BCH Codes -I

Qi Zhang

Aarhus University School of Engieering

24/02, 2014

- Let's look the example of Hamming code $C_{cyc}(7,4)$ with generator polynomial $g_1(X) = 1 + X + X^3$.
- This generator polynomial has no roots in GF(2), but it has three roots in the GF(2^3) which is generated by primitive polynomial $p_i(X) = 1 + X + X^3$.
- For this particular case, we can easily tell that α is one of the roots of $g_1(X)$.
- We also know that the other roots are the conjugate of α, according to Theorem B.1. Therefore, we find that the other two roots are α^2 and α^4.
- Assuming that the received polynomial is $r(X)$, we know the relation between the received polynomial and syndrome polynomial:

$$r(X) = q(X)g_1(X) + S(X)$$

- If substituting X by α, there is $r(\alpha) = q(\alpha)g_1(\alpha) + S(\alpha) = S(\alpha) = s_1$.
- Similarly if substituting X by α^2, there is $r(\alpha^2) = q(\alpha^2)g_1(\alpha^2) + S(\alpha^2) = S(\alpha^2) = s_2$.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

- It is possible to find a system of two equations that allows the solution of two unknowns, which are the position and the value of a single error in the polynomial.
- $g_1(X)$ has three roots, therefore, it cannot correct error patterns of $t = 2$.
- The other elements of the extended field GF(8), α^3, α^5 and α^6 which are the roots of another polynomial:

$$g_2(X) = (x + \alpha^3)(X + \alpha^5)(X + \alpha^6) = X^3 + X^2 + 1$$

- In fact, we know $g_1 = \phi_1(X)$ is the minimal polynomial of α, α^2 and α^4 and $g_2 = \phi_2(X)$ is the minimal polynomial of α^3, α^5 and α^6.
- If we take the lowest common multiple (LCM) of these two polynomials $\phi_1(X)$ and $\phi_2(X)$ will form a generator polynomial with roots α, α^2, α^3, α^4, α^5 and α^6.

$$g_4(X) = \phi_1(X)\phi_2(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

- $g_4(X)$ has 6 roots and have six equations which determine the positions and values of up to three errors in a given codeword.
- From another angle, $g_4(X)$ generates $C_{cyc}(7, 1)$ with $d_{min} = 7$, able to correct any error pattern of size $t = 3$ or less.

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

BCH codes properties

- BCH codes are a class of cyclic codes.
- BCH codes are a generalization of Hamming codes. It can correct any error pattern of size t.
- For any integer $m \geq 3$ and $t < 2^{m-1}$, there exists a binary BCH code $C_{BCH}(n, k)$, with properties:

	BCH code	Hamming code
Code length	$n = 2^m - 1$	$n = 2^m - 1$
Number of parity bits	$n - k \leq mt$	$n - k = m$
Minimum Hamming distance	$d_{min} \geq 2t + 1$	$d_{min} = 3$
Error correction capability	t	$t = 1$

- For example, $C_{BCH}(15, 7)$ has minimum distance $d_{min} = 5$ and $t = 2$. $n - k = 15 - 7 = 4 \times 2 = mt$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

BCH codes example

n	k	t
15	7	2
15	5	3
31	21	2
31	16	3
31	11	5
63	51	2
63	45	3
63	39	4
63	36	5
63	30	6
127	113	2
127	106	3
255	239	2
255	231	3

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator polynomial of BCH code

- The generator polynomial of BCH code $g(X)$ is described in terms of its roots which are taken from GF(2^m).
- Assuming $g(X)$ has roots: X_1, X_2, ... and X_i, $g(X)$ can be written in the format as

$$g(X) = (X + X_1)(X + X_2) \dots (X + X_i)$$

- There are binary BCH codes and non-binary BCH codes.
- The generator polynomial of binary BCH codes is a polynomial defined over GF(2).

