S-72.341 CODING METHODS

Tutorial 6, Solutions

1.

a) The generator polynomial $g(x)$ of an t-error correcting BCH code has $2t$ consecutive powers of the primitive element α^b as zeros. For narrow-sense BCH code $b = 1$. The required design distance $\delta = 2t+1 = 3$ implies that $\delta - 1 = 2$ consecutive powers of α are roots of $g(x)$. In other words the generator polynomial $g(x)$ is the least common multiple of the minimal polynomials for the selected powers of α.

We search for the polynmial in GF(q) where q=15. One of the cyclotomic cosets of the GF(16) is $\{1,2,4,8\}$ with the corresponding minimal polynomial being $x^4 + x + 1$.

For narrow-sense code with design parameter 3 the two required roots of $g(x)$ are α^1 and α^2. Both of these have the same corresponding minimal polynomial and therefore the generator polynomial is

$g(x) = x^4 + x + 1$.

b) The code rate is the ratio of *k,* the number of data symbols transmitted per code word, to *n,* the total number of symbols transmitted per codeword. The dimension of the code is the order of the codeword, $N = 15$, minus the order of the generator polynomial $m = 4$. The code rate is:

$N = 15, k = 15 - 4 = 11 \Rightarrow R = \frac{11}{15}$.

c) A BCH code is a cyclic code. The generaor matrix of a cyclic code can be composed from shifted versions of the generator polynomials. The amount of rows is equal to the amount of data symbols, in our case to 11.

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & & & \overline{0} & \\ 0 & 1 & 1 & 0 & 0 & 1 & & & & \\ & & & \overline{0} & & & \ddots & & & \\ & & & & & & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \Big\} 11$$

The parity check matrix can be constructed similarly by setting the coefficients of the parity check polynomial. An alternative way to create the parity check matrix is to notice as in eq. 8.1 (in the book) that if $\overline{r}$ is codeword then $rH = 0$. H is orthogonal to codeword if it contains the zeros of

the received code polynomial $\bar{r}$, i.e. $\{\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\delta-1}\}$. In our case $b = 1$ and the first line of the H is:

$$\mathrm{H}=\begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{14} \end{bmatrix}.$$

We have only two roots $\{\alpha^1, \alpha^2\}$. The row of H corresponding to the other root $\{\alpha^2\}$ can be set up similarly. However $\{\alpha^1, \alpha^2\}$ are zeros of the same minimal polynomial and therefore by adding the second row we add redudancy.

2. The design distance 4 requires that three consequitive powers of α are roots of the generator polynomial. The three first cyclotomic cosetes with corresponging minimal polynomimials represented in the binary field are:

   $\{0\}$

   $\{1,2,4,8\} \leftrightarrow M_1(x) = x^4 + x + 1$

   $\{3,6,12,9\} \leftrightarrow M_3(x) = x^4 + x^3 + x^2 + x + 1.$

   The generator polynomial has roots $\{\alpha^1, \alpha^2, \alpha^3\}$ if it is greated by multiplying minimal polynomials of two corresponding cyclotomic cosets

   $g(x) = M_1(x) M_3(x) = x^8 + x^7 + x^6 + x^4 + 1.$

   The generator polynomial has order 8 and the maximal message polynomial has order 15-8=7. The code rate is

   $$R = \frac{7}{15}.$$

3. The code rate is minimized if the generator polynomial has minimal possible order. The order of the generator polynomial is defined by the cyclotomic cosets where the required consecutive powers of α^b belong. By choosing appropriate b we can select the cosets and due that the minimal polynomials which are multiplied into generartor polynomial. First two cosets in and corresponding minimal polynomials with respect to GF(2) for GF(16) are:

   $$\{0\} \leftrightarrow M_0(x) = x + 1$$
   $$\{1,2,4,8\} \leftrightarrow M_1(x) = x^4 + x + 1.$$

   For error correction distance $t = 4$ we need three consecutive powers of α^b. By selecting b =0, the roots are $\{\alpha^0, \alpha^1, \alpha^2\}$. The generator polynomial is

   $g(x) = M_0(x) M_1(x) = x^5 + x^4 + x^2 + 1.$

   The code rate is more efficient than the code rate in previous exercise where $b = 1$.

$$R = \frac{2}{3} > \frac{7}{15}.$$

4. The good code is characterised by a high code rate. The code rate is maximaised when for the same amount of coded bits can be transmitted more information bits. The amount of information bits in a BCH code is limited by the order of the generator polynomial. The generator polynomial is calculated as a least common divisor of the minimal polynomials corresponding to the selected powers of α.

   In CF(2) $x^{19}+1$ factors into two polynomials, one of degree 1, the other of degree 18. If the design distance is more than 2 the generator polynomial has to have order of 18. We can not select the genetor polynomial with small order and therefore we can not have a good code of order 19.

5. $\left(2^9\right)^2$ is the smallest field where we can find a primitive 19-th root of unity. The cyclotomic cosets modulo 19 with respect to $GF\left(2^9\right)$ are:

$$\{0\},\{1,18\},\{2,19\},\{3,16\},\{4,15\},\{5,14\},\{6,13\},$$
$$\{7,12\},\{8,11\},\{9,10\}.$$

   First of the correspondig minimal polynomial is of order 1 rest of them are of order 2.

   For a t error correcting code we have to select $2t$ corresponding powers of the minimal element. Therefore a t error correcting 2^9-ary BCH code of length 19 will have dimension $\leq 19-2\times 2t$. It is a reasonable code, not bad, not good.

6.

   a) A Reed-Solomon code is a BCH code over GF(q^m) of length q^m-1. For constructing it we have to find the primitive element α in the field q^m. A norrow-sense code with design distance 3 requires two consequenct powers of the primitive element $\left\{\alpha^1,\alpha^2\right\}$.

      Because each cyclotomic coset of Reed-Solomon contains only one element we have

$$g(x) = (x+\alpha)\left(x+\alpha^2\right) = x^2+\alpha^5 x+\alpha^3.$$

      Where we used the add on table for GF(16) given in the Appendix B of the book.

   b) Rate of the code is calculated as usually for the BCH code.

$$R = \frac{15-2}{15} = \frac{13}{15}.$$

c) The rule for constructing the generator matrix for the Reed-Solomon code is same as for any cyclic code. (see for example the exercise 1 above)

$$G = \begin{bmatrix} \alpha^3 & \alpha^5 & 1 & 0 & & \overline{0} \\ 0 & \alpha^3 & \alpha^5 & 1 & & \\ & & & & \ddots & \\ & & \overline{0} & & & \\ & & & & \alpha^3 & \alpha^5 & 1 \end{bmatrix} \Big\} 13 rows .$$

The error correction matrix has two rows where one contains the powers of the primitive element α and other the powers of the α^2

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{13} \end{bmatrix}.$$

7. The narrow-sense double-error-correcting code requires that we select 4 consequitive powers of the primitive element α. The calculation of the generator polynomial is straigth forward:

$$\begin{aligned} g(x) &= (x+\alpha)\left(x+\alpha^2\right)\left(x+\alpha^3\right)\left(x+\alpha^4\right) \\ &= \left(x^2+\alpha^{19}x+\alpha^3\right)\left(x+\alpha^3\right)\left(x+\alpha^4\right) \\ &= \left(x^3+\alpha^{12}x^2+\alpha^{14}x+\alpha^6\right)\left(x+\alpha^4\right) \\ &= x^4+\alpha^{24}x^3+\alpha^{19}x^2+\alpha^{29}x+\alpha^{10}. \end{aligned}$$

We used for summation the add on table for GF(32) given in the Appendix B of the book.