Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 19
March 28, 2023

Cyclic codes

Recall

- △ If $\alpha \in F_q$ then the minimal polynomial of α over F_q is the (lowest degree) irreducible polynomial $f(x) \in F_p[x]$ such that $f(\alpha) = 0$, where $q = p^s$

Cyclic codes

Recall

- △ If $\alpha \in F_q$ then the minimal polynomial of α over F_q is the (lowest degree) irreducible polynomial $f(x) \in F_p[x]$ such that $f(\alpha) = 0$, where $q = p^s$
- △ If α has order e (note that in F_q, the multiplicative group $F_q \setminus \{0\}$ is a cyclic group) then the minimal polynomial is

$$\prod_{i=0}^{m-1} (x - \alpha^{p^i}),$$

where m is the smallest integer such that $p^m \equiv 1 \pmod{e}$

Cyclic codes

Recall

- △ If $\alpha \in F_q$ then the minimal polynomial of α over F_q is the (lowest degree) irreducible polynomial $f(x) \in F_p[x]$ such that $f(\alpha) = 0$, where $q = p^s$
- △ If α has order e (note that in F_q, the multiplicative group $F_q \setminus \{0\}$ is a cyclic group) then the minimal polynomial is

$$\prod_{i=0}^{m-1} (x - \alpha^{p^i}),$$

where m is the smallest integer such that $p^m \equiv 1 \pmod{e}$

- △ A generator of the multiplicative group of F_q is called a primitive element of the F_q

Cyclic codes

Recall

- △ If $\alpha \in F_q$ then the minimal polynomial of α over F_q is the (lowest degree) irreducible polynomial $f(x) \in F_p[x]$ such that $f(\alpha) = 0$, where $q = p^s$
- △ If α has order e (note that in F_q, the multiplicative group $F_q \setminus \{0\}$ is a cyclic group) then the minimal polynomial is

$$\prod_{i=0}^{m-1} (x - \alpha^{p^i}),$$

  where m is the smallest integer such that $p^m \equiv 1 \pmod{e}$
- △ A generator of the multiplicative group of F_q is called a primitive element of the F_q
- △ An element $\beta \in F_q$ such that $\beta^k = 1$ but $\beta^l \neq 1$, for $0 < l < k$ is called a primitive kth root of unity

Cyclic codes

Recall

- △ If $\alpha \in F_q$ then the minimal polynomial of α over F_q is the (lowest degree) irreducible polynomial $f(x) \in F_p[x]$ such that $f(\alpha) = 0$, where $q = p^s$
- △ If α has order e (note that in F_q, the multiplicative group $F_q \setminus \{0\}$ is a cyclic group) then the minimal polynomial is

$$\prod_{i=0}^{m-1}(x - \alpha^{p^i}),$$

  where m is the smallest integer such that $p^m \equiv 1 \pmod{e}$
- △ A generator of the multiplicative group of F_q is called a primitive element of the F_q
- △ An element $\beta \in F_q$ such that $\beta^k = 1$ but $\beta^l \neq 1$, for $0 < l < k$ is called a primitive kth root of unity
- △ Obviously, a primitive element of F_q is a primitive $(q-1)$th root of unity

Cyclic codes

Discovered independently by RC Bose, DK Ray-Chaudhuri (1960), and by A. Hocquenghem (1959)

Cyclic codes

Discovered independently by RC Bose, DK Ray-Chaudhuri (1960), and by A. Hocquenghem (1959)

BCH codes

→ Applications of the BCH codes were introduced for binary codes of length $2^m - 1$

Cyclic codes

Discovered independently by RC Bose, DK Ray-Chaudhuri (1960), and by A. Hocquenghem (1959)

BCH codes

- → Applications of the BCH codes were introduced for binary codes of length $2^m - 1$
- → Later it was extended by Gorenstein and Zierler to nonbinary codes in 1961

Cyclic codes

Discovered independently by RC Bose, DK Ray-Chaudhuri (1960), and by A. Hocquenghem (1959)