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Generator polynomial of BCH code

- How to find a generator polynomial which can generate codes for correcting t errors in a code vector of length $n = 2^m - 1$?
- Assuming α is a primitive element in $GF(2^m)$,
- The generator polynomial $g(X)$ of such a BCH code is the minimum-degree polynomial over GF(2) that has roots $\alpha, \alpha^2, \dots, \alpha^{2t}$, i.e.,

$$g(\alpha^i) = 0, \quad i = 1, 2, \dots, 2t$$

- Assuming $\phi_i(X)$ is the minimal polynomial of α^i, then $g(X)$ can be expressed by the *lowest common multiple (LCM)* of the minimal polynomials:

$$g(X) = \mathrm{LCM}\{\phi_1(X), \phi_2(X), \dots, \phi_{2t}(X)\}$$

- Due to repetition of conjugate roots, the generator polynomial $g(X)$ can be formed with ONLY the ODD index minimal polynomials:

$$g(X) = \mathrm{LCM}\{\phi_1(X), \phi_3(X), \dots, \phi_{2t-1}(X)\}$$

Table B.5 Minimal polynomial of all the elements of the Galois field $GF(2^4)$ generated by $p_i(X) = 1 + X + X^4$

conjugate roots	Minimal polynomials
0	X
1	$1 + X$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$1 + X + X^4$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$1 + X + X^2 + X^3 + X^4$
α^5, α^{10}	$1 + X + X^2$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$1 + X^3 + X^4$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator polynomial of BCH code

- As the degree of each minimal polynomial is m or less, the degree of $g(X)$ is at most mt.
- The parity check digits, $n-k$, of the code is at most equal to mt.
- There is no simple formula for enumerating $n-k$, but if t is small, $n-k=mt$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Generator polynomial of BCH code

- **Example 4.1**: Let α be a primitive element of GF(2^4) generated by primitive polynomial $p_i(X) = 1 + X + X^4$. To form the generator polynomial of a BCH code with $t = 2$ error correct capability. We know the minimal polynomial of α, α^3 and α^5 are, respectively,

$$\begin{aligned}\phi_1(X) &= 1 + X + X^4 \\ \phi_3(X) &= 1 + X + X^2 + X^3 + X^4 \\ \phi_5(X) &= 1 + X + X^2\end{aligned}$$

- **Solution**: As $t = 2$, $2t - 1 = 3$, the generator polynomial can be expressed by

$$g(X) = \text{LCM}\{\phi_1(X), \phi_3(X)\}$$

As $\phi_1(X)$ and $\phi_3(X)$ are irreducible,

$$\begin{aligned}g(X) &= \phi_1(X)\phi_3(X) = (1 + X + X^4)(1 + X + X^2 + X^3 + X^4) \\ &= 1 + X^4 + X^6 + X^7 + X^8\end{aligned}$$

- This generator polynomial $g(X)$ generates BCH code $C_{BCH}(15, 7)$.

Generator polynomial of BCH code

- **Example 4.1.1**: Of the same GF(2^4), to form the generator polynomial of a BCH code with $t = 3$ error correct capability. We known the minimal polynomial of α, α^3 and α^5 are, respectively,

$$\begin{aligned} \phi_1(X) &= 1 + X + X^4 \\ \phi_3(X) &= 1 + X + X^2 + X^3 + X^4 \\ \phi_5(X) &= 1 + X + X^2 \end{aligned}$$

- **Solution**: As $t = 3$, $2t - 1 = 5$, the generator polynomial can be expressed by

$$g(X) = \mathrm{LCM}\{\phi_1(X), \phi_3(X), \phi_5(X)\}$$

As $\phi_1(X)$, $\phi_3(X)$ and $\phi_5(X)$ are irreducible,

$$\begin{aligned} g(X) &= \phi_1(X)\phi_3(X)\phi_5(X) \\ &= (1 + X + X^4)(1 + X + X^2 + X^3 + X^4)(1 + X + X^2) \\ &= 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10} \end{aligned}$$

- This generator polynomial $g(X)$ generates BCH code $C_{BCH}(15, 5)$.

