X^4$
α^5, α^{10}	$1+X+X^2$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$1+X^3+X^4$

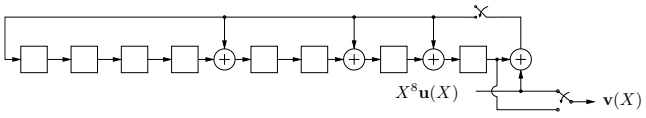
The generator polynomial $\mathbf{g}(X)$ must have the roots and thus

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

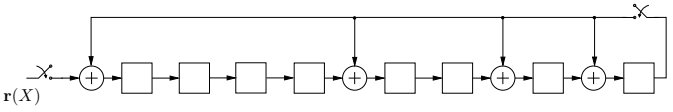
The parity-check polynomials is

$$\mathbf{h}(X) = \varphi_{\mathbf{0}}(X)\varphi_{\mathbf{5}}(X)\varphi_{\mathbf{7}}(X) = X^7 + X^6 + X^4 + 1.$$

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 $\mathbf{r}(X) = 1 + X^3 + X^5 + X^9 + X^{12}$ is

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

The contents of the syndrom calculation shift register after each step are as follows

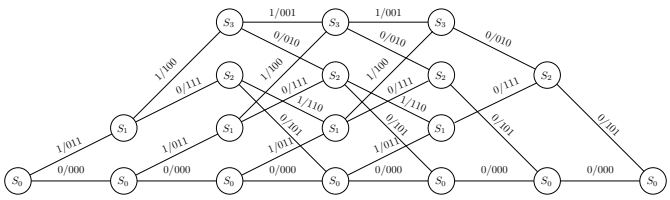
i	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0	0
5	0	0	1	0	0	0	0	0
6	1	0	0	1	0	0	0	0
7	0	1	0	0	1	0	0	0
8	0	0	1	0	0	1	0	0
9	0	0	0	1	0	0	1	0
10	1	0	0	0	1	0	0	1
11	1	1	0	0	1	1	1	1
12	0	1	1	0	1	1	0	0
13	0	0	1	1	0	1	1	0
14	0	0	0	1	1	0	1	1
15	**0**	**0**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

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

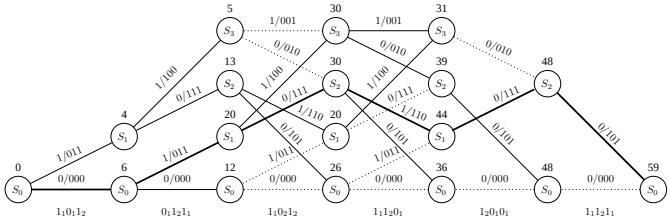
$$\mathbf{s}(X) = X^6 + X^5.$$

4

The trellis for the rate one-third 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 $\mathbf{m} = (0101)$.

5

The code C_1 is a subcode of C and consists of all codewords in C which have even weights. If A_i is the number of codewords of weight i in C and $A_i^{(1)}$ is the number of codewords of weight i in C_1, we have that

$$A_i^{(1)} = \begin{cases} A_i, & \text{if } i \text{ is even,} \\ 0, & \text{if } i \text{ is odd.} \end{cases}$$

Since the weight enumerator $A(z)$ is defined as

$$A(z) = \sum_{i=0}^{n} A_i z^i,$$

we have

$$\begin{aligned} \tfrac{A(z)+A(-z)}{2} &= \frac{\sum_{i=0}^{n} A_i z^i + \sum_{i=0}^{n} A_i (-z)^i}{2} \\ &= \tfrac{1}{2} \textstyle\sum_{i=0}^{n} A_i (1 + (-1)^i) z^i \\ &= \textstyle\sum_{j=0}^{\lfloor n/2 \rfloor} A_{2j} z^i \\ &= \textstyle\sum_{i=0}^{n} A_i^{(1)} z^i \\ &= A_1(z), \end{aligned}$$

which is what we had to show.