BCH codes

→ Applications of the BCH codes were introduced for binary codes of length $2^m - 1$

→ Later it was extended by Gorenstein and Zierler to nonbinary codes in 1961

→ The decoding algo for binary BCH codes was first proposed by Peterson in 1960

Cyclic codes

For $n(\geq 3)$ divisor of $q^m - 1$, for some positive integer, a cyclic code of block length n over the field F_q, an (n, k) BCH code with t-error-correction for $2 \leq 2t \leq n-1$ is generated by

$$g(x) = LCM\{m_{m_0}(x), m_{m_0+1}(x), \ldots, m_{m_0+2t-1}(x)\},$$

where $m_{m_0+i}(x)$, $i = 0, 1, \ldots, 2t-1$ are minimal polynomials of the $2t$ successive powers α^{m_0}, $\alpha^{m_0+1}, \ldots, \alpha^{m_0+2t-1}$ of some $\alpha \in F_q$ whose order is n in some extension field $GF(q^m)$.
$LCM\{\cdot\}$ denotes the least common multiple polynomial

Cyclic codes

For $n(\geq 3)$ divisor of $q^m - 1$, for some positive integer, a cyclic code of block length n over the field F_q, an (n, k) BCH code with t-error-correction for $2 \leq 2t \leq n - 1$ is generated by

$$g(x) = LCM\{m_{m_0}(x), m_{m_0+1}(x), \ldots, m_{m_0+2t-1}(x)\},$$

where $m_{m_0+i}(x)$, $i = 0, 1, \ldots, 2t - 1$ are minimal polynomials of the $2t$ successive powers $\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+2t-1}$ of some $\alpha \in F_q$ whose order is n in some extension field $GF(q^m)$.
$LCM\{\cdot\}$ denotes the least common multiple polynomial

> If α is a primitive element in the extension field $GF(q^m)$ then the code is called primitive BCH

Cyclic codes

For $n(\geq 3)$ divisor of $q^m - 1$, for some positive integer, a cyclic code of block length n over the field F_q, an (n, k) BCH code with t-error-correction for $2 \leq 2t \leq n-1$ is generated by

$$g(x) = LCM\{m_{m_0}(x), m_{m_0+1}(x), \ldots, m_{m_0+2t-1}(x)\},$$

where $m_{m_0+i}(x)$, $i = 0, 1, \ldots, 2t-1$ are minimal polynomials of the $2t$ successive powers α^{m_0}, $\alpha^{m_0+1}, \ldots, \alpha^{m_0+2t-1}$ of some $\alpha \in F_q$ whose order is n in some extension field $GF(q^m)$.
$LCM\{\cdot\}$ denotes the least common multiple polynomial

> If α is a primitive element in the extension field $GF(q^m)$ then the code is called primitive BCH
>
> The order of such an element $n = q^m - 1$, the length of the code

Cyclic codes

For $n(\geq 3)$ divisor of $q^m - 1$, for some positive integer, a cyclic code of block length n over the field F_q, an (n, k) BCH code with t-error-correction for $2 \leq 2t \leq n-1$ is generated by

$$g(x) = LCM\{m_{m_0}(x), m_{m_0+1}(x), \ldots, m_{m_0+2t-1}(x)\},$$

where $m_{m_0+i}(x)$, $i = 0, 1, \ldots, 2t-1$ are minimal polynomials of the $2t$ successive powers $\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+2t-1}$ of some $\alpha \in F_q$ whose order is n in some extension field $GF(q^m)$.
$LCM\{\cdot\}$ denotes the least common multiple polynomial

- If α is a primitive element in the extension field $GF(q^m)$ then the code is called primitive BCH
- The order of such an element $n = q^m - 1$, the length of the code
- Codes with $m_0 = 1$ are called narrow-sense BCH codes

Cyclic codes

Observation

The degree of $g(x) \leq 2tm$, as there are at most $2t$ distinct minimal polynomials and each has degree at most m