Parity check matrix

- For a BCH code $C_{BCH}(n, k)$ for correcting t errors or less and with code length $n = 2^m - 1$,
- As in cyclic code the code polynomial is a multiple of the generator polynomial, the code polynomial of this BCH code also has α, α^2, ..., α^{2t} and their conjugates as its roots.
- Assume the code polynomial $c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$ has a primitive element α^i as a root, there is

$$c(\alpha^i) = c_0 + c_1 \alpha^i + \ldots + c_{n-1} \alpha^{i(n-1)} = 0$$

- We can use an inner product of two vectors to represent the above equation:

$$(c_0, c_1, \ldots, c_{n-1}) \circ \begin{bmatrix} 1 \\ \alpha^i \\ \alpha^{2i} \\ \vdots \\ \alpha^{(n-1)i} \end{bmatrix} = 0$$

AARHUS UNIVERSITET INGENIØRHØJSKOLEN

Parity check matrix

- Similarly, if we substitute roots α, α^2, ..., α^{2t} into code polynomial $c(X)$, we can have $2t$ similar equations.
- These $2t$ equations can be written into a matrix form.

$$(c_0, c_1, \ldots, c_{n-1}) \circ \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \alpha & \alpha^2 & \alpha^3 & \ldots & \alpha^{2t} \\ \alpha^2 & (\alpha^2)^2 & (\alpha^3)^2 & \ldots & (\alpha^{2t})^2 \\ \alpha^3 & (\alpha^2)^3 & (\alpha^3)^3 & \ldots & (\alpha^{2t})^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{n-1} & (\alpha^2)^{n-1} & (\alpha^3)^{n-1} & \ldots & (\alpha^{2t})^{n-1} \end{bmatrix} = \mathbf{c} \circ \mathbf{H}^T = \mathbf{0}$$

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \ldots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \ldots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & (\alpha^{2t})^3 & \ldots & (\alpha^{2t})^{n-1} \end{bmatrix}$$

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Calculate the syndrome vector

- Parity check matrix:

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \dots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \dots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & (\alpha^{2t})^3 & \dots & (\alpha^{2t})^{n-1} \end{bmatrix}$$

- Syndrome vector can be expressed by

$$\begin{aligned} \mathbf{S} &= (s_1, s_2, \dots, s_{2t}) = \mathbf{r} \circ \mathbf{H}^T \\ &= (r_0, r_1, \dots, r_{n-1}) \circ \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha & \alpha^2 & \dots & \alpha^{2t} \\ \alpha^2 & (\alpha^2)^2 & \dots & (\alpha^{2t})^2 \\ \vdots & \vdots & \dots & \vdots \\ \alpha^{n-1} & (\alpha^2)^{n-1} & \dots & (\alpha^{2t})^{n-1} \end{bmatrix} \end{aligned}$$

therefore,

$$s_i = r_0 + r_1 \cdot \alpha^i + r_2 \cdot (\alpha^i)^2 + \dots + r_{n-1} \cdot (\alpha^i)^{n-1} = r(\alpha^i)$$

with $1 \leq i \leq 2t$.

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Calculate the syndrome vector

- **Summary**:
  - To calculate the ith component of the syndrome vector, we can replace the variable X with the root α^i in the received polynomial $r(X)$.
  - Syndrome vector consists of elements of the GF(2^m).

AARHUS UNIVERSITET
INGENIØRHØJSKOLEN

Calculate the syndrome vector

- **Example 4.3**: The Binary BCH code $C_{BCH}(15,7)$ can correct 2 or less errors. The generator polynomial has roots in GF(2^4) which is generated by primitive polynomial $p_i(X) = 1 + X + X^4$. If the received vector $\mathbf{r} = (100000001000000)$, calculate the syndrome vector.
- **Solution**: Since $\mathbf{r} = (100000001000000)$, $r(X) = 1 + X^8$, then substitute $\alpha^i, 1 \leq i \leq 2t = 4$, and look up Table B.4

$$\begin{aligned}
s_1 &= r(\alpha) = 1 + \alpha^8 = \alpha^2 \\
s_2 &= r(\alpha^2) = 1 + \alpha = \alpha^4 \\
s_3 &= r(\alpha^3) = 1 + \alpha^9 = 1 + \alpha + \alpha^3 = \alpha^7 \\
s_4 &= r(\alpha^4) = 1 + \alpha^2 = \alpha^8
\end{aligned}$$