Cyclic codes

Observation

The degree of $g(x) \leq 2tm$, as there are at most $2t$ distinct minimal polynomials and each has degree at most m

Thus for BCH codes over any finite field:

$$n - k = deg(g(x)) \leq 2t \cdot m \text{ and } n = q^m - 1$$

Cyclic codes

Observation

The degree of $g(x) \leq 2tm$, as there are at most $2t$ distinct minimal polynomials and each has degree at most m

Thus for BCH codes over any finite field:

$$n - k = deg(g(x)) \leq 2t \cdot m \text{ and } n = q^m - 1$$

Set $q = 2$.

Cyclic codes

Observation

The degree of $g(x) \leq 2tm$, as there are at most $2t$ distinct minimal polynomials and each has degree at most m

Thus for BCH codes over any finite field:

$$n - k = deg(g(x)) \leq 2t \cdot m \text{ and } n = q^m - 1$$

Set $q = 2$.
Suppose $m_i(x)$ is the minimal polynomial of α^i, also let $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ be a code polynomial with $c_j \in F_2$

If $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are roots of $c(x)$ then $c(x)$ is divisible by the minimal polynomials $m_1(x), m_2(x), \ldots, m_{2t}(x)$ of $\alpha, \alpha^2, \ldots, \alpha^{2t}$, respectively

Cyclic codes

Then the generator polynomial of the BCH code is given by

$$g(x) = LCM\{m_1(x), \ldots, m_{2t}(x)\}$$

where $m_i(x)$ is the minimal polynomial of α^i, for $i = 1, 2, \ldots, 2t$ and consists of $2t$ successive powers of α

Cyclic codes

Then the generator polynomial of the BCH code is given by

$$g(x) = LCM\{m_1(x), \ldots, m_{2t}(x)\}$$

where $m_i(x)$ is the minimal polynomial of α^i, for $i = 1, 2, \ldots, 2t$ and consists of $2t$ successive powers of α

The order of α is n in the extension field $GF(2^m)$

Cyclic codes

Then the generator polynomial of the BCH code is given by

$$g(x) = LCM\{m_1(x), \ldots, m_{2t}(x)\}$$

where $m_i(x)$ is the minimal polynomial of α^i, for $i = 1, 2, \ldots, 2t$ and consists of $2t$ successive powers of α

The order of α is n in the extension field $GF(2^m)$

Nonprimitive BCH codes are defined when α is a nonprimitive element of $GF(q^m)$, and the code length is the order of α

Cyclic codes

Then the generator polynomial of the BCH code is given by

$$g(x) = LCM\{m_1(x), \ldots, m_{2t}(x)\}$$

where $m_i(x)$ is the minimal polynomial of α^i, for $i = 1, 2, \ldots, 2t$ and consists of $2t$ successive powers of α

- The order of α is n in the extension field $GF(2^m)$
- Nonprimitive BCH codes are defined when α is a nonprimitive element of $GF(q^m)$, and the code length is the order of α

Cyclic codes

Then the generator polynomial of the BCH code is given by

$$g(x) = LCM\{m_1(x), \ldots, m_{2t}(x)\}$$

where $m_i(x)$ is the minimal polynomial of α^i, for $i = 1, 2, \ldots, 2t$ and consists of $2t$ successive powers of α

The order of α is n in the extension field $GF(2^m)$

Nonprimitive BCH codes are defined when α is a nonprimitive element of $GF(q^m)$, and the code length is the order of α

Example $(15, 7)$ BCH code: Let α be a primitive element of $GF(2^4)$ such that $1 + \alpha + \alpha^4 = 0$

Cyclic codes

For any positive integer pair m, t with $m \geq 3, t < n/2$, there exists a binary BCH code of block length $n = 2^m - 1$, where the number of parity-check bits satisfies $n - k \leq mt$, and the minimum distance $d_{\min} \geq d_0 = 2t + 1$, where d_0 is called the designed distance of the code.

Cyclic codes

For any positive integer pair m, t with $m \geq 3, t < n/2$, there exists a binary BCH code of block length $n = 2^m - 1$, where the number of parity-check bits satisfies $n - k \leq mt$, and the minimum distance $d_{\min} \geq d_0 = 2t + 1$, where d_0 is called the designed distance of the code.
Procedure to determine parameters of a BCH code:

1. Choose a primitive polynomial of degree m, and construct $GF(2^m)$

Cyclic codes

For any positive integer pair m, t with $m \geq 3, t < n/2$, there exists a binary BCH code of block length $n = 2^m - 1$, where the number of parity-check bits satisfies $n - k \leq mt$, and the minimum distance $d_{\min} \geq d_0 = 2t + 1$, where d_0 is called the designed distance of the code.
Procedure to determine parameters of a BCH code:

1. Choose a primitive polynomial of degree m, and construct $GF(2^m)$
2. Find the minimal polynomials $m_i(x)$ of α^i, $i = 1, 3, \ldots, 2t - 1$

Cyclic codes

For any positive integer pair m, t with $m \geq 3, t < n/2$, there exists a binary BCH code of block length $n = 2^m - 1$, where the number of parity-check bits satisfies $n - k \leq mt$, and the minimum distance $d_{\min} \geq d_0 = 2t + 1$, where d_0 is called the designed distance of the code.
Procedure to determine parameters of a BCH code:

1. Choose a primitive polynomial of degree m, and construct $GF(2^m)$
2. Find the minimal polynomials $m_i(x)$ of α^i, $i = 1, 3, \ldots, 2t - 1$
3. Find $g(x) = LCM\{m_1(x), m_3(x), \ldots, m_{2t-1}(x)\}$

Cyclic codes

For any positive integer pair m, t with $m \geq 3, t < n/2$, there exists a binary BCH code of block length $n = 2^m - 1$, where the number of parity-check bits satisfies $n - k \leq mt$, and the minimum distance $d_{\min} \geq d_0 = 2t + 1$, where d_0 is called the designed distance of the code.
Procedure to determine parameters of a BCH code:

1. Choose a primitive polynomial of degree m, and construct $GF(2^m)$
2. Find the minimal polynomials $m_i(x)$ of α^i, $i = 1, 3, \ldots, 2t - 1$
3. Find $g(x) = LCM\{m_1(x), m_3(x), \ldots, m_{2t-1}(x)\}$
4. Determine k from $deg(g(x)) = n - k$

Cyclic codes

For any positive integer pair m, t with $m \geq 3, t < n/2$, there exists a binary BCH code of block length $n = 2^m - 1$, where the number of parity-check bits satisfies $n - k \leq mt$, and the minimum distance $d_{\min} \geq d_0 = 2t + 1$, where d_0 is called the designed distance of the code.

Procedure to determine parameters of a BCH code:

1. Choose a primitive polynomial of degree m, and construct $GF(2^m)$
2. Find the minimal polynomials $m_i(x)$ of α^i, $i = 1, 3, \ldots, 2t - 1$
3. Find $g(x) = LCM\{m_1(x), m_3(x), \ldots, m_{2t-1}(x)\}$
4. Determine k from $deg(g(x)) = n - k$
5. Find $d_{\min} \geq 2t + 1$ through the parity-check matrix H, as discussed for the cyclic code

BCH code

Minimum distance of BCH code Let $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ be a code polynomial of a primitive t-error correcting BCH code of block length $n = 2^m - 1$

BCH code

Minimum distance of BCH code Let $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ be a code polynomial of a primitive t-error correcting BCH code of block length $n = 2^m - 1$

$\rightarrow$ Suppose $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are roots of $c(x)$, and hence $c(x)$ is divisible by the generator polynomial $g(x)$, the LCM of the $m_i(x)$, $1 \leq i \leq 2t$

BCH code

Minimum distance of BCH code Let $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ be a code polynomial of a primitive t-error correcting BCH code of block length $n = 2^m - 1$

- $\rightarrow$ Suppose $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are roots of $c(x)$, and hence $c(x)$ is divisible by the generator polynomial $g(x)$, the LCM of the $m_i(x)$, $1 \leq i \leq 2t$
- $\rightarrow$ $c(\alpha^i) = c_0 + c_1\alpha^i + \ldots + c_{n-1}(\alpha^i)^{n-1} = 0$ implies that

$$\mathbf{c}\begin{bmatrix} 1 \\ \alpha^i \\ \vdots \\ (\alpha^i)^{n-1} \end{bmatrix} = 0,\ 1 \leq i \leq 2t$$

and hence

$$\mathbf{c} \cdot H_i^T = 0,$$

where $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ and $H_i = \left(1\,\alpha^i\,\ldots\,(\alpha^i)^{n-1}\right), 1 \leq i \leq 2t$

BCH code

Now construct the matrix H as follows:

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

where the entries of H are nonzero elements in $GF(2^m)$

BCH code

Now construct the matrix H as follows:

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

where the entries of H are nonzero elements in $GF(2^m)$

$\rightarrow$ We want to show that any set of $d_0 - 1$ or $2t$ columns of H cannot be linearly dependent so that the t-error-correcting BCH code has minimum distance of at least d_0 or $2t + 1$

BCH code

Suppose there exists a codeword whose components consists of the nonzero digits $c_{j_u} = 1$, $1 \leq u \leq 2t$. Then we have

$$(c_{j_1},\, c_{j_2},\, \ldots,\, c_{j_{2t}}) \underbrace{\begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \ldots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{2t} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha^{j_{2t}} & (\alpha^{j_{2t}})^2 & \ldots & (\alpha^{j_{2t}})^{2t} \end{bmatrix}_{2t \times 2t}}_{D} = 0$$

where $c_{j_1} = c_{j_2} = \ldots = c_{j_{2t}} = 1$

BCH code

Suppose there exists a codeword whose components consists of the nonzero digits $c_{j_u} = 1$, $1 \leq u \leq 2t$. Then we have

$$(c_{j_1}, c_{j_2}, \ldots, c_{j_{2t}}) \underbrace{\begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \ldots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{2t} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha^{j_{2t}} & (\alpha^{j_{2t}})^2 & \ldots & (\alpha^{j_{2t}})^{2t} \end{bmatrix}_{2t \times 2t}}_{D} = 0$$

where $c_{j_1} = c_{j_2} = \ldots = c_{j_{2t}} = 1$
However, $|D| \neq 0$, where $|D|$ is called the van der Monde determinant

BCH code

Suppose there exists a codeword whose components consists of the nonzero digits $c_{j_u} = 1$, $1 \leq u \leq 2t$. Then we have

$$(c_{j_1}, c_{j_2}, \ldots, c_{j_{2t}}) \underbrace{\begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \ldots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \ldots & (\alpha^{j_2})^{2t} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha^{j_{2t}} & (\alpha^{j_{2t}})^2 & \ldots & (\alpha^{j_{2t}})^{2t} \end{bmatrix}_{2t \times 2t}}_{D} = 0$$

where $c_{j_1} = c_{j_2} = \ldots = c_{j_{2t}} = 1$
However, $|D| \neq 0$, where $|D|$ is called the van der Monde determinant

BCH codes

Now evaluating $|D|$ by factoring out α^{j_u}, $1 \le u \le 2t$,

$$\begin{aligned} |D| &= \alpha^{j_1+j_2+\ldots+j_{2t}} \begin{vmatrix} 1 & \alpha^{j_1} & \ldots & (\alpha^{j_1})^{2t-1} \\ 1 & \alpha^{j_2} & \ldots & (\alpha^{j_2})^{2t-1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha^{j_{2t}} & \ldots & (\alpha^{j_{2t}})^{2t-1} \end{vmatrix} \\ &= \alpha^{j_1+j_2+\ldots+j_{2t}} \prod_{v<u} \left(\alpha^{j_u} - \alpha^{j_v}\right) \neq 0 \end{aligned}$$

BCH codes

Now evaluating $|D|$ by factoring out α^{j_u}, $1 \leq u \leq 2t$,

$$
\begin{aligned}
|D| &= \alpha^{j_1+j_2+\ldots+j_{2t}} \begin{vmatrix} 1 & \alpha^{j_1} & \ldots & (\alpha^{j_1})^{2t-1} \\ 1 & \alpha^{j_2} & \ldots & (\alpha^{j_2})^{2t-1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha^{j_{2t}} & \ldots & (\alpha^{j_{2t}})^{2t-1} \end{vmatrix} \\
&= \alpha^{j_1+j_2+\ldots+j_{2t}} \prod_{v<u} \left(\alpha^{j_u} - \alpha^{j_v}\right) \neq 0
\end{aligned}
$$

Thus any set of $d_0 - 1$ columns is linearly independent and hence the assumption is invalid i.e. the minimum distance of the t-error-correcting BCH code is at least the designed distance $d_0 = 2t - 1 \geq d_{\min}$

BCH code

Decoding of BCH code computing syndrome

Suppose that a code polynomial $c(x)$ is transmitted and the received polynomial is $r(x) = c(x) + e(x)$, where $e(x) = e_0 + e_1 x + \ldots + e_{n-1}x^{n-1}$ is called the error polynomial.

BCH code

Decoding of BCH code computing syndrome

Suppose that a code polynomial $c(x)$ is transmitted and the received polynomial is $r(x) = c(x) + e(x)$, where $e(x) = e_0 + e_1 x + \ldots + e_{n-1}x^{n-1}$ is called the error polynomial.

Suppose there are $v \leq t$ non-zero coefficients of $e(x)$ in the umknown locations $j_1, j_2, \ldots, j_v$ i.e.

$$e(x) = \sum_{j=1}^{v} x^{j_i}, \; 0 \leq j_i \leq n-1$$

BCH code

Decoding of BCH code computing syndrome

Suppose that a code polynomial $c(x)$ is transmitted and the received polynomial is $r(x) = c(x) + e(x)$, where $e(x) = e_0 + e_1 x + \ldots + e_{n-1}x^{n-1}$ is called the error polynomial.

Suppose there are $v \leq t$ non-zero coefficients of $e(x)$ in the umknown locations $j_1, j_2, \ldots, j_v$ i.e.

$$e(x) = \sum_{j=1}^{v} x^{j_i}, \, 0 \leq j_i \leq n-1$$

Since $\alpha, \alpha^2, \ldots, \alpha^{2t}$ are roots of each code polynomial, $c(\alpha^i) = 0$ for $1 \leq i \leq 2t$. Thus, from $r(x) = c(x) + e(x)$, we have

$$r(\alpha^i) = e(\alpha^i), i = 1, 2, \ldots, 2t$$

BCH codes

Let $s(x)$ denote the syndrome polynomial from the received-word polynomial $r(x)$, given by

$$\mathbf{S} = (S_1, S_2, \ldots, S_{2t}) = \mathbf{r} \cdot H^T$$

so that

$$S_i = r(\alpha^i) = r_0 + r_1\alpha^i + \ldots + r_{n-1}\alpha^{(n-1)i} \in GF(2^m), 1 \leq i \leq 2t$$

which corresponds to the syndrome polynomial

$$s_i(x) = s_0^{(i)} + s_1^{(i)}x + \ldots + s_{n-k-1}^{(i)}x^{n-k-1} \equiv (s_0^{(1)}, s_1^{(i)}, \ldots, s_{n-k-1}^{(i)})$$

BCH codes

Let $s(x)$ denote the syndrome polynomial from the received-word polynomial $r(x)$, given by

$$\mathbf{S} = (S_1, S_2, \ldots, S_{2t}) = \mathbf{r} \cdot H^T$$

so that

$$S_i = r(\alpha^i) = r_0 + r_1\alpha^i + \ldots + r_{n-1}\alpha^{(n-1)i} \in GF(2^m), 1 \leq i \leq 2t$$

which corresponds to the syndrome polynomial

$$s_i(x) = s_0^{(i)} + s_1^{(i)}x + \ldots + s_{n-k-1}^{(i)}x^{n-k-1} \equiv (s_0^{(1)}, s_1^{(i)}, \ldots, s_{n-k-1}^{(i)})$$

Therefore, each syndrome entry of $\mathbf{S}$ can be computed by dividing $r(x)$ by the minimal polynomial $m_i(x)$ for $1 \leq i \leq 2t$ of α^i such that

$$r(x) = q_i(x)m_i(x) + p_i(x)$$

BCH code

Now, the remainder $p_i(x)$, where $x = \alpha^i$, is the syndrome entry S_i since $m_i(\alpha^i) = 0$. Therefore, computing $r(\alpha^i)$ is equivalent to computinf $p_i(\alpha^i)$, and hence

$$S_i = p_i(\alpha^i) = r(\alpha^i) = e(\alpha^i),\ 1 \leq i \leq 2t$$

which further implies that the syndrome vector **S** depends only on the error vector **e**

BCH code

Now, the remainder $p_i(x)$, where $x = \alpha^i$, is the syndrome entry S_i since $m_i(\alpha^i) = 0$. Therefore, computing $r(\alpha^i)$ is equivalent to computinf $p_i(\alpha^i)$, and hence

$$S_i = p_i(\alpha^i) = r(\alpha^i) = e(\alpha^i),\ 1 \leq i \leq 2t$$

which further implies that the syndrome vector **S** depends only on the error vector **e**

Next task Find the error locations

BCH code

Now, the remainder $p_i(x)$, where $x = \alpha^i$, is the syndrome entry S_i since $m_i(\alpha^i) = 0$. Therefore, computing $r(\alpha^i)$ is equivalent to computinf $p_i(\alpha^i)$, and hence

$$S_i = p_i(\alpha^i) = r(\alpha^i) = e(\alpha^i),\ 1 \leq i \leq 2t$$

which further implies that the syndrome vector $\mathbf{S}$ depends only on the error vector $\mathbf{e}$

Next task Find the error locations
Note that

$$S_i = e(\alpha^i) = \sum_{u=1}^{v} \left(\alpha^{j_u}\right)^i, 1 \leq i \leq 2t$$

BCH codes

Thus we have relations between the syndrome entries and the error parameters α^{j_u}, $1 \leq u \leq v$:

$$\begin{aligned} S_1 &= \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_v} \\ S_2 &= (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_v})^2 \\ \vdots & \quad\ \vdots \\ S_{2t} &= (\alpha^{j_1})^{2t} + (\alpha^{j_2})^{2t} + \ldots + (\alpha^{j_v})^{2t} \end{aligned}$$

where the unknown parameters α^{j_u}, $1 \leq u \leq v$ are called the error-location numbers

BCH codes

Thus we have relations between the syndrome entries and the error parameters α^{j_u}, $1 \le u \le v$:

$$\begin{aligned} S_1 &= \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_v} \\ S_2 &= (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_v})^2 \\ \vdots & \quad \vdots \\ S_{2t} &= (\alpha^{j_1})^{2t} + (\alpha^{j_2})^{2t} + \ldots + (\alpha^{j_v})^{2t} \end{aligned}$$

where the unknown parameters α^{j_u}, $1 \le u \le v$ are called the error-location numbers

When the parameters $\alpha^{j_u}, 1 \le u \le v$ are determined then the powers j_u can finally give the error locations in $e(x)$. These $2t$ equations are called power-sum symmetric functions